

*This project has received funding from the European's Union Horizon 2020 research innovation programme under Grant Agreement No. 957258*



## Architecture for Scalable, Self-\*, Human-centric, Intelligent, Secure, and Tactile next generation IoT



### D3.1 – State-of-the-Art and Market Analysis Report

<b>Deliverable No.</b>	D3.1	<b>Due Date</b>	31-JAN-2021
<b>Type</b>	Report	<b>Dissemination Level</b>	Public
<b>Version</b>	1.0	<b>WP</b>	WP3
<b>Description</b>	Document with main results of SotA review and stakeholders and market analysis carried out.		

# Copyright

Copyright © 2020 the ASSIST-IoT Consortium. All rights reserved.

The ASSIST-IoT consortium consists of the following 15 partners:

UNIVERSITAT POLITÈCNICA DE VALÈNCIA	Spain
PRODEVELOP S.L.	Spain
SYSTEMS RESEARCH INSTITUTE POLISH ACADEMY OF SCIENCES	Poland
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	Greece
TERMINAL LINK SAS	France
INFOLYSIS P.C.	Greece
CENTRALNY INSTYTUT OCHRONY PRACY – PAŃSTWOWY INSTYTUT BADAWCZY	Poland
MOSTOSTAL WARSZAWA S.A.	Poland
NEWAYS TECHNOLOGIES BV	Netherlands
INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	Greece
KONECRANES FINLAND OY	Finland
FORD-WERKE GMBH	Germany
GRUPO S 21SEC GESTION SA	Spain
TWOTRONIC GMBH	Germany
ORANGE POLSKA SPOLKA AKCYJNA	Poland

# Disclaimer

This document contains material, which is the copyright of certain ASSIST-IoT consortium parties and may not be reproduced or copied without permission. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The information contained in this document is the proprietary confidential information of the ASSIST-IoT Consortium (including the Commission Services) and may not be disclosed except in accordance with the Consortium Agreement. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the Project Consortium as a whole nor a certain party of the Consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk and accepts no liability for loss or damage suffered by any person using this information.

The information in this document is subject to change without notice.

The content of this report reflects only the authors' view. The Directorate-General for Communications Networks, Content and Technology, Resources and Support, Administration and Finance (DG-CONNECT) is not responsible for any use that may be made of the information it contains.

## Authors

Name	Partner	e-mail
Carlos E. Palau	P01 – UPV	<a href="mailto:cpalau@com.upv.es">cpalau@com.upv.es</a>
Ignacio Lacalle-Úbeda	P01 – UPV	<a href="mailto:iglaub@upv.es">iglaub@upv.es</a>
Alejandro Fornés	P01 – UPV	<a href="mailto:alforlea@upv.es">alforlea@upv.es</a>
César López	P01 – UPV	<a href="mailto:csalpepi@upv.es">csalpepi@upv.es</a>
Carlos Guardiola	P01 – UPV	<a href="mailto:carguaga@upv.es">carguaga@upv.es</a>
Andreu Belsa	P01 – UPV	<a href="mailto:anbepel@upv.es">anbepel@upv.es</a>
Ángel Martínez-Cavero	P02 – PRO	<a href="mailto:amartinez@prodevelop.es">amartinez@prodevelop.es</a>
Eduardo Garro	P02 – PRO	<a href="mailto:egarro@prodevelop.es">egarro@prodevelop.es</a>
Miguel Ángel Llorente	P02 – PRO	<a href="mailto:mllorente@prodevelop.es">mllorente@prodevelop.es</a>
Maria Ganzha	P03 – IBSPAN	<a href="mailto:maria.ganzha@ibspan.waw.pl">maria.ganzha@ibspan.waw.pl</a>
Paweł Szmeja	P03 – IBSPAN	<a href="mailto:pawel.szmeja@ibspan.waw.pl">pawel.szmeja@ibspan.waw.pl</a>
Marcin Paprzycki	P03 – IBSPAN	<a href="mailto:marcin.paprzycki@ibspan.waw.pl">marcin.paprzycki@ibspan.waw.pl</a>
Katarzyna Wasielewska	P03 – IBSPAN	<a href="mailto:katarzyna.wasielewska@ibspan.waw.pl">katarzyna.wasielewska@ibspan.waw.pl</a>
Piotr Lewandowski	P03 – IBSPAN	<a href="mailto:piotr.lewandowski@ibspan.waw.pl">piotr.lewandowski@ibspan.waw.pl</a>
Georgios Stavropoulos	P04 – CERTH	<a href="mailto:stavrop@iti.gr">stavrop@iti.gr</a>
Konstantinos Votis	P04 – CERTH	<a href="mailto:kvotis@iti.gr">kvotis@iti.gr</a>
Francisco Blanquer	P05 – TL	<a href="mailto:ho.fblanquer@terminal-link.com">ho.fblanquer@terminal-link.com</a>
Nikolaos Vrionis	P06 - INF	<a href="mailto:nvrionis@infolysis.gr">nvrionis@infolysis.gr</a>
Angeliki Papaioannou	P06 - INF	<a href="mailto:apapaioannou@infolysis.gr">apapaioannou@infolysis.gr</a>
Vaios Koumaras	P06 - INF	<a href="mailto:vkoumaras@infolysis.gr">vkoumaras@infolysis.gr</a>
Anna Dąbrowska	P07 – CIOP-PIB	<a href="mailto:andab@ciop.lodz.pl">andab@ciop.lodz.pl</a>
Krzysztof Baszczyński	P07 – CIOP-PIB	<a href="mailto:krbas@ciop.lodz.pl">krbas@ciop.lodz.pl</a>
Grzegorz Owczarek	P07 – CIOP-PIB	<a href="mailto:growc@ciop.lodz.pl">growc@ciop.lodz.pl</a>
Piotr Dymarski	P08 – MOW	<a href="mailto:P.Dymarski@mostostal.waw.pl">P.Dymarski@mostostal.waw.pl</a>
Ron Schram	P09 – NEW	<a href="mailto:roel.vossen@newayselectronics.com">roel.vossen@newayselectronics.com</a>
Dennis Engbers	P09 – NEW	<a href="mailto:dennis.engbers@newayselectronics.com">dennis.engbers@newayselectronics.com</a>
Konstantinos Naskou	P10 – ICCS	<a href="mailto:konstantinos.naskou@iccs.gr">konstantinos.naskou@iccs.gr</a>
Daniel Roettger	P12 – FORD	<a href="mailto:droettge@ford.com">droettge@ford.com</a>
Klaus Schusteritz	P12 – FORD	<a href="mailto:kschust4@ford.com">kschust4@ford.com</a>
Oscar Lopez	P13 – S21SEC	<a href="mailto:olopez@s21sec.com">olopez@s21sec.com</a>
Zbigniew Kopertowski	P15 – OPL	<a href="mailto:zbigniew.kopertowski@orange.com">zbigniew.kopertowski@orange.com</a>
Jaroslav Legierski	P15 – OPL	<a href="mailto:jaroslav.legierski@orange.com">jaroslav.legierski@orange.com</a>

## History

Date	Version	Change
18-Nov-2020	0.1	ToC and task assignments
03-Dic-2020	0.2	First contributions to the State of the Art
07-Dic-2020	0.3	ToC for the market analysis and assignments
14-Dic-2020	0.4	Second integration from several partners
23-Dic-2020	0.5	Third integration from several partners
12-Jan-2021	0.6	Fourth integration from several partners
15-Jan-2021	0.7	Harmonized version to be confirmed by UPV contributors
21-Jan-2021	0.71	Harmonized version to be confirmed by ICCS contributors. Added Market analysis first iteration
26-Jan-2021	0.72	Harmonized version to be confirmed by CErTH/SRIPAS contributors
01-Feb-2021	0.74	Harmonized version with CErTH/SRIPAS contributions in the SotA, and the market analysis from NEW and the workshop minutes
05-Feb-2021	0.8	Version to be reviewed by IR
17-Feb-2021	0.9	Version corrected according to IR comments
19-Feb-2021	1.0	Version corrected according to WPL and PC review

## Key Data

<b>Keywords</b>	State-of-the-Art, Market Analysis, NG-IoT, Edge/Fog computing, Interoperability, DLT, Self-*, Port Automation, Cohesive Diagnostics, Safety of Workers
<b>Lead Editor</b>	Angel Martínez-Cavero P02 PRO Eduardo Garro P02 PRO
<b>Internal Reviewer(s)</b>	Anna Dąbrowska P07 CIOP-PIB Piotr Dymarski P08 MOW



# Executive Summary

The evolution of human-machine interaction is just as remarkable as the technological advances that made the impossible possible and changed the way we live. The relationship with machines has been redefined: machines moved from tool to partner and from automation to autonomy. The Internet of Things is connecting physical, digital, virtual, and cyber worlds, leading to a new evolution in human-machine interaction. The next-generation Tactile Internet will allow real-time interaction between humans and machines.

The EU-funded ASSIST-IoT (EU H2020 ICT-56-2020) project<sup>1</sup> will develop the reference architecture in which intelligence can be distributed among nodes by implementing artificial intelligence and machine learning close to data generation and actuation, and hyper connecting nodes, in the edge-cloud continuum, over software and smart networks. Smart networks will be realised by means of virtualized functions, with clear separation of control and data planes, facilitating efficient infrastructure programmability. Moreover, the action will follow a DevSecOps methodology to ensure the integration of security, privacy, and trust, by design, in all aspects of the envisioned ecosystems. In addition, the ASSIST-IoT initiative will be supported by several pillars: (i) innovative IoT architecture to adapt to the Next Generation Internet paradigm supporting decentralized collaborative decision-making; (ii) moving from semantic interoperability to semantically-enabled cross-platform, cross-domain data transactions, within decentralized governance, Distributed Ledger Technologies anchoring transaction security, privacy and trust; (iii) development and integration of innovative devices, supporting context-aware computing, to enable effective decision making close to events; (iv) introduction of self-\* mechanisms, supporting self-awareness and (semi-)autonomous behaviours across IoT deployments, and (v) tactile internet support for latency applications, like Augmented Reality – Virtual Reality – Mixed Reality (AR/VR/MR), and human-centric interaction with IoT components. Results of the action will provide foundation for a comprehensive practice-based methodology, for future designers and implementers of smart IoT ecosystems.

Finally, in order to validate research results, developed solutions and to ensure their wide applicability in the industry, extended pilot deployments with strong end-user participation will take place in: (i) port automation; (ii) smart safety of workers, and (iii) cohesive vehicle monitoring and diagnostics, bringing about domain-agnostic aspect of the approach. In ASSIST-IoT there is continuous assessment and verification of the initial hypothesis during the whole timeframe of the project in order to ensure that developments carried out makes sense for the industry which will make easier its future adoption in the real market. Deliverable D3.1 (i.e., State-of-the-Art and Market Analysis Report) is the first step in such direction since it presents not only an exhaustive state of the art of the core technologies of the ASSIST-IoT initiative, but also a detailed review of the current situation of the market (in both technological opportunities and verticals where the pilots will be carried out). The market analysis has been populated taking into account several sources of information: desk research, a workshop with industry stakeholders and representatives, an online survey and several 1-to-1 interviews with well-known leaders and experts from both academia and the industries contemplated in the project.

---

<sup>1</sup> <https://cordis.europa.eu/project/id/957258/es>

# Table of contents

1	About this document .....	14
1.1	Deliverable context .....	14
2	Introduction .....	15
3	State of the art .....	16
3.1	NG-IoT technologies .....	16
3.1.1	NGIoT architectures .....	16
3.1.2	Hyperconnectivity .....	27
3.1.3	Edge/fog computing .....	46
3.1.4	Interoperability .....	64
3.1.5	DLT and semantics .....	75
3.1.6	Distributed intelligence .....	76
3.1.7	Self-* .....	86
3.1.8	Human-machine interfaces for collaboration .....	98
3.1.9	Vertical applications of the Tactile Internet .....	100
3.1.10	IoT security and software development using DevSecOps on IoT ecosystems .....	109
3.2	NG-IoT pilots / testbeds .....	113
3.2.1	State of the art in Port Automation .....	113
3.2.2	State of the art in Smart Safety of Workers .....	119
3.2.3	State of the art in Cohesive Vehicle Monitoring and Diagnostics .....	128
4	NG-IoT H2020 Ecosystem .....	132
4.1	European IoT calls .....	132
4.2	Non-IoT but related calls .....	154
4.2.1	5G Research Projects Ecosystem and 5G-PPP .....	155
5	Market analysis .....	166
5.1	NG-IoT market analysis .....	166
5.1.1	The Global IoT market .....	166
5.1.2	IoT value chain analysis .....	166
5.1.3	Market Size and Forecast .....	167
5.1.4	Market Drivers .....	173
5.1.5	Competitive landscape .....	176
5.1.6	The IoT global intellectual property landscape .....	178
5.2	Verticals addressed in ASSIST-IoT .....	179
5.2.1	Port automation – Maritime logistics .....	179
5.2.2	Smart safety of Workers – Construction .....	184
5.2.3	Cohesive Vehicle monitoring – Automotive .....	190
5.3	Stakeholders engagement .....	196
5.3.1	Workshop .....	196
5.3.2	Interviews .....	199
5.3.3	Online survey .....	208
6	Conclusions .....	215
	References .....	217

## List of tables

Table 1. Relevant IoT Reference Architectures from funded research projects.....	23
Table 2. Relevant IoT Reference Architectures from public-private/private consortiums and SDOs.....	25
Table 3. Relevant IoT Reference Architectures from private industrial providers.....	26
Table 4. List of VNFs by activity.....	32
Table 5. List of common SDN controllers .....	37
Table 6. AI proposals over SDN .....	39
Table 7. Open RAN initiatives .....	42
Table 8. Proposals implementing SDN in radio networks .....	42
Table 9. Proposals implementing SDN in wireless IoT networks .....	44
Table 10. Proposals implementing SDN in SD-WAN networks.....	44
Table 11. Glossary clarification about edge/fog computing .....	48
Table 12. Summary of edge computing implementations comparison.....	50
Table 13. Edge/Fog computing standardization entities.....	61
Table 14. Edge/Fog computing alliances.....	62
Table 15. Edge/Fog computing research projects.....	62
Table 16. IoT standard activities.....	69
Table 17. Interoperability approach in IoT European Open Platforms.....	71
Table 18. IoT European Platforms Initiative.....	72
Table 19. Example table caption above table.....	73
Table 20. Summary of considered papers.....	79
Table 21. Known tools for distributed learning.....	85
Table 22. Federated Learning Tools.....	85
Table 23. Comparison among existing Federated Learning Libraries.....	86
Table 24. Fault classes levels .....	93
Table 25. Tactile applications based on haptic information.....	105
Table 26. Tactile applications based on human interaction information .....	106
Table 27. Tactile applications based on M2M information .....	107
Table 28. Application-agnostic architectures for tactile internet.....	108
Table 29. Expected global edge market size and CAGR from different consultancy enterprises.....	167
Table 30. Expected global 5G market size from different consultancy enterprises .....	170
Table 31. Expected global industrial connectivity market size from 2020 up to 2024.....	171
Table 32. Expected global AI market size from different consultancy enterprises .....	172
Table 33. Peer-to-peer interviewees profile and their most relevant answers .....	200

## List of figures

Figure 1. Functional-decomposition viewpoint of the IoT-A reference architecture. Source: IoT-A D1.5 [NG-IoT-18].	19
Figure 2. SGAM structure [NG-IoT-20].	19
Figure 3. IIRA functional domains and system characteristics [NG-IoT-4].	20
Figure 4. Reference architectural model Industry 4.0 (RAMI 4.0) [NG-IoT-22].	20
Figure 5. LSP IoT 3D reference architecture [NG-IoT-23].	21
Figure 6. OpenFog Reference Architecture [NG-IoT-24].	22
Figure 7. Reference Architecture Model Edge Computing (RAMEC) [NG-IoT-25].	22
Figure 8. Programmable network concept	28
Figure 9. Main SDN structure.	28
Figure 10. Main NFV architecture [HYP-7].	29
Figure 11. Single/hierarchical physically distributed architectures.	31
Figure 12. RAN solution architecture.	33
Figure 13. IoT infrastructure implementation.	34
Figure 14. Software defined mesh & home networks.	34
Figure 15. Software-defined WAN approach vs traditional approach.	35
Figure 16. SD-WAN architecture [HYP-24].	35
Figure 17. SDN management approach.	38
Figure 18. FlowVisor location in a SDN network example	38
Figure 19. FINE framework [HYP-34].	39
Figure 20. FTDP implementation [HYP-36].	39
Figure 21. CISCO NFV Infrastructure <sup>19</sup> .	40
Figure 22. NFV and SDN interface abstraction [HYP-37].	41
Figure 23. MANO and RAN initiatives [HYP-39].	41
Figure 24. O-RAN architecture	42
Figure 25. SoftAir architecture [HYP-42]	43
Figure 26. SDN-WISE architecture [HYP-39].	43
Figure 27. B4 element distribution concept [HYP-46]	44
Figure 28. Classic processing and analytics approach, where the computation is mainly done at cloud level.	46
Figure 29. Edge-to-cloud computing continuum approach and its advantages [EDGE-10]	47
Figure 30. Wide spectrum of potential edge-to-cloud continuum devices.	49
Figure 31. Main differences between edge computing implementations. From left to right: MEC, Cloudlet and FC.	50
Figure 32. Venn diagram about paradigms, orientations and naming in edge computing [EDGE-33].	51
Figure 33. ETSI specification architecture and API for MEC in 5G.	52
Figure 34. Left: Cloudlet illustrative diagram [EDGE-127]. Right: Offloading basics in a cloudlet schema [EDGE-126]	52
Figure 35. Mobile cloud (or mesh) architecture [EDGE-127].	54
Figure 36. Fog computing structure basis [EDGE-127].	56
Figure 37. OpenFog Reference Architecture. Extracted verbatim from the official specification [EDGE-102].	57
Figure 38. Fog node basics software according to OpenFog RA.	58
Figure 39. EdgeX Foundry fog computing platform.	59
Figure 40. Fog node implementation for EdgeX: Fledge.	60
Figure 41. FogAtlas platform architecture.	60
Figure 42. Physical IoT gateway from INTER-IoT as potential fog node.	61
Figure 43. Number of published papers concerning federated databases, federated cloud, and federated learning	79
Figure 44. Schema of Federated Learning Architecture [DL-13]	80
Figure 45. Tools for Distributed Learning	84
Figure 46. LRA-M architecture	89
Figure 47. model@run.time architecture.	91

Figure 48. Metrics for self-aware systems [SELF-51].....	93
Figure 49. Self-security taxonomy [SELF-60] .....	95
Figure 50. Observer/Controller architecture used for the trustworthy self-* layer [SLF-61] .....	96
Figure 51. Tactile Internet context evolution [TI-3]. .....	101
Figure 52. ITU-T multi-stage hierarchy proposal [TI-2]. .....	102
Figure 53. IEEE 1918.1 architecture with gateway node and network controller at the tactile edge (left) and at the network domain (right) [TI-5]. .....	102
Figure 54. Tactile internet infrastructure elements that intervene in the delay of data transmission.....	103
Figure 55. Tactile Internet main architecture. ....	104
Figure 56. FIWI multirobot network architecture [TI-23]. ....	106
Figure 57. Hospital campus tactile internet proposal [TI-24]. ....	106
Figure 58. VR phobia treatment architecture concept [TI-1]. ....	107
Figure 59. Interactive VR game proposal. ....	107
Figure 60. Automated driving core subsystems [TI-30]. ....	108
Figure 61. Smart city 5-layer architecture proposal .....	108
Figure 62. FlexNGIA concept [TI-32].....	109
Figure 63. SDN/NFV architecture for Tactile Internet [TI-10]. ....	109
Figure 64: DevOps cycle.....	110
Figure 65: DevOps evolution model in 5 stages.....	112
Figure 66: DevOps evolution and platform evolution .....	112
Figure 67: DevSecOps. DevSecOps with security [IoTDSO-4] .....	113
Figure 68. Dell-Intel edge and IoT portfolio for port operations [PA-10]. ....	115
Figure 69. ML deployment over smart ports [PA-11]. ....	116
Figure 70. Helmet developed by Arayl et al. a) Facial skin temperature monitoring locations; b) Test person wearing a developed helmet [SSW-27]. ....	122
Figure 71. (a) A vest with temperature sensors (b) and LED diode signalling incorrect temperature values [SSW-28]. ....	123
Figure 72. A view of the measuring system for construction workers (A), where: a) a heart rate and acceleration sensor WHS-2, b) smart clothing (COCOMI), c) data acquisition device (CC2650), and the system configuration (B) [SSW-29] .....	123
Figure 73. Procedure of stress recognition [SSW-32]. ....	124
Figure 74. Thermal manikin wearing cooling devices for construction workers a) fans; b) PCM; c) reference clothing [SSW-37].....	126
Figure 75. A vest with location tracking system developed by RPC.....	127
Figure 76. The principle of operation of the system of automatic identification and management of personal protective equipment in the workplace [SSW-59]. ....	128
Figure 77. Evolution of IoT ecosystem based on different research action. ....	132
Figure 78. Overview of the 5G-PPP Programme .....	156
Figure 79 Mapping of use cases to vertical categories .....	156
Figure 80. 5G Infrastructure PPP Phase 3 Platforms Projects – Geographic Cartography .....	157
Figure 81. Vertical industries under validation by ICT-17 and ICT-19 projects.....	158
Figure 82. 5G-PPP Phase 3 Reference Figure.....	158
Figure 83. 5G-PPP Key Achievements v3.0.....	159
Figure 84. Global market estimations [MA-2] .....	166
Figure 85. Simplified vertical domains stakeholders' value of the IoT value chain.....	167
Figure 86. IoT value chain [MA-3] .....	167
Figure 87. Global IoT Edge computing hardware per application segment [MA-6].....	168
Figure 88. Global Edge computing market per application segment [MA-5].....	169
Figure 89. IDC global fog computing market estimations.....	169
Figure 90. 5G Technology Market by application segment.....	171
Figure 91. 5G market compass 2020-2030 - ericsson.com .....	171
Figure 92. Global AI market by application .....	172
Figure 93. Global Blockchain DL by Type and End-users [MA-17] .....	173
Figure 94. Competitive IoT Edge Computing Technology [MA-20] .....	177
Figure 95. Major fields of investment by leading AI enterprises [MA-21] .....	178

Figure 96. Global IoT Patents landscape <sup>111</sup> .....	179
Figure 97. Global IoT Company Patens ranking <sup>111</sup> .....	179
Figure 98. Growth of real trade to growth of real GDP [MA-23]. .....	180
Figure 99. Diffusion of key port terminal automation technologies <sup>112</sup> .....	181
Figure 100. Existing and planned automated container terminals [MA-29] .....	182
Figure 101. Proportion of automated container terminals worldwide [MA-29]. .....	183
Figure 102. Fatal and non-fatal accidents at work in EU-27 in 2018 [MA-30]. .....	184
Figure 103. Fatal accidents trend at work for the five riskiest NACE sections in EU-27 from 2010 to 2018. ....	185
Figure 104. Percentage of fatal and non- fatal accidents at work in EU-27 in 2018. ....	186
Figure 105. ELA innovation localisation suite. Anchors (left), tags (centre), and gateways (right). ....	187
Figure 106. AeroScout suite. Active RFID tags (left), Wi-Fi access points (centre), and MobileView software (right). ....	187
Figure 107. nanotron HW equipment, including nanoTAG, nanoTAG LP and nanoTAG RX, and nanotron edge anchor (top). Nanotron real-time localisation positioning working diagram (bottom). ....	188
Figure 108. Work-related injuries and illnesses result to a cost in euros of approximately 2,680 billion globally and 476 billion in EU, respectively [MA-31]. ....	189
Figure 109. Digital construction future trends .....	189
Figure 110. ECU vehicle connectivity to the OEM will benefit both the OEM and the customer. ....	191
Figure 111. Automotive revenue pool in high-disruption scenario, USD billion [MA-38]). ....	194
Figure 112. Forecast of fleet management market, by region in USD billion [MA-39]. ....	194
Figure 113. SOVD - Service Oriented Vehicle Diagnostics project by ASAM. ....	195
Figure 114. ASSIST-IoT 1 <sup>st</sup> workshop communication on social media channels. ....	196
Figure 115. ASSIST-IoT 1 <sup>st</sup> workshop submission form webpage. ....	197
Figure 116. Pilot environments slide from the 1 <sup>st</sup> ASSIST-IoT workshop. ....	198
Figure 117. Online Survey announcement slide of 1 <sup>st</sup> ASSIST-IoT workshop. ....	198
Figure 118. ASSIST-IoT online survey form webpage .....	208
Figure 119. ASSIST-IoT social posts for attracting attention to project's online survey .....	208
Figure 120. ASSIST-IoT survey participant profiles. ....	210
Figure 121. Main tasks using ICT solutions (top), and most important features required for the successful deployment of an ICT system (bottom). ....	211
Figure 122. Execution efficiencies without ICT systems (left), and main concerns for ICT proper functioning and deployment (right). ....	212
Figure 123. Data management analysis .....	212
Figure 124. Business operations based on data analysis. ....	213
Figure 125. Unstructured data and real-time predictions. ....	213
Figure 126. Interest on ICT cloud-based deployments .....	214
Figure 127. Data rate limitations, zero-latency, and HMI needs. ....	214



## List of acronyms

Acronym	Explanation	Acronym	Explanation
3D	Three-dimensional	CPS	Cyber-Physical Systems
3GPP	Third Generation Partnership Project	CPU	Central processing unit
4G	4th Generation Mobile Systems	CSA	Coordination and Support Action
5G	5th Generation Mobile Systems	DCAN	Devolved Control of ATM Networks
5G-PPP	5G Infrastructure Public Private Partnership	DCN	Dynamic circuit network
6LoWPAN	IPv6 over Low -Power Wireless Personal Area Networks	DevOps	Software Development and IT operations
ACO	Ant Colony Optimisation	DHT	Distributed Hash Table
AGV	Automated Guided Vehicles	DIT	Decentralised Interoperable Trust
AI	Artificial Intelligence	DL	Distributed / Deep Learning
AIOTI	Alliance for the Internet of Things Innovation	DLT	Distributed Ledger Technology
AIS	Automatic Identification System	ECG	Electrocardiography
AMQP	Advanced Message Queuing Protocol	ECM	Electronic Control Modules
API	Application Programming Interface	ECS	Equipment Control & Scheduling system
AR	Augmented Reality	ECU	Engine Control Unit
ASC	Automated Stacking Cranes	EECC	European Edge Computing Consortium
AWS	Amazon Web Services	EEG	Electroencefalography
B5G	Beyond 5G	EGP	Exterior Gateway Protocol
BDRA	Big Data Reference Architecture	ENISA	European Union Agency for Cybersecurity
BDVA	Big Data Value Association	ESP	European Security and Privacy Projects
BFSI	Banking, Financial Services, and Insurance	ETA	Estimated Time of Arrival
BGP	Border Gateway Protocol	ETC	Estimated Time of Completion
BH	Back Haul	ETSI	European Telecommunications Standards Institute
BIM	Building Information Modelling	EU	European Union
BLE	Bluetooth Low Energy	FC	Fog Computing
BMI	Body Mass Index	FCAPS	Fault, Configuration, Accounting, Performance, Security
CAGR	Compound Annual Growth Rate	FG	Functional Groups
CAN	Control Area Network	FH	Front Haul
CC	Cloud Computing	FL	Federated Learning
CCAM	Cooperative Connected and Automated Mobility	FPGA	Field-programmable gate array
CCD	Charge Coupled Device	GA	Grant Agreement
CHE	Cargo Handling Equipment	GAN	Generative Adversarial Networks
CI/CD	Continuous Integration and Continuous Delivery	GAS	Gate Automation System
CMOS	Complementary MOS	CPS	Cyber-Physical Systems

GDP	Gross Domestic Product	JSON	JavaScript Object Notation
GDPR	General Data Protection Regulation	JTAG	Joint Test Action Group
GNSS	Global Navigation Satellite System	KNN	K-Nearest Neighbors
GPRS	General Packet Radio Service	LED	Light-Emitting Diode
GPS	Global Positioning System	LF	Linux Foundation
GPU	Graphics processing unit	LPWAN	Low Power Wide Area Network
GVR	Grand-view-Research	LRA	Learn-Reason-Act
H&S	Health and Safety	LSP	Large-Scale Pilots
HACCP	Hazard Analysis Critical Control Points	LSP	Large Scale Pilots
HARM	Hierarchical Attack Representation Model	LTE	Long Term Evolution
HD	High Defintion	LXD	Linux Containers
HLA	High-Level Architecture	M2M	Machine to Machine
HMI	Human-to-Machine Interface	MAC	Media Access Control
HPC	High-Performance Computing	MANO	Management and Orchestration
HTTP	Hypertext Transfer Protocol	MAPE	Monitor-Analyze-Plan-Execute
IaaS	Infrastructure as a Service	MAS	Multi-Agent Systems
ICT	Information and Communications Technologies	MCU	Microcontroller Unit
IEC	International Electrotechnical Commission	MEC	Multi-access Edge Computing
IEEE	Institute of Electrical and Electronics Engineers	ML	Machine Learning
IETF	Internet Engineering Task Force	mMTC	massive Machine Type Communications
IGP	Interior Gateway Protocol	MNO	Mobile Network Operator
IIC	Industrial Internet Consortium	MPC	Multi-Party Computation
IIoT	Industrial IoT	MPLS	Multiprotocol Label Switching
IIRA	Industrial Internet Reference Architecture	MQTT	Message Queuing Telemetry Transport
ILP	Inter-ledger Protocol	MQTT	Message Queuing Telemetry Transport
IM	Innovation Manager	MR	Mixed Reality
INS	Inertial Navigation System	MW	MicroWaves
IoT	Internet of the Things	NA	Network Analytics
IP	Internet Protocol	NBI	Northbound Interface
IPR	Intellectual Property Rights	NB-IoT	NarrowBand IoT
IR	Interal review	NCP	NetWare Core Protocol
ISC	In-Service Conformity	NFC	Near Field Communication
ISO	International Organization for Standardization	NFV	Network Function Virtualisation
ISP	Internet Service Provider	NFVI	Network Function Virtualisation Infrastructure
ITU	International Telecommunciations Union	NFVO	NFV Orchestrator
IVT	Immersive Visual Technologies	NG-EPON	Next Generation Ethernet passive optical network
LPWAN	Low Power Wide Area Network	NGI	Next Generation Internet of Things



NIST	National Institute of Standards and Technology	SD-SEC	Software Defined Security
NR	New Radio	SD-WAN	Software Define Wide Area Networks
NSaaS	Network Slice as a Service	SGAM	Smart Grid Architecture model
OBD-II	On Board Diagnostic II	SGD	Stochastic Gradient Descent
OCR	Optical Character Recognition	SIFT	Scale-Invariant Feature Transform
OEM	Original Equipment Manufacturer	SLA	Service Level Agreement
ONAP	Open Network Automation Platform	SME	Small and Medium-sized Enterprise
OPC-UA	OPC Unified Architecture	SNMP	Simple Network Management Protocol
ORM	Object-Role Modelling	SOA	Service oriented architecture
OS	Operating System	SOAP	Simple Object Access Protocol
OSH	Occupational safety and health	SON	Self-Organised Networks
OSS/BSS	Operations Support Systems	SSD	Single Shot Detectors
OTA	Over-The-Air	SVM	Support Vector Machine
OWL	Web Ontology Language	SVM	Support Vector Machine
PC	Project Coordinator	TCI	Thermal Comfort Index
PCM	Phase Change Materials	TCP	Transmission Control Protocol
PKI	Public Key Infrastructure	TOGAF	The Open Group Architecture Framework
PPE	Personal Protective Equipment	TOS	Terminal Operating Systems
QoS	Quality of Service	TPU	Tensor Processing Unit
QR	Quick Response	TSN	Time Sensitive Networks
RA	Reference Architecture	UAV	Unmanned Aerial Vehicle
RAMEC	Reference Architecture Model Edge Computing	UHF	Ultra High Frequency
RAMI	Reference Architectural Model Industry	UML	Unified Modelling Language
RAN	Radio Access Network	UN	United Nations
RCP	Routing Control Platform	URLLC	Ultra-Reliable Low Latency Communication
RDF	Resource Description Framework	USB	Universal Serial Bus
RDF	Resource Description Framework	UV	Ultraviolet
ReLU	Rectified Linear Units	UWB	Ultra Wide Band
REST	Representational State Transfer	VIM	Virtualised Infrastructure Manager
REST	Representational state transfer	VIMS	Virtual IoT Maintenance System
RFID	Radio-frequency identification	VNF	Virtualised Network Function
RGB	Red-Green-Blue	VR	Virtual Reality
RIA	Research and Innovation Action	WBGT	Wet Bulb Globe Temperature
RMG	Rail Mounted Gantry	WIMU	Wearable Inertial Measurement Units
RNC	Radio Network Controller	WLAN	Wireless Local Area Network
RNN	Random Neural Networks	WP	Work Package
RRM	Radio Resource Management	WSN	Wireless Sensor Network
RTG	Rubber Tyred Gantry	XML	Extensible Markup Language
SBI	Southbound Interface	ZDM	Zero Defect Manufacturing
SDG	Sustainable Development Goals	ZTM	Zero Touch Management
SDK	Software Development Kit		
SDN	Software Defined Networking		

# 1 About this document

To successfully meet the ASSIST-IoT envisioned objective (including design, development, and deployment in realistic scenarios), an initial stage focused on an in-depth state-of-the-art analysis of the existing, and newly materializing solutions and trends in the research ecosystem is needed. The scope of this report is to gather the most recent insights into current IoT architectures, approaches to NGI edge/fog computing, scalability, self-\*, manageability and adaptability mechanisms, new automatic and dynamic network paradigms, with focus on real deployments. It starts with an in-depth State-of-the-Art assessment of existing, and newly materializing, solutions and trends – with special focus on existing/proposed standards and research projects – followed by a market analysis using four different approaches: desk research by means of market reports analysis, in-depth interviews with experts and ASSIST-IoT stakeholders, end-user online surveys, and an online workshop held on 18<sup>th</sup> January 2021. Therefore D3.1 is seen by ASSIST-IoT consortium as a baseline milestone of the technological and innovation features that will be carried out in the project and presented in follow-up reports.

## 1.1 Deliverable context

Keywords	Lead Editor
<b>Objectives</b>	<p><i><b>O1: Design, implementation, and validation of an NGIoT Reference Architecture.</b></i></p> <p><i><b>O2: Definition and implementation of distributed smart networking components.</b></i></p> <p><i><b>O3: Definition and implementation of decentralized security and privacy exploiting DLT</b></i></p> <p><i><b>O4: Definition and implementation of smart distributed AI enablers</b></i></p> <p><i><b>O5: Definition and implementation of human-centric tools and interfaces</b></i></p> <p><i><b>O6: Definition, deployment and evaluation of real-life pilots</b></i></p> <p><i><b>O7: Establishment of an innovative cooperation and business framework.</b></i></p> <p>ASSIST-IoT architecture will enable algorithms offering centralized and decentralized human-centric AI; effective deployment of scalable interoperability on all levels; self-* mechanisms across IoT ecosystems; smart networking and integration with NFV and SDN; and security, privacy, and trust by design, supported by DLT. To carry out this ambitious plan, D3.1 is seen as the technical and innovation benchmarking report needed to clearly identify the missing components and bottlenecks that have not been addressed yet and that will be used and enhanced in ASSIST-IoT. Because of that, D3.1 addresses almost all objectives of ASSIST-IoT from a state-of-the-art/market perspective.</p>
<b>Work plan</b>	<p>This deliverable belongs to the set of WP3 deliverables and it is directly linked to the T3.1 activity. T3.1 main objective is to refresh most recent insights into IoT architectures, edge/fog computing, scalability, self-*, manageability and adaptability mechanisms, with focus on real-world deployments. Hence, D3.1 can be used as a key reference for the following work to be carried out on the formalization of the use cases (T3.2), the rest of technical WPs (WP4-WP6), pilots' WP7, as well as to the business model in T3.3 and exploitation and innovation activities within T9.4.</p>
<b>Milestones</b>	<p>D3.1 has an indirect contribution to WP3 milestones MS2 Use cases and requirements defined and MS3 Enablers defined.</p>
<b>Deliverables</b>	<p>This deliverable precedes the work to be carried out regarding the ASSIST-IoT architecture definition to be assessed within D3.5, D3.6, D3.7, which will consequently impact the enablers design activities covered within WP4, WP5, and WP6. Additionally, the initial market analysis carried out will also serve as a guideline and blueprint for identifying the exploitation and innovation activities at ASSIST-IoT, which will be reported in D9.2, D9.6, D9.7, and D9.8.</p>

## 2 Introduction

The ASSIST-IoT project aims at designing, implementing, and validating an open, decentralized, reference Next Generation IoT (NG-IoT) architecture, with its corresponding enablers, services, and tools for assisting human-centric applications within multiple verticals. This objective is fully aligned with Next Generation Internet (NGI) vision, in which an Internet that responds to people's fundamental needs, including trust, security, and inclusion, while reflecting the values and the norms all citizens enjoy in Europe is envisioned.

To accomplish ASSIST-IoT and NGI visions, several key enablers will be required for guaranteeing the successful deployment of NG-IoT reference architecture in the three human-centric pilots embraced in the project, i.e., port automation, smart safety of workers, and cohesive vehicle monitoring. ASSIST-IoT follows the AIOTI<sup>2</sup> response to public consultation on European Partnership for the successful development of Smart Networks and Services under the Horizon Europe Programme, in which AI-based control systems (distributed intelligence) in critical areas (edge computing, tactile-internet) will depend on data (interoperability) provided by billions of IoT nodes (hyperconnectivity), communicating over smart networks. Furthermore, ASSIST-IoT forms its human-centric leitmotif adding fundamental NGI pillars such as resilience, sustainability, privacy, and trust with the help of e.g., Distributed Ledger Technologies (DLTs), seen as instrumental to the digital transition and Europe's industrial future<sup>3</sup>.

However, to successfully attain the ASSIST-IoT envisioned objective (including design, development, and deployment in realistic scenarios), an initial stage focused on an in-depth state-of-the-art analysis of the existing, and newly materializing solutions and trends in the research ecosystem is needed. This deliverable gathers the most recent insights into current IoT architectures, including but not limited to hyperconnectivity, interoperability, edge/fog computing, distributed intelligence, and human-machine interfaces (HMI), DLT and semantics, and tactile internet, with a special focus on existing and proposed Standard Development Organisations (SDOs).

A solid foundation beyond already standardised solutions is a fundamental pillar for the successful accomplishment of ASSIST-IoT vision. Therefore, to build a strong and resilient reference structure, ASSIST-IoT has targeted active or recently finished European IoT Security and Privacy (ESP), and Large-Scale Pilots (LSP) projects. Moreover, ASSIST-IoT will contribute to the consolidation and coherence work that will be implemented by the CSA EU-IoT supporting the activities defined under "Horizontal Activities" of the topic call text H2020-ICT56- 2020, boosting these synergies with the other retained Research and Innovation Action (RIA) projects funding under this topic. Because of this commitment, this deliverable provides a study of current and NG-IoT technologies from the aforementioned EU research projects as a baseline for further investigation and development of its own innovative solutions in Section 4.

Finally, this report has performed a market analysis, based on four different approaches in Section 5, to provide an analysis of the most important players in the industry, and to define the market and its needs and position the project offering accordingly. The market analysis includes a desk research, in-depth interviews with experts and ASSIST-IoT stakeholders (i.e., partners or supporting members), online users' surveys, and a workshop (held on 18th Jan 2021). This information will be essential for the business development in the forthcoming work in Work Package 9 (Impact creation) in general, and for Task 9.4 (Exploitation, Innovation, Business and Market operations) in particular.

---

<sup>2</sup> <https://aioti.eu/>

<sup>3</sup> European Commission, "Next Generation Internet – The Internet of Humans", August 2019

## 3 State of the art

### 3.1 NG-IoT technologies

#### 3.1.1 NGIoT architectures

Internet of Things, in its wider sense, is a combination of existing technologies that are integrated to fulfil things-enabled applications' requirements rather than a technology per se [NG-IoT-1]. It involves a large ecosystem of tools, methods and services that have to be integrated in order to deliver a complete solution. According to [NG-IoT-2] an IoT architecture can be defined as the fundamental organisation of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution. However, IoT architectures can be too specific and focused on the particular constraints or characteristics of the case study for which it is intended to be instantiated, and for this reason emerged the concept of Reference Architectures (RA).

IoT Reference Architectures are useful models of the IoT ecosystem that serve as guidelines to implement an IoT system. They aim at handling all their requirements, forming a complete set of functionalities, information structures and mechanisms [NG-IoT-3], and acting as the reference for building compliant IoT architectures. These requirements are related to different aspects such as device management, connectivity and communications, data collection, analysis and aggregation, heterogeneity and interoperability, dynamicity, scalability, and security in order to conform IoT services and applications. As a RA stays at a higher level of abstraction, it facilitates the identification of the most important issues and patterns across its utilisation in different use cases [NG-IoT-4]. Still, it should find an adequate level of abstraction to be actually useful (i.e., if it is too abstract, it may have no utility).

Architectures are built according to the guidelines of a Reference Architecture while considering the specific constraints, opportunities, and other needed feedback from the particular targeted system. As any architecture is much more concrete and domain-specific than the RAs, not all the aspects of a RA are addressed. Besides, following the guidelines of a RA is only needed if the scope of a system is large and multiple product creations are interrelated, but not very useful for small-scale or standalone developments.

Defining a single RA as a blueprint for any potential IoT deployment is a challenging task. For this reason, even without considering novel NGI enablers, many of them coexist and the choice among them to instantiate an IoT system depend on its requirements. According to NGIoT project, a Coordination and Support Action for the Next Generation Internet of Things, the following technologies have been identified as key enablers for the next generation of IoT [NG-IoT-1]: Edge Computing, 5G (including NFV features), Artificial Intelligence and analytics, Augmented Reality and Tactile Internet, Digital Twin and Distributed Ledgers. Hence, since NGIoT architectures will include some (or all) of these enablers, RAs targeting this kind of architectures will have to address them.

Despite many of these enablers will be further reviewed in the following sections, a brief description of them as well as their applicability within the IoT domain is provided below.

- **Edge Computing.** Edge-cloud computing continuum introduces novel capabilities into IoT architectures, providing data analytics capabilities with minimum or no support from the cloud, bringing the possibility of new applications and services (e.g., human-centric) and prospect of deploying new business models. This enabler is crucial to reduce the large amounts of data that would travel to cloud premises. In combination with other technologies, such as AI, it can be used for spreading intelligence along different edge nodes, unlocking the possibility of taking decisions locally, which not only reduces response times but can also facilitate intelligent system decisions.
- **5G.** The current evolution of cellular technology is able to handle the requirements of large IoT deployments, greatly improving the current possibilities offered by other wireless technologies (e.g., LPWAN) in terms of latency, reliability, and number of connected devices. Besides, this technology does not only stand for access network, but also to backbone management, introducing infrastructure virtualisation capabilities as well as novel hardware virtualisation mechanisms. Network Function

Virtualisation (NFV) brings up new and agile methods to deploy and orchestrate IoT infrastructures, facilitating the instantiation and reconfiguration of other NGI enablers.

- **AI.** The introduction of Artificial Intelligence and its combination with other enablers, such as Edge Computing and NFV, is fundamental to improve the performance of new IoT platforms. AI libraries, frameworks and models can be applied on smart devices, on edge nodes (if they have enough computing capabilities), on network elements and/or on centric/cloud premises, being thus transversal to different layers of the system. This technology can unlock novel business models thanks to the possibility of enabling context-awareness distributed and decentralised intelligence within the system as well as facilitate human-centricity applications (see next enablers).
- **AR and Tactile Internet.** AR can offer to users an intuitive way to visualize and interact with IoT objects and their data, providing a direct and semi-tangible interface that can facilitate the comprehension of data and being highly useful for everyday and/or anywhere usage [NG-IoT-5]. Tactile Internet, on the other hand, was defined by the ITU as a *network with very low latency, an extremely short transit, a high availability, high reliability, and a high level of security*<sup>4</sup>. The purpose of this enabler is to facilitate interaction with distant humans and cyber-physical systems in real time, considering haptic interfaces and promoting human-centricity.
- **Digital Twin.** Rather than a technology by itself, it is a combination of some of the previous enablers with software analytics to realise a virtual replica of a physical entity. Its goal is to have the ability of monitoring, controlling, and simulating a physical system in the most realistic way.
- **Distributed Ledgers.** This enabler allows novel approaches for data management and governance in distributed environments. The inherent distributed nature of Edge Computing poses security and privacy challenges due to the heterogeneity of edge nodes and migration of services among the nodes in the edge. This can be solved by means of DLT, providing reliable access and control of the network, enhancing data integrity and computation validity [NG-IoT-6], being data owners the ones that control who can access these data.

Similar enablers have been defined in [NG-IoT-7], in which they consider *Hyperconnectivity* as well as end-to-end distributed security. Hyperconnectivity does not only stand for 5G and network slicing, but also for the application of SDN and NFV concepts. Thanks to all these enablers, novel IoT ecosystems must be able to fulfil the six Cs: (i) Collect data, processed or not, from heterogeneous devices, (ii) Connect distributed heterogeneous devices, (iii) Cache (i.e., store) information in a distributed IoT environment, (iv) Compute -advanced processing of information, (v) Cognise -extract insights from data thanks to AI, and (vi) Create novel interactions, services and solutions, from (a) Anything, to be transferred to/from (b) Anyone, in (c) Any place, at (d) Any time, using the appropriate path from (e) Any path, to provide (f) Any Service.

### 3.1.1.1 Scientific review

There are different architectural styles and distribution patterns according to which an IoT architecture can be designed. Among architectural styles, one can find layer-based, cloud/fog-based, service oriented, microservices, restful, and publish-subscribe architectures. One or more of these styles can be used to design an architecture (as not all of them all mutually exclusive), being the layered approach the more leveraged design pattern [NG-IoT-8]. In this approach, the inherent functions of each layer are clearly delimited, covering only a subset of the required IoT functionalities or processes [NG-IoT-9]. Three-layer architectures define the main idea of IoT: a perception layer, which includes the sensors in charge of gathering different parameters of the environment; a network layer, responsible to transmit and connect to other things; and an application layer, responsible of serving specific services to the user. Still, IoT can be much more complex, and hence additional layers are needed in this architectural style [NG-IoT-10]. The number and naming of layers vary greatly among designs, encountering four-, five-, six- and seven-layer approaches [NG-IoT-11], or even higher (for instance, LSP RA consists of eight layers [NG-IoT-12]). In [NG-IoT-9], the authors present a general evolution of -mostly - layered IoT architectures from 2008 to 2018. As a result of their analysis, they confirm the evolution addressing aspects such as scalability, security, and interoperability, but they also note the lack of privacy preservation in IoT. Cloud-based architectures are also quite common, and it is not unusual to find architectures that follow this and the layered style since many of the styles are not mutually exclusive. On the other hand, the

<sup>4</sup> <https://www.itu.int/en/ITU-T/techwatch/Pages/tactile-internet.aspx>



IoT distribution patterns (related to edge intelligence) can be classified in centralised, collaborative, connected intranets and distributed. In [NG-IoT-8] concluded that most architectures are centralised and, most importantly, that only a few follow distributed patterns.

Both RA and IoT architectures, regardless of the architectural style and distribution selects, must address a set of question such as (i) which are the functional elements, (ii) how they interact, (iii) how is the information managed, (iv) what are the operational features, (v) and how is the system deployed [NG-IoT-13]. To answer these questions, architects make use of the concepts of views, viewpoints and perspectives, originally presented in 1977 [NG-IoT-14] and recently formalised in [NG-IoT-15].

Views, viewpoints, and perspectives can be defined as:

- **Architecture view** is a representation of one or more structural aspects of an architecture that illustrates how the architecture addresses one or more concerns held by one or more of its stakeholders [NG-IoT-16].
- **Architecture viewpoint** is a collection of patterns, templates, and conventions for constructing one type of view. It defines the stakeholders whose concerns are reflected in the viewpoint and the guidelines, principles, and template models for constructing its views [NG-IoT-17]. It is not uncommon to see references which make use of the terms view and viewpoint synonymously.
- **Architectural perspective** is a collection of activities, checklists, tactics and guidelines to guide the process of ensuring that a system exhibits a particular set of closely related quality properties that require consideration across a number of the system's architectural views [NG-IoT-16]. In many RAs, perspectives are addressed/name such as cross-cutting concerns.

The previous definitions must be extended with the following ones [NG-IoT-17]:

- **Stakeholder.** Individuals, groups, and organizations with some architectural interest in the system.
- **Concerns.** Topic of interest to one or more stakeholders pertaining to the architecture.

The first main IoT conference in Europe was held in 2008<sup>5</sup>, and according to Cisco<sup>6</sup> that was the year in which IoT was born (i.e., more connected devices than people). The first IoT architectures appeared around that year, however, the first main initiative to provide a reference architecture IoT came with the IoT-A European project<sup>7</sup>. One of its main objectives was to provide a wide reference for implementing compliant architectures tailored to different kinds of needs. Rather than following an organisation based on layers, the IoT-A Reference Architecture has a modular structure of *Functional Groups* (FG) with a set of components. According to its last release [NG-IoT-18], these groups can be summarised as follows: (i) the IoT Process Management FG aims at providing the needed interfaces to augment traditional business processes with the IoT paradigm (i.e., integration of external management systems); (ii) the Service Organisation FG acts as a communication hub between other FGs, used for composing and orchestrating services with different abstraction levels; (iii) the Virtual Entity FG serves as a virtualisation mechanism that offers a layer of abstraction of data and IoT services, enabling uniform manipulation of the managed data; (iv) the IoT Service FG contains not just the IoT services but the functionalities related to their discovery, look-up and name resolution; (v) the Communication FG provides a level of abstraction for the IoT services FG, acting as a gateway to the connected devices by modelling the variety of interaction schemes of the IoT protocols and networks; (vi) the Security FG targets transversal security functionalities related to authorisation, authentication, identity management, trust, etc.; the (vii) Management FG, also transversal to the other FGs, is in charge of some FCAPS functionalities [NG-IoT-19] like fault, configuration and performance as well as reporting and monitoring tasks. Device and Application layers are outside of the scope of this reference architecture.

<sup>5</sup> <https://iot-conference.org/iot2008/>

<sup>6</sup> [https://www.cisco.com/c/dam/en\\_us/about/ac79/docs/innov/IoT\\_IBSG\\_0411FINAL.pdf](https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf)

<sup>7</sup> <https://cordis.europa.eu/project/id/257521>

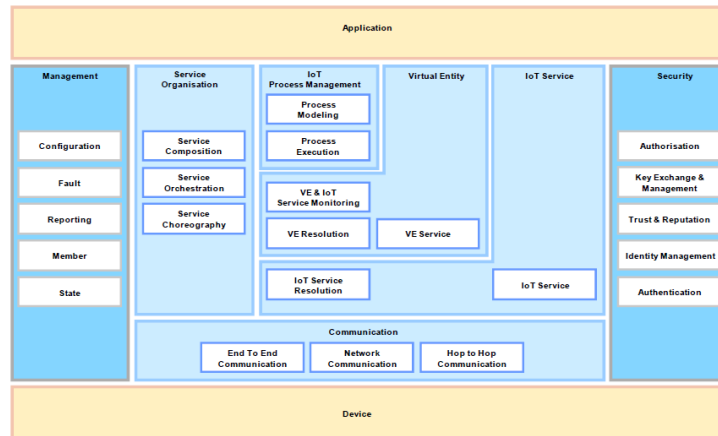


Figure 1. Functional-decomposition viewpoint of the IoT-A reference architecture. Source: IoT-A D1.5 [NG-IoT-18].

Many of the RAs that appeared later followed the ISO/IEC/IEEE standard [NG-IoT-15] of 2011, which not only harmonizes the terms of architecture, architecture framework, views, viewpoints, and perspectives, but also outlines the requirements regarding a system, software, and enterprise level architecture. One of the first ones that applied this standard was the Smart Grid Architecture Model (SGAM) [NG-IoT-20], a RA presented by CEN, CENELEC and ETSI on Smart Grids for solving interoperability issues among systems at different levels. It leverages significant existing material like the NIST Conceptual Model [NG-IoT-21], the GridWise Architecture Council Stack interoperability categories and architecture standards such as TOGAF and Archimate. The architecture was composed of five interoperability layers (Component, Communication, Information, Function and Business layers), five domains (which reflect the physical viewpoint of the electrical delivery process, from the generation of power, to its transmission, distribution, energy resources and customer premises) and six zones (corresponding to the hierarchy of the management of the process), in a 3D representation as can be seen in Figure 2.

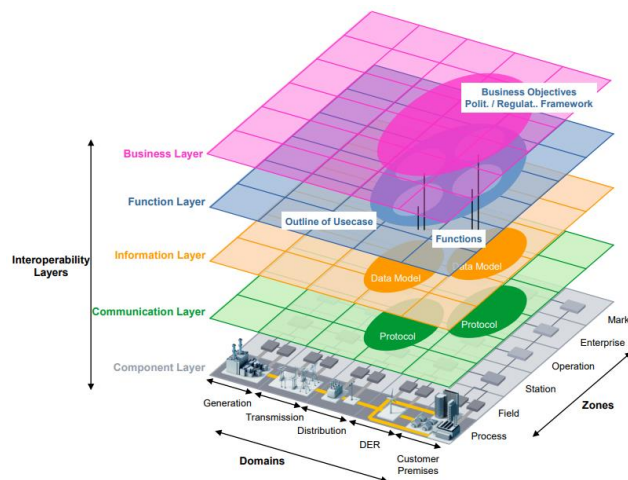


Figure 2. SGAM structure [NG-IoT-20].

The Industrial Internet Consortium (IIC) proposed a RA focused on Industrial IoT (IIoT) in 2015. The Industrial Internet Reference Architecture (IIRA), which also follows the aforementioned ISO/IEC/IEEE standard, has the purpose of providing a guideline and assistance in the development, documentation, communication and deployment of IIoT systems [NG-IoT-4], aiming at defining the constituent components and interfaces needed for developing end-to-end architectures for the industrial internet ecosystem. According to its latest version (i.e., v1.9) and focusing on its functional view, they decompose a typical IIoT into five domains, supported by specific system characteristics and cross-cutting functions that have to be available throughout the functional components. The domains are: (i) Control domain, which are functions performed by industrial assets or control systems executing fine-grained closed-loops, involving reading data from sensors, applying rules and logic, and exercising control over the physical system through actuators; (ii) Operations Domain, in charge of management and maintenance of the Control Domain to ensure its continuous operation, including health monitoring, configuration, update and diagnosis; (iii) Information Domain, which manages and processes data, including

persisting, modelling and analysing the data to acquire high-level intelligence about the overall system; (iv) Application Domain, which implements use-case specific logic, rules and models at a coarse-grained high level for optimisation in a global scope (including APIs and user interfaces); and (v) Business Domain, which support business processes and procedural activities functions (like CRM, ERP, MES) that an IIoT system must integrate to enable end-to-end operations of IIoT systems (similar to the IoT Process Management FG of IoT-A RA). The defined system characteristics can involve Safety, Security, Resilience, Reliability, Privacy and Scalability, whereas the crosscutting function include concerns related to Connectivity, Distributed Data Management, Analytics and Intelligent and Resilient Control. These two axes can be extended with additional system properties and other functions.

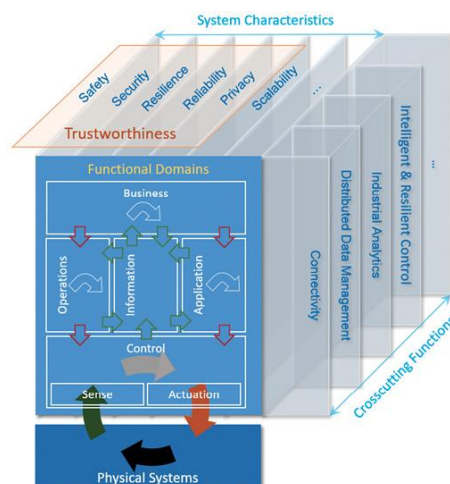


Figure 3. IIRA functional domains and system characteristics [NG-IoT-4].

The German organisation i4.0 proposed also in 2015 the first version of the Reference Architectural Model Industry 4.0 (RAMI 4.0), which in contrast with the previous ones has become an international pre-standard (IEC PAS 63088). It defines a Service-Oriented Architecture for Industry 4.0 use cases, depicted as a three-dimensional model to represent the Industry 4.0 ecosystem [NG-IoT-22]. The first dimension corresponds to *layers* (Asset, Integration, Communication, Information, Functional and Business), which describe the system structure and its properties with their functions and function-specific data. These layers can be almost directly mapped to IIRA domains and cross-cutting functions, with the exception of Assets, which can be mapped to IIRA's - not formally defined - physical systems. Besides, *Life Cycle and Value Stream* dimension is defined to track a particular product from the first idea at development stages to the maintenance of an instantiation of that product (identifier, meta data, certificates, instance identification, etc.), while *hierarchies* describe the breakdown structure of assembled components, from a product to the connected world, as it can be seen in Figure 4. This RA is focused on manufacturing (i.e., making things), whereas IIRA addresses cross-industry commonality and interoperability (i.e., making things work).

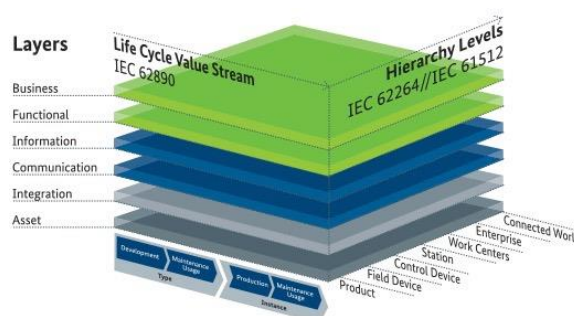


Figure 4. Reference architectural model Industry 4.0 (RAMI 4.0) [NG-IoT-22].

While IIRA and RAMI are the two most leveraged references for developing architectures for IoT, they are focused on the industrial domain, especially RAMI 4.0 (very coupled to manufacturing processes). The CREATE-IoT project of the IoT European Large-Scale Pilots (LSP) programme came up in 2018 with a domain-agnostic 3D IoT Reference Architecture. Since many of the involved projects proposed RAs that shared a lot of commonalities, they were combined to present the LSP IoT 3D architecture [NG-IoT-12] which is based



on layers, cross-cutting functions and non-functional properties, thus having a similar structure as IIRA. In this RA, the Physical layer is composed of devices for collecting data and to perform actuating decisions (hardware and also needed software). The Network Communication Layer defines technologies and protocols to transport data, including gateways. The Processing Layer, which includes edge computing capabilities for analysing data streams, is in this RA separated from the Storage Layer, which can be either centralised or decentralised for long term analysis. The Abstraction Layer covers data semantic features, to create higher level models of real world. The three upper layers have a similar function as some of the upper modules/layers of previously mentioned RAs, aimed at developing and orchestrating IoT services and applications, tools for advanced visualisation, analytics, and reporting, as well as integration with existing business-level solutions and third-party systems.

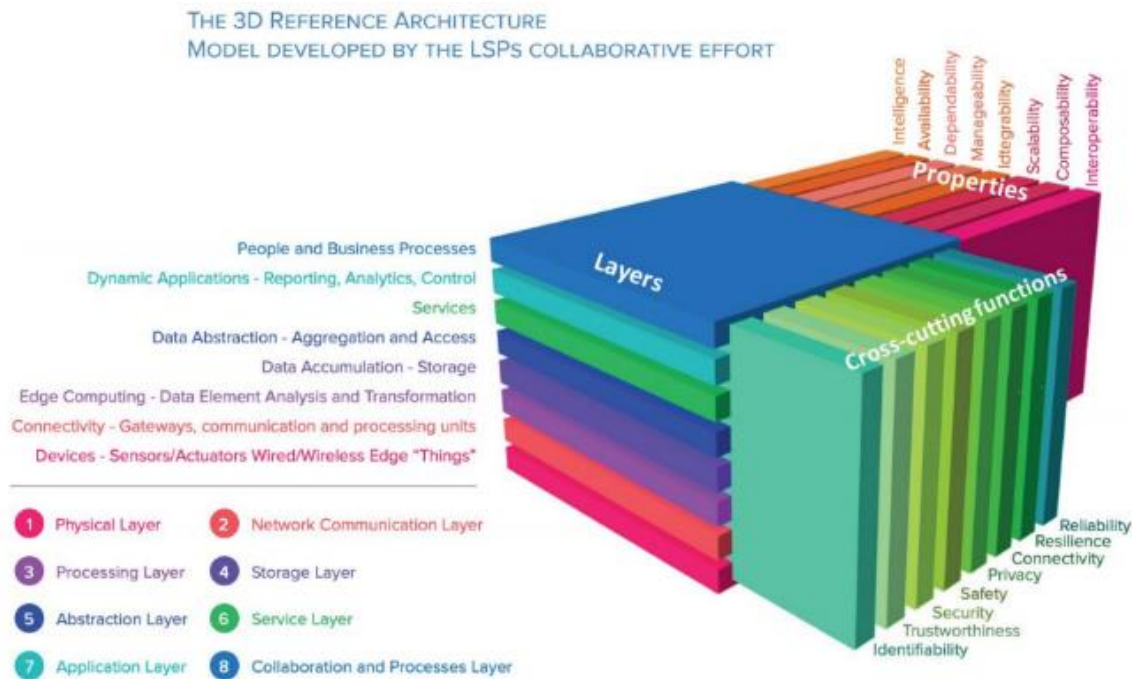


Figure 5. LSP IoT 3D reference architecture [NG-IoT-23].

As one can observe, Edge Computing capabilities are addressed in a dedicated layer, showing the importance that this enabler has been gaining recently in IoT. In fact, similar layers will be shown in the following RAs, without meaning in any case that these capabilities cannot be addressed in other layers of previous RAs. Two Consortia, the OpenFog Consortium (public-private ecosystem, founded by ARM, Cisco, Dell, Intel, Microsoft and Princeton University Edge Computing Laboratory and with more than 750 members including system integrators, industrial suppliers and academia, now part of the IIC), and the European Edge Computing Consortium (EECC), an industry-driven initiative with key industrial partners such as players like ARM, Huawei, Intel or National Instruments), have also presented their own RAs for driving the adoption of Edge Computing paradigm in IoT. Released by the OpenFog Consortium in 2017, the OpenFog Reference Architecture [NG-IoT-24] follows the aforementioned ISO/IEC/IEEE standard and promotes the adoption of fog computing to improve different communication aspects (bandwidth, latency, etc.) of IoT, AI and robotics.

The abstract architecture, presented in the next figure, includes in a single representation both (i) the Perspectives (i.e., analogous to cross-cutting concerns), which are represented as vertical grey bars and include aspects such as performance (e.g., latency), security, manageability, data analytics and control and interoperability with other IT businesses and cross fog applications; (ii) the views, including their related layers, consisting of the node view (including the sensors, actuators as well as the protocol abstraction layer), the system view (the middle layers related to platform hardware, network, security and virtualisation) and the software view (which include the upper three layers, Application Services, Application Support and Node Management). In 2019, this Consortium was absorbed by the IIC, opening the possibility of a new integrated architecture from the outcomes of this RA and IIRA.

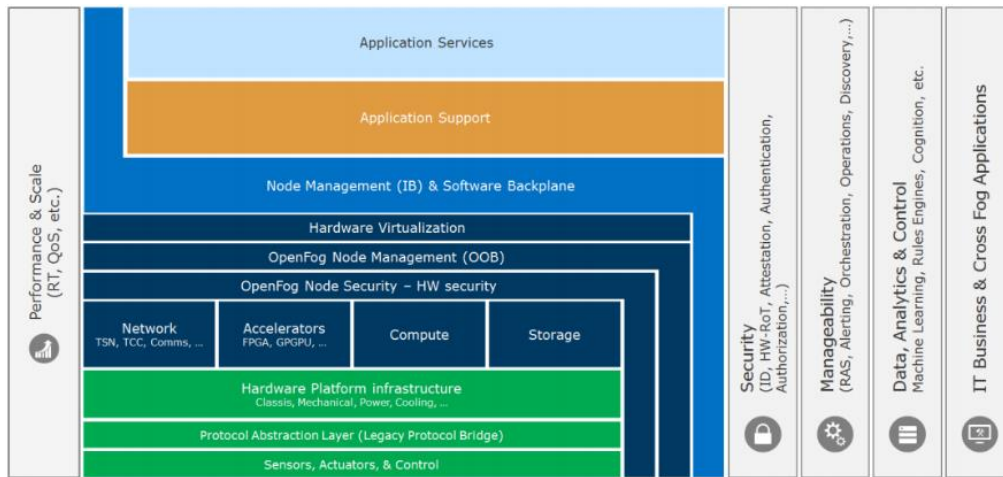


Figure 6. OpenFog Reference Architecture [NG-IoT-24].

On the other hand, the Reference Architecture Model Edge Computing (RAMEC) was presented by EECC in 2019 aiming at accelerating the adoption of software-based, interoperable, programmable, secure, and easy to use industrial ICT infrastructures. It consists of a 3D matrix consisting of concerns, layers and hierarchy levels [NG-IoT-25]. The latter depict the broad continuum in which Edge Computing functionalities can be located, which depends on applications specific requirements (in a product, in an actuator, in a gateway, at network nodes, within a private cloud, etc.). Besides, multiple technological layers are considered in this paradigm, from connectivity (Ethernet/IP, TSN, 5G, etc.) to middleware (which includes among other developments, the data transport protocol stack), information (e.g., data models, semantics) and applications. The concerns are related to requirements that expand across all layers, such as security, latency needs, AI acceleration (like TPU, GPU, FPGA), virtualisation and management features. Still, RAMEC is not considered purely a technical system architecture, but rather an orientation guide for a multi-dimensional problem space, similarly to SGAM and RAMI4.0.

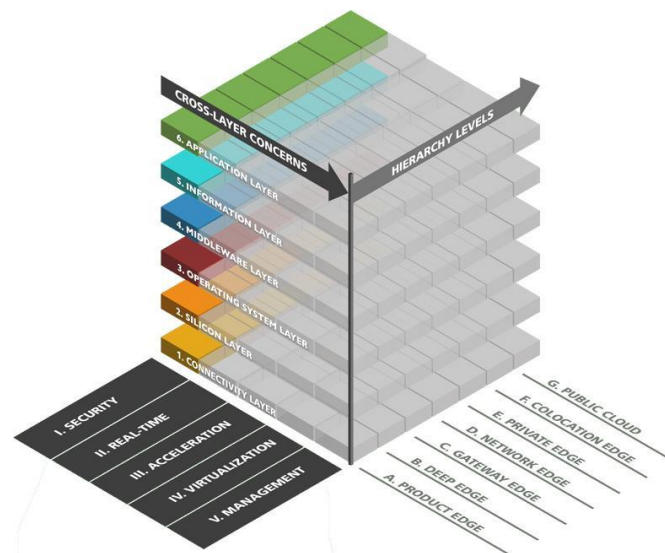


Figure 7. Reference Architecture Model Edge Computing (RAMEC) [NG-IoT-25].

The presented ones are some of the most relevant RAs currently available and show the evolution trends of these solutions. To date, most IoT RAs do not directly address many of the NGI enablers for IoT. However, it can be observed in LSP RA, OpenFog RA and RAMEC that Edge Computing has been gaining space in them even in the form of new layers, and in addition the latter addresses many other NGI enablers, such as 5G (and the promising TSN set of standards) in the connectivity layer, and both virtualisation and real-time concerns (that can be related to AR and tactile internet). Besides, some research work is already being performed towards this end, in which Next Generation IoT enablers are being introduced for proposing novel IoT architectures. For instance, SerIoT is a European project that has developed a RA mostly focused on security aspects for current IoT systems [NG-IoT-26], leveraging traditional solutions such as Honeypots as well as novel enablers like

cognitive routing for SDN and Blockchain, among others. BlockIoTIntelligence [NG-IoT-27] also addresses Blockchain, in this case AI-driven, for decentralised (cloud/fog/edge/device) IoT systems. Authors presented a thorough analysis on current trends of these technologies for IoT. In [NG-IoT-28], an architecture called AI4SAFE-IoT is presented, composed by three layers (edge/network/application) and powering security features for the edge level through AI. Besides, a novel IoT architecture based on 5G and next generation technologies has been presented in [NG-IoT-29], consisting of eight layers: Physical Devices, Connectivity and D2D communication (both supported by 5G), Edge/Fog Computing, Data Storage, Management Services (including Data Analytics, Cloud Computing and Network Management), Application, Collaboration and Processes (similar to previous Business layers), and a transversal Security layer. Despite being quite generic, it does not address any kind of Distributed Ledger Technology nor Tactile Internet.

### 3.1.1.2 Relevant initiatives and solutions

Apart from ASSIST-IoT, there are other ongoing European projects such as TERMINET<sup>8</sup>, IntellIoT<sup>9</sup> and IoT-NGIN<sup>10</sup> whose objectives include the development of novel Reference Architectures for Next Generation Internet of Things, considering the aforementioned enablers. All these projects will continue and adapt the effort that has been performed so far and for this reason the solutions developed until now, as well as the standards and guidelines that followed, must be studied. In some cases new versions of existing RAs are being released over time, especially if they are from Standards Developing Organisations (SDOs), addressing NGI or other novel aspects. Still, in order to keep coherence over time, layers (or analogous blocks) are not usually changed, and they are addressed adding or modifying existing internal components and interfaces.

In this section are listed and briefly described the most relevant initiatives that have provided Reference Architectures for IoT during the past decade. Three separate tables are presented: (i) RAs provided from Research Projects, which usually are more innovative and integrate first novel technologies and concepts; (ii) RAs developed by SDOs as well as private and public/private consortiums, which are usually more formal than the previous ones (especially those from SDOs) and generally address more stable and reliable solutions; and (iii) RAs presented by industrial providers, which apart from rely on stable technologies tend to include their particular solutions. Tables include the release date of the RAs, the domain (i.e., either IoT generic, industrial, or specific for a use case or vertical) and some comments and hints regarding their functional viewpoints. Regarding the initiatives from European projects, only the most recent relevant actions are listed (with the exception of IoT-A, the most relevant one), since in general they are discontinued once the project finishes.

*Table 1. Relevant IoT Reference Architectures from funded research projects.*

Reference architecture	Domain and Year	Comments
IoT-A [NG-IoT-18]	Generic 2011 (v1.0), 2013 (v3.0)	The IoT-A provides a set of best practices, guidelines, and a starting point to generate specific IoT architectures. Its functional viewpoint follows a modular structure of <i>Functional Groups</i> with a set of components: IoT Process Management, Service Organisation, Virtual Entity, IoT Service, Communication, and two transversals to the others, namely Security and Management. Device and Application levels are outside of the scope of this RA.
FAR-EDGE RA [NG-IoT-30]	Industrial - Factory Automation 2017	This RA is influenced by IIRA, RAMI, OpenFog RA and the ISO/IEC/IEEE 42010:2011 standard. It considers three high-level <i>Functional Domains</i> for factory automation, namely Automation, Analytics and Simulation, and four <i>Crosscutting Functions</i> , Management, Security, Digital Models and Field Abstraction & Data Routing. It also presents the concept of <i>tiers</i> , consisting in a detailed and technical-oriented classification of deployment concerns: Field (which includes edge nodes -connected devices and smart objects - as well as things, people and environments), Edge, Ledger and Cloud (Services and Applications).
LSP 3D RA [NG-IoT-12]	Generic 2018	Resulting from the analysis of the commonalities of the RAs of the LSP projects, it is a layer-based model of eight <i>layers</i> (Physical Network Communication, Processing, Storage, Abstraction, Services, Dynamic Applications and People

<sup>8</sup> <https://terminet-h2020.eu/>

<sup>9</sup> <https://cordis.europa.eu/project/id/957218/es>

<sup>10</sup> <https://iot-ngin.eu/>

Reference architecture	Domain and Year	Comments
		and Business), <i>cross-cutting functions</i> (Security, Safety, Resilience, Privacy, Connectivity, Reliability, Trustworthiness and Identifiability) and <i>non-functional properties</i> of the system, which may be present depending on the implementation of the previous layers and functions (Intelligence, Availability, Dependability, Manageability, Integrability, Scalability, Composability and Interoperability).
MANTIS [NG-IoT-31]	Industrial - Proactive Maintenance 2018	It is founded on the ISO 13374 standard [NG-IoT-32], IoT-A and IIRA. It consists of six <i>Functional Domains</i> (Application, Maintenance, Communication, Device, Management, and Security, being the two latter transversal to the others). These domains are in turn composed of Functional Components, which result from the extension of the ISO 13374 functional elements with maintenance planning and execution, combined with typical functions of CPS and IoT systems taken from the IoT-A reference model. Different types of maintenance applications can be built: Reactive, Proactive, Predictive and Adaptive.
SynchroniCity [NG-IoT-33]	Smart City 2019	This project presents a RA as a result of real implementations in European cities. It is composed of different horizontal layers named <i>Logical Modules</i> , including Data Sources/Devices, Southbound Uniform Interfaces, Context Data Management, IoT Management (which is a module represented in parallel to the former), Data Storage Management, Marketplace and Asset Management and Northbound Uniform Interfaces. The Logical Modules are supported by two <i>vertical layers</i> , Monitoring and Platform Management Services, and Security, Privacy and Governance.
QU4LITY RA [NG-IoT-34]	Industrial - Manufacture 2019	This project provides a RA for Zero Defect Manufacturing (ZDM) in Industry 4.0, leveraging Cyber Physical Systems and advanced digital technologies (e.g. Big Data, Edge/Fog Computing, Artificial Intelligence). It is based on RAMI4.0 and the RAs from the IIC (IIRA and OpenFog). This RA is composed of stacked <i>Tiers</i> (Field, Line, Factory and Ecosystem), with one Digital Infrastructure that provides common services like connectivity and distributed processing. It considers three <i>Functional Domains</i> orthogonal to Tiers (Adaptive Digital Shopfloor Automation, Multiscale ZDM Processes and User-Centric ZDM), as well as <i>Cross-cutting Functions</i> (Security, Digital Infrastructures and Digital Models).

Among other RAs that could have been mentioned, one can found ESPRESSO [NG-IoT-35], intended for Smart Cities environments; FIESTA-IoT, compliant with IoT-A, for enabling federated semantic interoperability; SerIoT [NG-IoT-26], built upon the ISO/IEC 30141 IoT RA (briefly presented in the next table) to develop security and privacy aspects (to recognize suspicious patterns, to detect security leaks and privacy threats while offering background mitigation actions); DEMETER [NG-IoT-36], which is based on the architecture model introduced by the Industrial Data Space (IDS [NG-IoT-37]) for supporting fluid data exchange across the entire agri-food chain; and OPEN DEI [NG-IoT-38] and BIG IoT [NG-IoT-39], which in contrast to the former provide generic RAs for data exchange among IoT either to enable cross-platform and cross-domain application developments or to monetise IoT resources and foster collaboration among the stakeholders. Studying these RAs is useful for both following a methodology for developing our RA on top of existing solutions as well as for implementing specific components or modules to address particular technologies or concerns such as security or interoperability.

In the next table, the RAs provided by some representative SDOs (ISO, IEC, IEEE, ITU, ETSI) are briefly presented, sometimes being a result of a joint effort. As one can see from the previous table, with the exception of IoT-A, projects tend to leverage one or many of the RAs, models, guidelines, and recommendations provided by SDOs to develop their own on top of them rather than starting from scratch, considering as well different existing standards to develop it, mainly ISO/IEC/IEEE 42010:2011, as well as other standards to specify required interfaces. Depending on the level of abstraction of an RA, different standards can be integrated for its development. For instance, RAMI 4.0 was based on a significant number of them<sup>11</sup>, from standards related to communications (e.g., IEC 61784) to life-cycle management for the systems and products (e.g., IEC 62890).

<sup>11</sup> <http://i40.semantic-interoperability.org/>



Not only SDOs but also consortiums provide their own RAs, sometimes aiming at boosting a particular technology (for instance, RAMEC for Edge Computing), or to facilitate the development of solutions for specific domains (e.g., IIRA for industry).

*Table 2. Relevant IoT Reference Architectures from public-private/private consortiums and SDOs.*

Reference architecture	Domain and Year	Comments
ITU-T Y.2060 [NG-IoT-43]	Generic 2012	Through this recommendation, ITU-T clarifies the concept and scope IoT, identifies the fundamental characteristics, high-level requirements and provides their Reference Model for IoT. It consists of <i>four layers</i> (Application, Service Support and Application Support, Network and Device) as well as Management and Security <i>capabilities</i> associated with the four layers.
AIOTI HLA [NG-IoT-40]	Generic 2015 (v.1.0), 2018 (v.4.0)	The functional model of the High-Level Architecture presented consists of three <i>layers</i> , namely Application, IoT and Network. It is based on ISO/IEC/IEEE 42010 and has evolved along releases, addressing concerns such as privacy, virtualisation, Big Data and AI in IoT, and systems' autonomy in the components of the layers rather than as addition of them. Security and management are also considered, but <i>intrinsic to interface specifications instead of represented as cross-cutting layers</i> .
IIC IIRA [NG-IoT-4]	Industrial 2015 (v1.7), 2019 (v1.9)	From the Industrial Internet Consortium, this RA is one of the most relevant ones and consists of a 3D model of five <i>domains</i> (Control, Operations, Information, Application and Business) supported by specific <i>system characteristics</i> (Safety, Security, Resilience, Reliability, Privacy and Scalability) and <i>cross-cutting functions</i> (Connectivity, Distributed Data Management, Analytics and Intelligent and Resilient Control).
RAMI 4.0 [NG-IoT-22]	Industrial - Manufactory 2015	Three-dimensional model to represent the Industry 4.0 space, aiming at providing a common understanding to all the involved stakeholders. The first dimension of its RA corresponds to <i>Layers</i> , describing the system structure, its properties, functions, and data (Asset, Integration, Communication, Information, Functional and Business); the second one is related to <i>Life Cycle and Value Stream</i> (IEC 62890); and the last dimension considers <i>Hierarchies</i> (IEC 62264 and IEC 61512), which describe the breakdown structure of assembled components, from a product to the connected world.
OneM2M [NG-IoT-41]	Generic 2015 (v.1.0), 2019 (v. 4.0)	This global organisation is formed by ICT standard bodies as well as around 200 members from different sectors. Being one of the main references for IoT, it is developing specifications for the service layer for machine-to-machine communication and the IoT. It provides a three-layer architecture model, each of them with a logical entity: Application Layer, Common Services Layer and Network Services Layer, all them communicating through reference interface points. It allows building systems together with other platforms, enabling multi-platform interoperability. They provide a framework for supporting applications and services for smart grid, connected car, home automation, public safety, and health use cases.
ECC RA 2.0 [NG-IoT-42]	Generic - Edge centric 2017	Proposed by the Edge Computing Consortium and the Alliance of Industrial Internet, it consists of four main horizontal layers, including Edge Computing Node (which internally is composed of Resources Layer, Virtualisation Layer and Edge Virtualisation Functions), Connectivity and Computing Fabric, Service Fabric and Smart Service. Vertically, the architecture uses Management Services, Lifecycle Data Services and Security Services to deliver smart services in the entire services process and lifecycle. It is guided by standards defined by ISO/IEC/IEEE 42010:2011.
OpenFog RA [NG-IoT-24]	Generic -Edge centric 2017	Guided by ISO/IEC/IEEE 42010:2011, this architecture is composed by <i>Views</i> and <i>Perspectives</i> . The Views include Node (which integrates sensors, actuators, and protocol abstraction layers), System (layers related to platform hardware, network, security, and virtualisation) and Software (which include Application Services, Application Support and Node Management layers). The Perspectives, equivalent to cross-cutting functions, include aspects like Performance, Security, Manageability, Data Analytics and Control, and Interoperability.
ISO/IEC 30141 IoT RA [NG-IoT-44]	Generic 2018	This standard provides a RA using a common vocabulary, reusable designs, and industry best practices for IoT. Following a top-down approach, it consists of six <i>domain functions</i> and six <i>cross-domain capabilities</i> . The domains include Physical

Reference architecture	Domain and Year	Comments
		Entity, Sensing and Controlling, Access and Communication, Operations and Management (OSS/BSS), Application and Service (APIs, Portal, analytics, etc.) and User Domain (interfaces). The capabilities aim at providing trustworthiness, hence including Connectivity, Security, Resilience, Dynamic Composition, Interoperability, and Personally Identifiable Information (PII).
RAMEC [NG-IoT-25]	Generic - Edge centric 2019	Present a RA in the form of a 3D matrix consisting of <i>concerns</i> , <i>layers</i> , and <i>hierarchy levels</i> . The latter depict the broad continuum in which Edge Computing functionalities can be located. Multiple technological layers are considered: Connectivity, Silicon, Operating System, Middleware (which includes data transport protocol stack), Information (data models, semantics, etc.) and Applications. The concerns expand across all layers, like Security, Real Time, Acceleration, Virtualisation and Management.

The number of available RAs of this kind is quite large and hence only the most relevant for the project have been listed. Other architectures that could have been mentioned are the ones presented by BDVA [NG-IoT-45] and ISO BDRA [NG-IoT-46], more devoted to Big Data; ETSI M2M [NG-IoT-47], which is intended for machine-to-machine communications that make use of an IP capable underlying network including the IP network provided by 3GPP (hence, less generic) and has been superseded by OneM2M specification; or IDS Reference Architecture Model [NG-IoT-37], from IDSA for data exchange among IoT platforms. The RA of ASSIST-IoT will be two-dimensional, consisting of four horizontal Planes (Device and Edge, Smart Network and Control, Data, and Application and Services) and five vertical Capabilities (Self\*, Interoperability, Scalability, Manageability, and Security, Privacy and Trust). It will be formalised considering not only current initiatives from SDOs, both generic and industrials, but also aiming at leveraging novel components, interfaces and/or approaches proposed either within the project or from both European funded projects and private initiatives like the aforementioned ones.

Finally, private providers have also proposed their architectures for IoT. In general, these kinds of RAs tend to relate the components of each level/layer to the specific solutions that these companies offer. Still, among them one can find the Cisco reference model, which is quite abstract and not related to any specific solution.

*Table 3. Relevant IoT Reference Architectures from private industrial providers.*

Reference architecture	Domain and Year	Comments
Cisco IoT World Forum RA [NG-IoT-48]	Generic 2014	The proposed IoT reference model is comprised of seven <i>levels</i> : Physical devices and Controllers, Connectivity, Edge/Fog Computing, Data Accumulation (e.g., storage), Data Abstraction (e.g., aggregation and access, Application, and Collaboration and Processes). The model describes how tasks at each level should be handled to keep simplicity, enable high scalability, and ensure supportability. Finally, the model defines the functions required for an IoT system to be complete.
Intel IoT RA [NG-IoT-49]	Generic 2015	Intel proposes a modular solution, facilitating the reuse of containers, virtual machines and NFV while allowing SDN support. It consists of six horizontal <i>layers</i> , namely Communications and Connectivity, Data, Management, Control, Application and Business, as well as two vertical ones, Security and Developer Enablers (APIs, SDKs, Dev Tools). Apart from specifying the needed interfaces among components, they propose a set of existing solutions for composing a real implementation. In 2018, they proposed jointly with SAP an edge-centric RA for IoT [NG-IoT-50], specifying a set of components in three different groups, Edge Endpoint, Edge Gateway and Cloud.
WSO2 [NG-IoT-51]	Generic 2015	Follows a classical layered approach, with five <i>layers</i> (device, communication, aggregation/bus, event processing and analytics, and client/external communication layers) and two <i>cross-cutting</i> ones (namely device manager, and identity and management layers). They map their proposal to WSO2 components for further instantiations.
Microsoft Azure IoT RA [NG-IoT-52]	Generic 2016 (v.1.0), 2018 (v.2.1)	They recommend a cloud native, microservices and serverless based architecture for IoT, presenting a set of subsystems that communicate over REST/HTTPS using JSON. The <i>core subsystems</i> are Devices (and/or on-premise edge gateways), Cloud Gateway Service (or Hub), Stream Processors (that consume that data, integrate with business processes, and place the data into storage) and a User Interface. These subsystems

		could be expanded with Intelligent Edge Systems, Data Transformation, Machine Learning and User Management functions. Regarding <i>cross-cutting needs</i> , their RA addresses Security, Deployment aspects and High Availability and Disaster Recover.
--	--	--

### 3.1.2 Hyperconnectivity

Hyperconnectivity is a term first time used in 2005 by Anabel Quan-Haase and Barry Wellman [HYP-1]. Hyperconnectivity means everything is connected: person to person, person to machine and machine to machine. In a hyperconnected world, Next Generation IoT implementation is needed to enable every device to detect its environment, to transmit information, to provide feedback, or to trigger an action. Sensors and devices used in Next Generation IoT systems need to increase their productivity and incorporate continuous improvement tools, and hyperconnectivity is needed to achieve a higher level of connectivity between them. The future networks will become intelligent platform infrastructures that will provide multiple functionalities enabled by edge node, Software-Defined Networking (SDN)/Network Function Virtualisation (NFV) components, Artificial Intelligence (AI) modules, self-\* components, and Distributed Ledger Technology (DLT), among others. As the network grows in heterogeneity and complexity, virtualization plays an important role in improving resource efficiency and increasing service reliability and security. To assist in hyperconnectivity deployment, new infrastructure based on programmable and virtualised networks is being developed nowadays.

“Programmable networks” has been proposed as a way to facilitate network evolution. It is a new networking paradigm that decouples hardware and control decisions and simplifies network management by centralising intelligence and implementing network devices as simple packet forwarding devices. The idea of programmable networks and decoupled control logic starts the context of early programmable networking efforts [HYP-2].

#### Historical perspective of different programmable networks instances

In 1995, the Open Signaling movement began working toward making Asynchronous Transfer Mode (ATM), Internet and mobile networks more open, extensible, and programmable by proposing separated control and data signalling programmable interfaces. In this scenario, the communication between hardware and control software was necessary but challenging due to vertically integrated switches and routers. With the same goal, Devolved Control of ATM Networks (DCAN) in the mid-1990s was developed to design the infrastructure for scalable control and management of ATM networks [HYP-3]. Besides, Active Networking proposed a new data plane programmability paradigm [HYP-4], with the idea that each node had the capability to perform computations on packets, or modify their content.

The NetWare Core Protocol (NCP) was the first attempt to separate control and data plane signaling. NCPs were introduced by AT&T to improve the management and control of its telephone network. Similarly, other initiatives such as Forwarding and Control Element Separation (ForCES), Routing Control Platform (RCP), and Path Computation Element (PCE) proposed the separation of the control and data planes for improved management in ATM, Ethernet, Border Gateway Protocol (BGP), and Multiprotocol Label Switching (MPLS) networks, respectively [HYP-2]. In 2004, 4D project appeared to emphasize the separation between routing decision logic and the protocols governing the interaction between network elements. Afterwards, the Internet Engineering Task Force (IETF) Network Configuration Working Group proposed NETCONF as a management protocol for modifying the configuration of network devices to allow network devices to expose an Application Programming Interface (API) through which extensible configuration data could be sent and retrieved. Another management protocol, widely deployed in the past and used until today, is Simple Network Management Protocol (SNMP), which was addressed in a later version of NETCONF protocol.

Ethane was considered as the predecessor to OpenFlow. This project defined a new architecture for enterprise networks focused on using a centralized controller to manage both policy and security in a network. The similarities to SDN are mainly the controller to decide if a packet should be forwarded, and a switch consisting of a flow table and a secure channel to the controller.

#### Programmable Networks

The explosion of new heterogeneous devices and services are driving the trends in networking industry to reconsider traditional network architectures. Many conventional networks are hierarchical based client-server computing with tiers of switches arranged in a tree structure [HYP-5].

Data networks consist of a set of autonomous systems that execute Interior Gateway Protocols (IGP), used for exchanging routing information between gateways, selecting the best routes strictly obeying technical criteria. These networks are interconnected with each other thanks to Exterior Gateway Protocols (EGP), that allows the implementation of complex – but not flexible – routing policies.

The main problem faced by this methodology is the limitation of traffic, which poses severe limitations on network performance when high traffic requirements. Furthermore, current network devices lack the flexibility to deal with different packet types with various contents because of the underlying hardwired implementation of routing rules [HYP-6]. Due to this need, the evolution of networks architectures is guided to architectures where the forwarding state in the data plane is managed by a remotely controlled plane decoupled from the former, being enabled to program the behaviour of a network without being tied to inflexible rules and conditions.

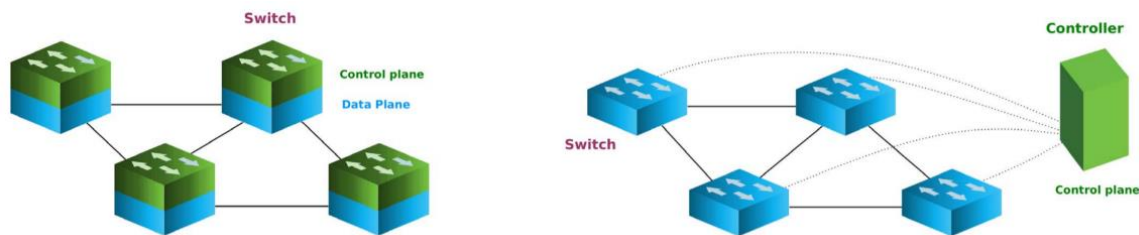


Figure 8. Programmable network concept

Initially proposed by Stanford University, and now standardized by the Open Networking Foundation (ONF), the structure of OpenFlow and the description of SDNs approach was made.

By definition, main SDN structure consists of three parts. From the bottom: data plane, control plane and application plane. The communication between the controller and data plane is able via Southbound Interface (SBI), which is located in SDN switches. The communication between applications and controllers is maintained by a Northbound Interface (NBI), located in the control plane. Controller helps applications to reach their purpose by controlling SDN switches through forwarding tables. Network adjusts itself to users' needs and, using controller and API, network managers can easily control the network automatically by adding new features to the control plane without making changes in the data plane.

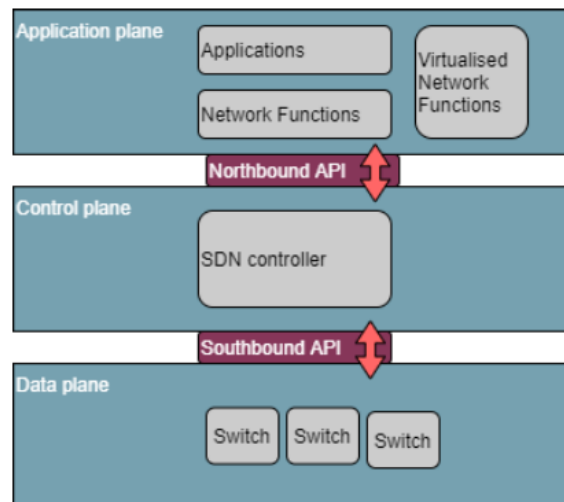


Figure 9. Main SDN structure.

### Virtualised Networks

Network virtualization also has its roots back in the 1990s with the Tempest framework, one of the first initiatives to introduce virtualization in network implementation. That was possible by introducing the concept of switchlets in ATM networks, allowing multiple of them on top of a single ATM switch. That enabled multiple independent ATM networks to share the same physical resources [HYP-7].



Since then, important advances have been made in network virtualization, trying to replace physical network equipment by specific functions in generic equipment whose function is virtualised. The first step to concept standardisation was generated in 2012, through the drafting, by the main telecommunication providers, of a technical document in which an industrial and investigative action was requested. The European Telecommunications Standards Institute (ETSI) was selected to host the Industry Specification Group for Network Function Virtualization (ETSI ISG NFV). The first ETSI documents include an overview of the infrastructure, an updated architectural framework, descriptions of the network, hypervisor and infrastructure computing domains. It also covers Management and Orchestration (MANO), security and trust, resilience, and quality of service.

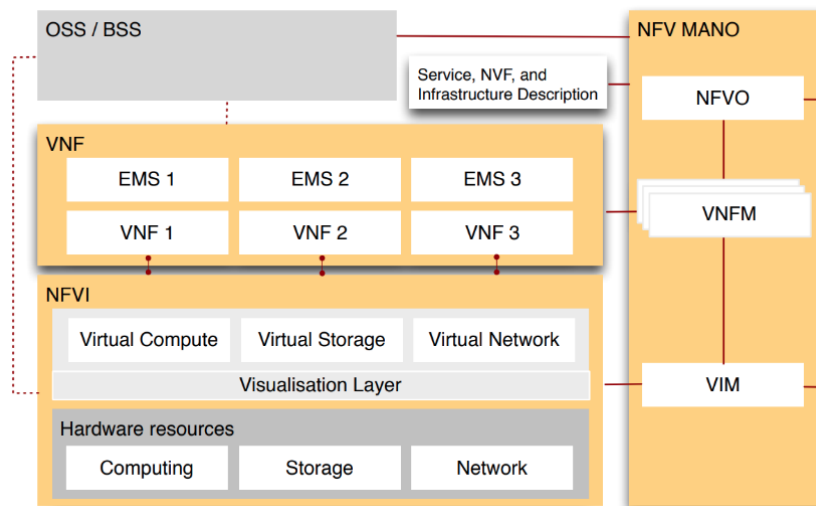


Figure 10. Main NFV architecture [HYP-7].

Every NFV system requires access to hardware computing, storage, and network resources. These resources make up the physical equipment of the NFV Infrastructure (NFVI), which is assigned via Virtualized Network Functions (VNF) in the NFVI virtualization layer, depending on the specific demands. VNFs are managed locally by the Element Management System (EMS).

The Operations Support Systems and Business Support Systems (OSS/BSS) includes legacy management systems and assists MANO in enforcing network policies. It is considered as part of the NFV framework and can act either automatically or manually.

All the hardware/virtual systems and the virtualized functions have to be managed by the NFV Management and Orchestration (NFV-MANO), that is composed of three main components: the NFV Orchestrator (NFVO), the VNF Manager (VNFM), and the Virtualised Infrastructure Manager (VIM).

- The entire NFVI is managed by the VIM component. The NFVI computation, storage, and network-related resources are assigned to the virtual resources needed by specific functions.
- The VNF access the respective resources, globally configured, and supervised by the VNFM component. The VNFM also performs the respective coordination and adaptation role for configuration and event reporting between the VIM and the EMS.
- The NFVO. Due to its highest position in the NFV-MANO hierarchy, the NFVO is responsible of connecting or combining NFVs as building blocks, managing orchestration of NFVI resources across multiple VIMs and lifecycle management of network services.

### 3.1.2.1 Scientific Review

#### 3.1.2.1.1 SDN Controller

In SDN, the network intelligence is logically centralized in software-based controllers, so network devices become simple packet-forwarding devices. To improve controllers' performance, some APIs have been developed to communicate the controller with the switches (southbound) and applications (northbound) in an SDN network.

##### Southbound

Southbound APIs facilitate control over the network and enable the controller to dynamically make changes. A first approach to standardization was made with Forwarding and Control Element Separation (ForCES), defining networking and data forwarding elements, and their communication specifications, without changing the essential network architecture. OpenFlow is the protocol used for managing the southbound interface of the generalized SDN architecture. It is the first standard interface defined to facilitate interaction between the control and data planes of the SDN architecture. It also provides software-based access to the flow tables that instruct switches and routers [HYP-5] [HYP-8]; lastly it is the main protocol specification but it is not the only available southbound interface for SDN [HYP-9]:

- NETCONF/YANG (Yet Another Next Generation)
- SoftRouter
- Path Computation Element Protocol
- Open vSwitch database management protocol
- Protocol Oblivious Forwarding
- OpFlex control protocol
- OpenState
- Revised OpenFlow Library
- Hardware Abstraction Layer
- Programmable Abstraction of Data path

Other solutions such as Locator ID Separation Protocol (LISP) paradigm do not program the network but rather the Mapping System. The control policies can be programmed and stored on the Mapping System; then the LISP data-plane will operate accordingly [HYP-10].

##### Northbound

Northbound APIs allow applications to dictate network behavior, abstracting network functions with a programmable interface for applications to dynamically consume network services and configure the network [HYP-9][HYP-11].

- REST API - Representational State Transfer (REST) API or an API that is RESTful (that adheres to the constraints of REST) is neither a protocol, language nor an established standard but API architectural style.
- Programming Languages provide a variety of building blocks to enable easy application and software module development. Some examples of different programming languages [HYP-8][HYP-4] are as follows:
  - Maple translates a high-level policy into sets of rules on distributed switches, providing an abstraction that runs on every packet entering a network.
  - Fault tolerating regular expressions (FatTire). It is a new language for writing fault-tolerant network programs.
  - Flow-based Management Language (FML) is a high-level declarative policy language that specifies management and security policies for OpenFlow networks, calculating and deploying flow table entries on switches.

- Procera - is a language that applies the principles of functional reactive programming to provide a declarative, expressive, and compositional framework that allows operators to express network policies based on both reactive and temporal behaviours, which are typically necessary to express common, simple network policies.
- Frenetic - language allows the programs written for one platform to work in other platforms. It eliminates complicated asynchronous and event-driven interactions between SDN applications and switching devices. Additionally, supports for designing a compiler, run-time environment, and modular programming constructs for SDN, also constructs for certain tasks such as updates.
- Other APIs. Many existing SDN Controllers define their own northbound API such that they are customized to their specific needs. Onix, MobileFlow, PANE use NVP NBAPI, SDMN API, PANE API as their Northbound APIs respectively. Two interfaces that were created earlier and require special mention are NOSIX and SFNet.

### 3.1.2.1.2 Centralized / Distributed Architecture

The intelligence in an SDN network is moved to the controller. The data layer will be distributed to favour the exchange of data between different points, although the control layer can be centralized or distributed, depending on how the controller has been developed and the use case. For cases where the control plane is physically centralized, only a single controller is needed for the entire network. While recommended for small, simple networks, it does not meet the different requirements of large-scale network deployments [HYP-12]. Hence, networks with a physically distributed control plane are defined to solve scalability, single point of failure, bottlenecks, etc.

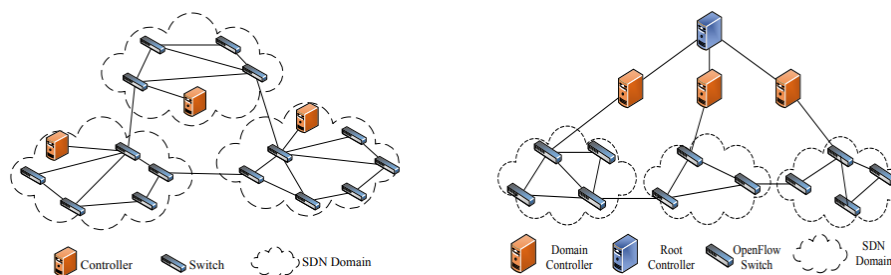


Figure 11. Single/hierarchical physically distributed architectures.

- A single controller handling horizontal slices of the network into multiple areas with a subset of SDN switches.
- A hierarchical SDN control architecture with a vertically partitioned control plane into multiple levels (layers).

Due to the limited processing capacity of a controller, single controller architectures are not suitable for large networks. Thus, several approaches address the lack of management of the distributed architecture with a single controller. In a logically centralized approach, a set of controllers collaborate to manage the network and they have the same view of the network and the same shared database. To achieve a scalable control plane for networks that are highly distributed over multiple domains, logically distributed architectures are proposed. In this approach, each domain is managed by its controller and can share only some useful information with the other controllers to achieve some services such as the topology view.

### Eastbound / Westbound APIs

To manage the control of large-scale networks, an interface protocol that manages the interactions between the different controllers is needed. The east and west APIs allow controllers to communicate with each other and to be synchronized for greater availability in order to control large-scale networks. They use a notification and message system or a distribution protocol similar to the BGP (Border Gateway Protocol) or OSPF (Open Shortest Path First). The controllers cooperate and pass messages with each other and share the resources logically. The system can read the information from each controller, monitor the exchanged messages by analysing the complete state of the network, and then determine the packet forwarding actions on the switches. [HYP-13] [HYP-14].

### 3.1.2.1.3 Network Function Virtualization

NFV systems use virtual machines to run different processes and software on network servers, switches, storage, and even cloud computing infrastructure, so there is no need to customize the hardware for each network function. Some functions of the SDN controller can be deployed as virtual functions, meaning that the OpenFlow switches will be controlled by a VNF with SDN functions. This software network can be created by SDN, with a set of tunnels and virtual switches that prohibits sudden interactions between different virtual network functions [HYP-15] [HYP-16].

The VNFs are located on the application layer, where user applications can be executed in different operating systems sharing the same hardware resources. This virtualisation requires the coordination of the infrastructure layers. Orchestration and Management layer (NFV MANO) is responsible to ensure the availability of enough resources for the instantiation of the VNF apps. The most significant samples of VNFs that can be developed and their categorization according to the function they perform are named below [HYP-17].

*Table 4. List of VNFs by activity.*

Feature	Network functions
Switching elements	Broadband Network Gateway (BNG), Carrier Grade Network Address Translation (CG-NAT), routers.
Mobile network nodes	Home Location Register/Home Subscriber Server (HLR/HSS), Mobility Management Entity (MME), Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN)/Packet Data Network Gateway, Radio Network Controller (RNC), Node B, eNode B.
Tunnelling gateway elements	Internet Protocol Security (IPSec)/Secure Sockets Layer (SSL) Virtual Private Network (VPN) gateways.
Traffic analysis	Deep Packet Inspection (DPI), QoE measurement.
Next Generation Network signalling	Session Border Controllers, IP Multimedia Subsystem (IMS).
Converged and network-wide functions	Authentication, Authorisation, Accounting (AAA) servers, policy control and charging platforms.
Application-level optimisation	Content Delivery Networks (CDNs), Cache servers, load balancers, application accelerators.
Security functions	Firewalls, virus scanners, Intrusion Detection Systems (IDSs), spam protection.

### 3.1.2.1.4 SD-Wireless Network Architectures

IT companies and organizations are focusing on applying SDN and network virtualisation to data-centre local area networks (LANs), as well as wireless local area networks (WLANs) and wide area networks (WANs).

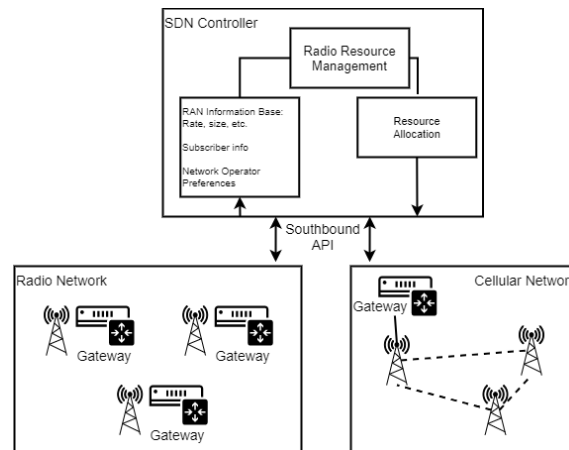
#### Cellular and radio networks

SDN can be applied for cellular and radio solutions, providing the state-of-the-art novel and diverse frameworks [HYP-18] [HYP-19]. In radio networks, a physical intervention in radio technologies is required. SDN can be applied abstracting the Radio Access Network (RAN) by a centralised control plane, while the resource allocation is enabled by a big base station. The controller allocates resources in the domain of frequency, time and space slot.

In cellular networks, the radio access networks consist of base stations that connect to unmodified User Equipments (UEs) using existing protocols for managing mobility, sessions, and authentication that are implemented at the control plane. The UE retains a single IP address as it moves between base stations in the same cellular core. Different implementations change **how the base stations communicate with the core**

**network**, by having the base stations coordinate the controller to enforce service policies. Controller applications should be able to express policy in terms of subscriber attributes, rather than IP addresses or physical locations, as captured in a subscriber information base.

- To improve control-plane scalability, each switch should run a local control agent that performs simple actions (such as polling traffic counters and comparing against a threshold), at the behest of the controller.
- Switches should support more flexible data-plane functionality, such as deep packet inspection and header compression.
- Base stations should support remote control of virtualized wireless resources to enable flexible cell management.



*Figure 12. RAN solution architecture.*

Cognitive radio is a way of offloading traffic on cellular networks with next-generation technologies. Cognitive radio can be extended to improve the spectrum utilization within new types of spectrum sharing models and acting as an enabler with new techniques such as massive Multiple Input Multiple Output (MIMO) and Ultra-dense Deployment [HYP-20] [HYP-21].

### IoT networks

Typical wireless technologies considered for IoT today range from short range and low power consumption (Bluetooth LE, 802.15.4 / Zigbee 3.0 or LP802.11), to wide area coverage (Low-Power Wide-Area Network LPWAN): LTE Cat-M1, LoRaWAN, Sigfox or NB-IoT. Access networks scale efficiently to manage resources and optimize operation. To this end, adequate network infrastructure facilities are implemented to handle the large amount of data [HYP-22].

SDN-based IoT management frameworks require an additional step to complete the communication between the IoT sensor/device and the controller. For this, IoT gateways combined with SDN switches for access to different IoT devices such as RFIDs and sensors through the control data plane interface form the infrastructure layer. The operating system on the control plane provides centralized control and visibility of different IoT services. Through the implementation of NFV in SDN-based technologies, it is possible to achieve the functions of the IoT network such as routing, access control in firewalls, secure tunnelling between the IoT gateway and the utility server in the IPSec protocol, and QoS (see Figure 13).

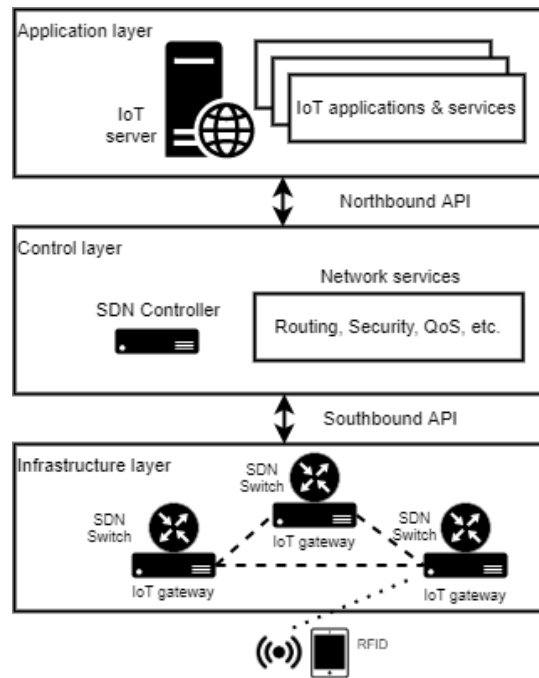


Figure 13. IoT infrastructure implementation.

### Mesh & home networks

The mesh network is a local network topology in which network components (i.e., routers, switches and other devices) can connect directly, dynamically without hierarchy usage. To provide Internet access to clients, a set of wireless routers that form the network structure are required. Due to the congestion that can arise from the limited number of routers acting as gateways, efficient allocation and management of resources is crucial to maximize capacity. Home networks have a high use of multimedia-rich entertainment applications that stream video and audio. Some of these applications have real-time limitations, including gaming and video conferencing applications, requiring high bandwidth and low latency [HYP-19].

The continued emergence and proliferation of home automation systems introduces additional traffic with stringent Quality of Service (QoS) and Quality of Experience (QoE) requirements. With SDN, a centralized controller can offer better resource allocation and management to avoid congestion, and distribute the load among routers, while NFV provides better resource utilization abstracting computation.

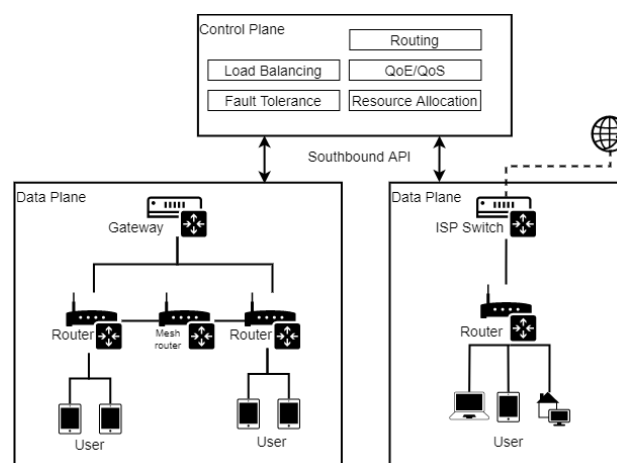


Figure 14. Software defined mesh & home networks.

#### 3.1.2.1.5 SD-Wide Area Network (SD-WAN)

As a network grows in complexity and diversity, a new approach to face these challenges is needed. SD-WAN allows dynamic bandwidth configuration, routing, and traffic efficiency to deploy services in scattered places



[HYP-23]. The main SD-WAN use-case is to provide access to different kinds of network infrastructure, devices, or permission. The advantage over traditional WAN is that a common management platform defines the policy once and it applies to all devices.

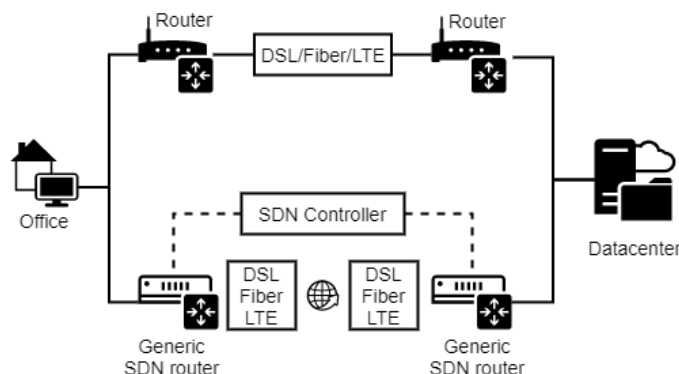


Figure 15. Software-defined WAN approach vs traditional approach.

SD-WAN uses a layered approach with abstraction in its architecture. SD-WAN architecture consists of the data plane, control plane, management plane and orchestration plane [HYP-24]. In its main architecture, SD-WAN is made up a physical or virtual SD-WAN edge, WAN gateway and SDN controller. The orchestration plane acts as a first layer of security to analyze third-party devices. The orchestration plane challenges the device and asks for some credentials. When the orchestration plane ensures that the device is indeed intended for the particular enterprise, it provides the address of the controller and the management plane. Therefore, the edge device becomes part of the management fabric. A subscriber web portal can be added to create or modify client services.

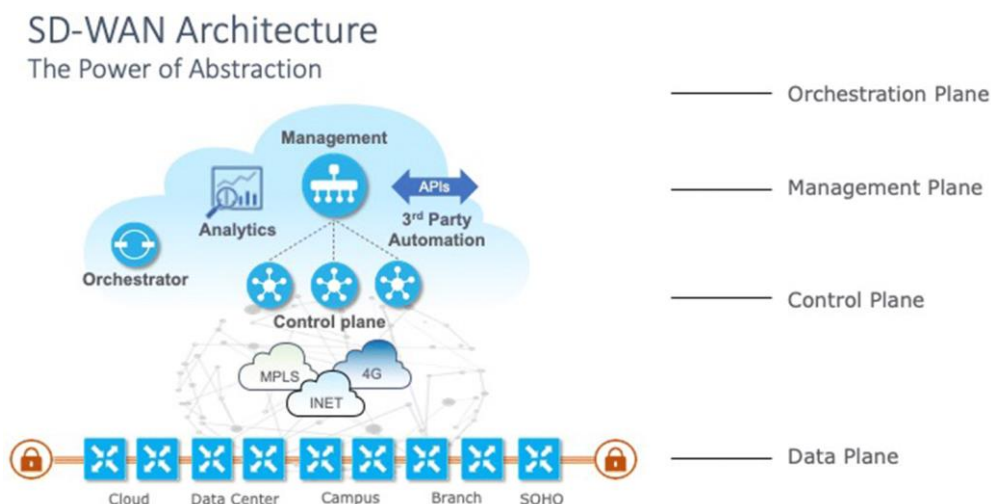


Figure 16. SD-WAN architecture [HYP-24].

### 3.1.2.1.6 Other Implementations

Different needs on the market imply different requirements that can be fulfilled by implementing SDN in other forms and approaches that vary depending on performance and communication technologies.

Cloud computing services require physical resources, so virtual and programmable networks become more important in data centers (DCs) management on a large scale, improving the infrastructure performance and its power consumption. The most important issues of domain controllers are scalability with the growth of virtual machines (VMs). SDN adds a virtualization layer to the fabric architecture of cloud providers. Hence, SDN allows the network to manage tenants according to their demands, and its controller can provide new devices to the network, allowing to receive the configuration policy when they appear online [HYP-14].

The next challenge is related to the interconnection between DCs. The characteristics of heterogeneous DCN architectures need re-routing mechanisms to avoid connectivity interruptions. Some solutions can be found in

the literature to mitigate the interconnection challenges in a cloud DCN, or to facilitate live and offline VM migration, in east-west connectivity between DCs.

The lack of compatibility between different equipment uncovers the need for improved control and management, as in optical networks. It is possible to provide technology-independent and unified control for optical transport networks using SDN, due to its data traffic being treated as flows. This can be handled effectively by the SDN. The Open Network Foundation (ONF) formed in 2013 the Optical Transport Working Group (OTWG) to develop SDN and the OpenFlow standard applications for optical transport networks [HYP-25].

Other implementations do not require relevant changes to the basic SDN architecture. For instance, Industrial IoT (IIoT) and Smart Grid have real-time systems that request for more resources or bandwidth in unpredictable situations, subject to traffic profiles and application types. When a request in the path is computed by high layers, the infrastructure layer allocates resources to perform that data-forwarding request. The adaptations allow the data layer to monitor local information, so that the data path management can be estimated locally at this layer using node-to-node negotiations in real-time [HYP-26].

### 3.1.2.2 Relevant Initiatives

Once the main structure of SDN networks is known, as well as the virtualization of network functions and their management by MANO, the different variations that it may have, depending on the application in which it has been described, can be defined. Below are presented the most relevant initiatives found in the state of the art of these technologies, as well as open source and commercial solutions.

#### 3.1.2.2.1 SDN controllers

A large number of controllers, with different characteristics are designed to support state consistency, scalability, flexibility, security, etc [HYP-8]. These controllers are developed using different programming languages such as C, C ++, Java, Java Script, Python, Ruby, Haskell, Go, Erlang, etc. to allow efficient memory allocation that improves performance, as well as cross-platform compatibility [HYP-27] [HYP-28].

As mentioned in the scientific review (Section 3.1.2.1.1), the controllers can be classified according to their characteristics on physically and logically distributed networks support.

NOX<sup>12</sup> was the world's first-generation OpenFlow controller and performs an event-based programming model. The development of NOX-MT allows an improved version of NOX with multi-thread compatibility for better performance. POX<sup>13</sup> is a controller developed in Python for a more developer-friendly environment. After its appearance and observing the great possibilities offered by this new paradigm, other solutions came onto the market in the following years like Ryu, Maestro or FloodLight.

ONOS arises as an open-source framework solution, based on OpenFlow, that adopts a distributed architecture providing a global network view to application through its logically implementation. OpenDayLight, however, presents a new SDN controller architecture based on Services Abstraction Layer (SAL) concept such that it supports protocols other than OpenFlow.

Many implementations in the literature are following a logically centralized control approach, with a physically distributed implementation. As there is no standard for this communication, different protocols and techniques are used to achieve scalable control plane scalability.

In this approach, there are different techniques to achieve controller state redundancy. ONIX and SMaRtLight perform state replication. For instance, ONIX use a Distributed Hash Table (DHT) to store the distributed network information.

Another mode of communication is based in event replication, propagating selected network events and maintaining the global network-wide view across controllers, like HyperFlow using WheelFS as distributed file system, or Ravana.

---

<sup>12</sup> <https://github.com/noxrepo/nox#readme>

<sup>13</sup> <https://github.com/noxrepo/pox>



Other types of projects have considered extending the SDN paradigm to cross-domain networks while remaining compatible with their distributed implementation, allowing logically distributed control. The DISCO project<sup>14</sup> suggests an architecture where each controller administers its own SDN network domain and interacts with other controllers by a unique lightweight control channel to provide end-to-end network services. It is designed to operate in such multi-domain heterogeneous environments, such as WANs and overlay networks. Other proposals like D-SDN enable a logical distribution of the SDN control plane based on a controller's hierarchy.

Data distribution mechanisms act as east/westbound communication in logically distributed controllers. DISCO uses the Advanced Message Queuing Protocol (AMQP), and other projects such as EW Bridge synchronize data between controllers using publish/subscribe model.

Other proposals try to define interfaces between controllers, such as SDNi, were defined to establish flow coordination requirements, and ForCES CE-CE interface or ONIX include data import/export functions.

*Table 5. List of common SDN controllers*

	Control plane architecture	Control plane design	Programming language
<b>NOX</b>	Physically centralised		C++
<b>POX</b>	Physically centralised		Python
<b>Floodlight</b>	Physically centralised		Java
<b>Ryu</b>	Physically centralised		Python
<b>Maestro</b>	Physically centralised		Java
<b>ONIX</b>	Logically centralised	Flat	Python, C
<b>ONOS</b>	Logically centralised	Flat	Java
<b>OpenDayLight</b>	Logically centralised	Flat	Java
<b>DISCO</b>	Logically distributed	Flat	Java
<b>Kandoo</b>	Logically distributed	Hierarchical	Python, C, C++

### Network Slicing

To solve SDN management, some approaches can be found in the literature offering different perspectives. In [HYP-29] a combination of Network Management System (NMS) with SDN is defined, replacing legacy NMS in network operators. The Software-Defined Network Management Protocol (SDNMP) tries to manage SDN and virtual networks using traditional NMS. In details, SDNMP unified interface is mainly divided into three functions:

- Data acquisition function is mainly used to extract network topology and related resources data of SDN.
- Data storage and processing function mainly stores data which is acquired by SDN controller and makes corresponding processing for front-end display.
- View function. Because the information of SDN is changing timely, real-time response to a user request and present the latest state of the network is needed.

<sup>14</sup> <http://anr-disco.ens-lyon.fr/>

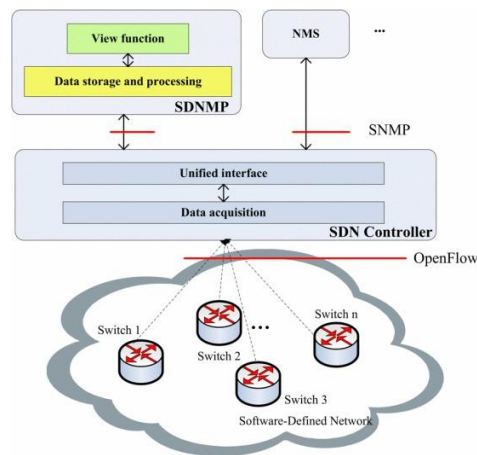


Figure 17. SDN management approach.

Other approaches offer different possibilities for developing a new abstraction layer. In [HYP-30] a Network Hypervisor layer provides a single common interface by which SDN applications can control and leverage the various underlying SDN network technologies and a high-level abstraction designed to make it easy for SDN applications to create commonly used SDN networks.

A decentralized SDN requires multiple logic controllers. To manage these controllers, a network virtualization layer is added to OpenFlow networks, called FlowVisor [HYP-31]. This acts as a proxy controller that allows multiple controllers to simultaneously control overlapping sets of physical switches. As a virtualization layer, FlowVisor is located between the underlying physical hardware and the software that controls it. With a set of instructions to control the underlying hardware, FlowVisor hosts multiple guest OpenFlow controllers, one controller per segment. These segments are a set of flows running on a topology of switches.

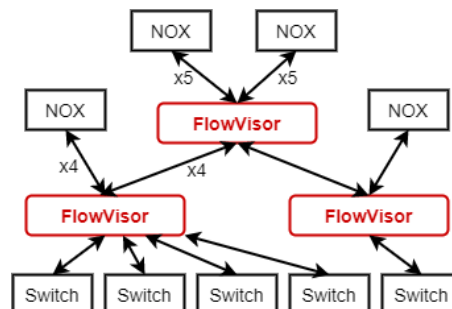


Figure 18. FlowVisor location in a SDN network example

FlowVisor divides the bandwidth of the link by assigning a minimum data rate to the set of flows that make up a segment and splits the flow table on each switch by keeping track of the flow entries that belong to each guest controller.

### Artificial Intelligence/Machine Learning

As the networks grow in complexity, both the heterogeneity of resources and the dynamics of traffic grow. Artificial Intelligence and new learning technologies analyze data-traffic characteristics to automatically manage and control network operations. SDN controller uses the API to send programming instructions to a network device. In an AI-based SDN, controllers collect network statistics information to lay a solid foundation for continuous network optimization, and program intelligent strategies into the task script, assigning them into the network allocation tasks with the API.

Some Artificial Intelligence (AI) and Machine Learning (ML) approaches can be found in the literature to solve different issues, allowing SDN to improve on routing, traffic classification, flow clustering, intrusion detection, load balancing, fault detection, QoS and QoE optimization, admission control and resource allocation [HYP-32]. AI network planning assists in planning heterogeneous networks, including network management and

operations, cognitive management architecture for managing 5G networks, network security and breach Detection


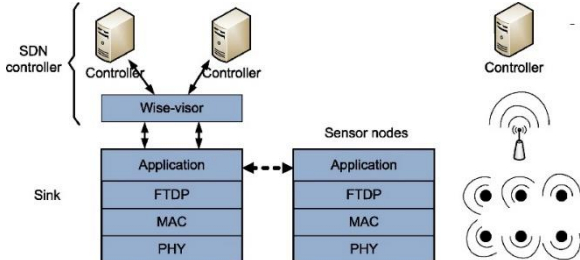
Machine learning techniques learn from the data available in the environment and uses it to improve overall performance. In SDN, supervised learning methods start with a pre-defined knowledge and unsupervised learning methods are provided without a pre-defined knowledge. These methods are mainly used in SDN for intrusion prevention and detection, improve performance and detect DDoS attacks. On reinforcement learning, as Q-learning, the system learns based on a set of reinforcements from its environment and is widely applied in SDN paradigm for routing and adaptive video streaming.

Other techniques, such as metaheuristic algorithms, try to solve optimization problems in SDN that cannot be solved with any specific approach in a reasonable time. Some examples found in the literature include Ant Colony Optimisation, Simulated Annealing, Firefly Optimisation, or Grey Wolf Optimisation.

AI techniques as in Fuzzy Inference represents human-like knowledge and explanation skills by using multivalued logic systems in the SDN paradigm to introduce new protocols, intrusion detection, selection of optimal network implementation schemes, and traffic engineering [HYP-33].

Some relevant initiatives that develop AI/ML into software-defined networks are listed below:

*Table 6. AI proposals over SDN*

Proposal	Description
Future Intelligent Network (FINE) [HYP-34]	<p>This proposal includes a framework divided into three different planes: intelligence plane, agent plane and business plane. The intelligent plane is the brain of the network, which is based on AI with a wide range of algorithms (deep learning artificial neural network).</p>  <p><i>Figure 19. FINE framework [HYP-34].</i></p> <p>To include AI into an SDN/NFV network, FINE propose to deploy DPIs for every component, and send the information collected to a big data module in the basic layer of the intelligence plane.</p>
Knowledge defined networks (KDN) [HYP-35]	<p>This paradigm is based on SDN, Network Analytics (NA) and AI. The KDN is divided into four different functional planes: data plane, control plane, Knowledge Plane (KP) and management plane. The KP applies machine learning and deep learning techniques to transform the network analysis collected by the management plane into knowledge and uses it to make decisions.</p>
Fuzzy Topology Discovery Protocol (FTDP) [HYP-36]	<p>The objective of the devised fuzzy protocol is to choose the best next hop according to the decision parameters. The protocol is designed for SDN-WISE architecture and depicts the network architecture in which FTDP is deployed. In FTDP, the sink nodes receive all the information from the nodes and extract the required parameters from them. Then, the information is sent to the controller.</p>  <p><i>Figure 20. FTDP implementation [HYP-36].</i></p>

### 3.1.2.2.2 NFV MANO

As mentioned in the scientific review (Section 3.1.2.1.3), the main NFV architecture is formed by VNFs and MANO. The main NFV Management and Orchestration solutions are developed by open-source projects as Open Source MANO (OSM)<sup>15</sup>, Open Network Automation Platform (ONAP)<sup>16</sup>, and Open Platform for NFV (OPNFV)<sup>17</sup>.

Other open-source MANOs that can be found nowadays have emerged mainly from different sources. For instance, some cloud open-source projects, such as Tacker in OpenStack, deploys Generic VNF Manager and an NFV Orchestrator to operate Network Services and Virtual Network Functions (VNFs).

- Other open-sourced solutions that served as orchestration/test tool in private companies, such as Telefonica OpenMANO, NTT's Gohan and Open-O.
- Vendor/university projects such as Cloudify, Open Baton.

Other private solutions offer deployment of MANO stacks. Ericsson Cloud Manager<sup>18</sup> is the Ericsson proprietary MANO solution. This solution offers on-boarding and instantiation of virtual applications allowing orchestration and management of network services and cloud resources like storage, networking and VMs.

Nokia's MANO<sup>19</sup> proprietary implementation, CloudBand, can be flexibly deployed for any combination of NFV Infrastructure/Virtualized Infrastructure Manager (NFVI/VIM), generic VNF Manager (VNFM-g), and NFV Orchestrator, and serves VNFs from Nokia and other suppliers.

Some commercial solutions, as CISCO NFV<sup>20</sup>, develop its own architecture. CISCO is one of the cloud services industry leaders and its fully open platform is ETSI compliant. It offers carrier-grade high availability, reliability, and predictable performance through its NFV infrastructure solution.

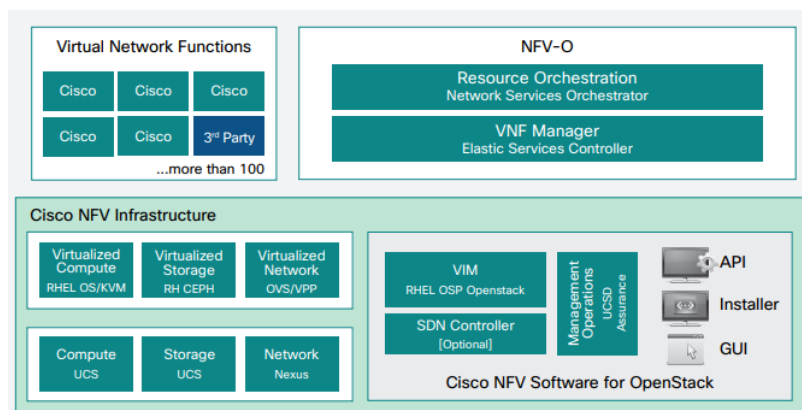


Figure 21. CISCO NFV Infrastructure<sup>20</sup>.

NFV can be utilized virtualizing network resources by making slices where the southbound is involved, and controlling these slices through the northbound interface. Both interfaces then become an integral part of NFV, while still being used for flow installation and application communication by the SDN controller [HYP-37].

<sup>15</sup> <https://osm.etsi.org/>

<sup>16</sup> <https://www.onap.org/>

<sup>17</sup> <https://www.opnfv.org/>

<sup>18</sup> <https://www.ericsson.com/en/portfolio/digital-services/automated-network-operations/orchestration/ericsson-orchestrator>

<sup>19</sup> <https://www.nokia.com/networks/solutions/cloudband/>

<sup>20</sup> <https://www.cisco.com/c/en/us/solutions/service-provider/network-functions-virtualization-nfv/index.html>

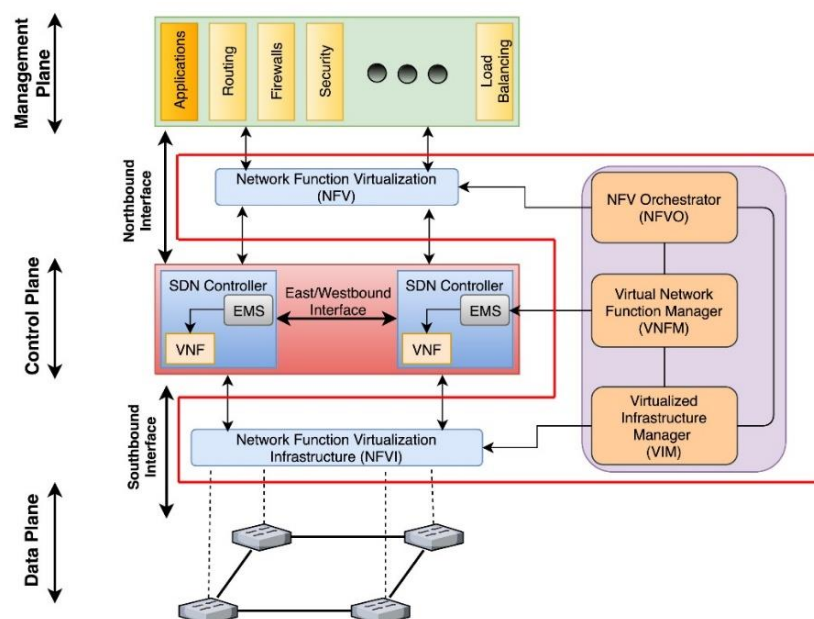


Figure 22. NFV and SDN interface abstraction [HYP-37].

### 3.1.2.2.3 SD-Wireless Networks

In wireless networks, many studies have been carried out that have resulted in architectural proposals and their possible implementations. Some proposals, like OpenRadio, aim to enable programmability on the physical and MAC layers [HYP-38]. Radio and cellular solutions focus their proposals on optimising the connection between the base station and the core network [HYP-39].

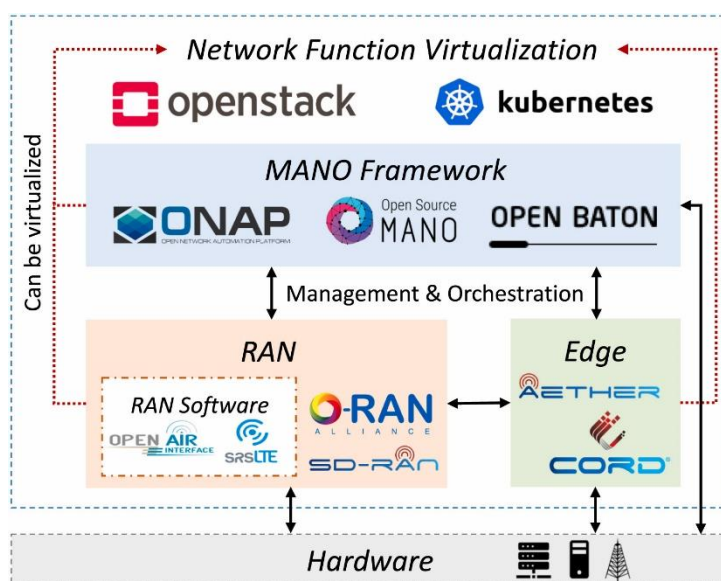
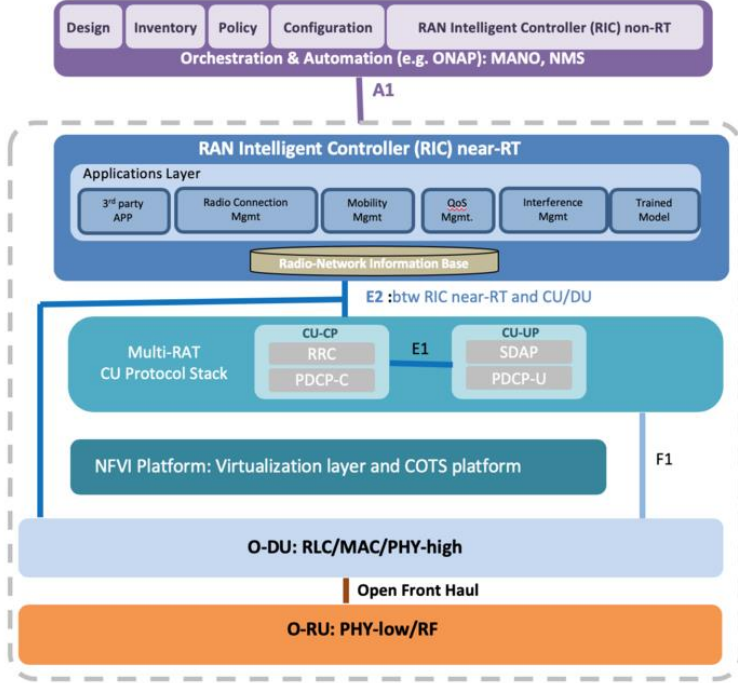


Figure 23. MANO and RAN initiatives [HYP-39].



Table 7. Open RAN initiatives

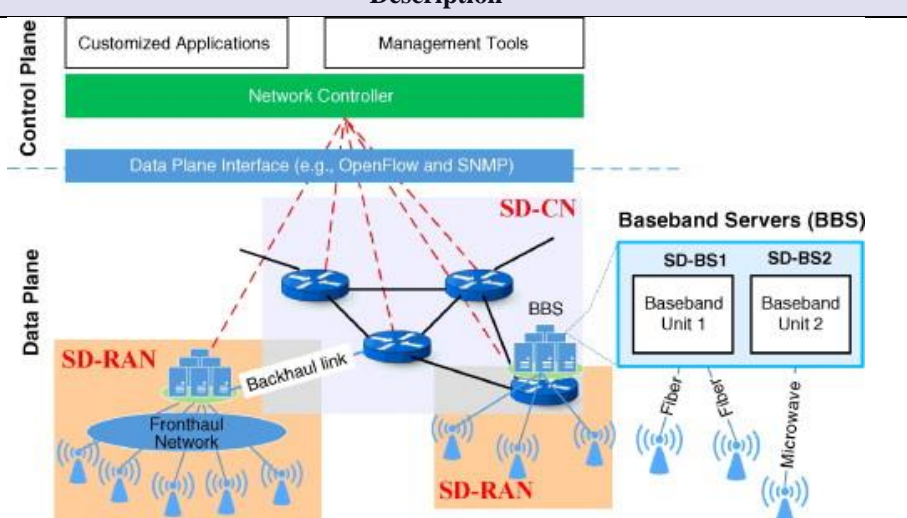
Initiative	Description
O-RAN [HYP-38]	<p>Open Radio Access Network Alliance is world-wide community of different types of organisations from industry (network operators, vendors), research and academic domains with main aims: (1) To create new O-RAN architecture and standards towards more intelligent (AI based radio control solutions), open, virtualised and fully interoperable among mobile network operators, (2) to build architecture based on standards fully supporting and complimentary to standards promoted by 3GPP and other industry standards organizations, (3) to develop open software for the RAN (cooperation with Linux Foundation) and (4) to test and integrate RAN solutions by different member companies.</p>  <p style="text-align: center;"><i>Figure 24. O-RAN architecture</i></p> <p>O-RAN architecture is focusing on developing open-source RAN AI empowered, with modularity and operability capabilities which is envisioned as next generation RAN [HYP-38].</p>
SD-RAN <sup>21</sup>	<p>SD-RAN<sup>21</sup> is ONF's new exemplary platform for 3GPP compliant software-defined RAN that is consistent with O-RAN architecture. SD-RAN creates open-source components for the mobile RAN space. It is cloud native and complementing the focus on O-RAN architecture and interfaces by building and testing compatible open-source components.</p>

Design approaches that implement SDN in radio networks are described below.

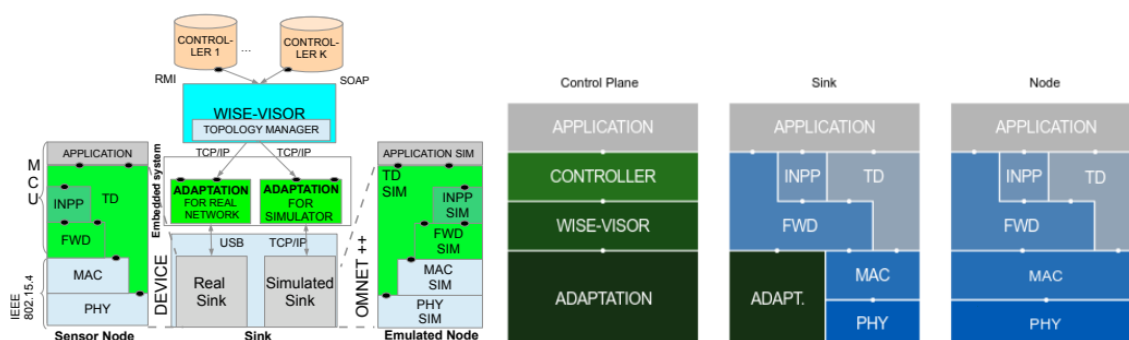
Table 8. Proposals implementing SDN in radio networks

Proposal	Description
Hybrid SDN-SDR [HYP-41]	Provides cross-layer combination of SDN and Software-Defined Radio (SDR) for exploiting frequency spectrum and link information in the 5G network. The cross-layer controller is used to request frequency spread spectrum and make the decision for flow traffic. This architecture also manages user authorization in the cross-layer controller and grant access to a better band.
SoftAir [HYP-42]	The whole data plane consists of software-defined radio access network (SD-RAN) and software-defined core network (SD-CN). The programmability of the plane allows an open and virtualizable network forwarding infrastructure. The SD-RAN consists of a set of SD-BSs, while the SD-CN is composed of a collection of SD-switches. The control plane mainly consists in network management tools and customized applications of service providers or virtual network operators.

<sup>21</sup> <https://opennetworking.org/sd-ran/>

Proposal	Description
	 <p><i>Figure 25. SoftAir architecture [HYP-42]</i></p> <p>This architecture introduces three essential management tools, namely mobility-aware control traffic balancing, resource-efficient network virtualization, and distributed and collaborative traffic classifier.</p>

In IoT-based wireless sensor networks, the main focus is to adapt information from the sensor to the SDN controller. An approximation can be observed in Wireless Sensor Networks as SDN-WISE [HYP-39] [HYP-40]. This approach mainly consists in a middle layer managed by a visor that collect sensor/device packets. An adaptation layer is needed to perform translation between the sensor node and the Visor.



*Figure 26. SDN-WISE architecture [HYP-39].*

The controller implements topology management, building the overall topology of the network by collecting reports of topology discovery from each sensor node. WISE-Visor allows multiple controllers to run on the same data plane network using abstraction and virtualization.

- In the sensor, the forwarding layer (FWD in Figure 26) handles incoming packets according to the rules specified in the WISE flow table. This flow table is updated according to the flow instructions sent from the controller.
- Topology Discovery (TD in Figure 26) sets neighbourhood and creates a table consisting of the list of neighbours to a sensor node, allowing to calculate the best next route to the sink so that the sensor nodes can send control packets or reports to the controller through it.
- In-Network Packet Processing (INPP in Figure 26) performs data aggregation and other processing tasks on the network by running on top of the forwarding layer.

Other proposals found in the literature, such as WSN-SDN, aims to develop an architecture that consist of a Base Station (BS) and several sensor nodes. SDN controller operates on BS taking routing decision. Sensor nodes contain flow table as in the SDN concept which is populated by SDN controller [HYP-19].

Table 9. Proposals implementing SDN in wireless IoT networks

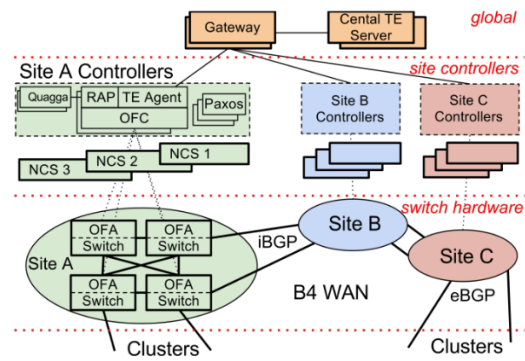
Proposals	Description
SD-WSN	Proposes an architecture for reconfigurable WSN network on the basis of customer need by using role injection and delivery mechanism. The role compiler generates scenarios which are injected through wireless communication. The change in the sensor nodes is carried by Field Programmable Gate Array (FPGA) integrated circuits and a Microcontroller Unit (MCU).
Integrate WSDN	A multi-purpose sensor network exploited NFV for sharing single infrastructure for many applications in a sensor network. Each node has an abstraction layer for a shared hardware which works on the overlay network and creates multiple virtual sensor networks (VNS).
Sensor OpenFlow (SOF)	The concept of reprogramming and re-tasking in WSN was proposed in SOF, where the control layer is formed by “sensor re-configuration” module. Query strategy control module perform flow-based forwarding in the data plane consisting of sensor nodes.

For home and enterprise networks, a framework for management of 802.11 networks infrastructures such as Odin tackles the issue of authentication, authorisation, and accounting in the Wireless Local Area Network (WLAN) services. Odin enables network operators to deploy WLAN services as network applications. It consists of a master, agents, and applications. The master runs as an application on the OpenFlow controller, controls the agents, and updates the forwarding table of access points (APs) and switches, and the agents run on the APs and collect information about the clients [HYP-45].

### 3.1.2.2.4 SD-WAN and DCNs

Different SDN applications have been proposed in DCN to improve and modify its performance. Some changes in DCN infrastructure and virtualization of data-centre LANs and WANs.

Table 10. Proposals implementing SDN in SD-WAN networks

Proposals	Description
Google B4 [HYP-46]	<p>B4 is a private WAN that connects Google’s datacentres across the planet. Its massive bandwidth requirements deployed to a modest number of sites. Each B4 site consists of multiple switches linked to remote sites. It is a challenge that relies on SDN to improve elastic demand management that seeks to maximize average bandwidth. A B4 SDN architecture approach can be logically viewed in three layers that provides full control over the edge servers and network. SDN-based B4 has to support existing distributed routing protocols, both for interoperability with non-SDN WAN implementation and to allow for gradual deployment.</p> <ul style="list-style-type: none"> <li>The switching hardware layer forwards traffic and does not run complex control software.</li> <li>The site controller layer needs servers to host OpenFlow controllers that maintain network state based on Network Control Applications (NCAs) directives and instruct switches to set forwarding table entries based on this changing network state. Servers enable distributed routing and central traffic engineering as a routing overlay.</li> <li>The logically centralized applications enable the central control. The SDN Gateway abstracts details of OpenFlow and switch hardware from the central server. This global layer applications are replicated across multiple WAN sites with separate leader election to set the primary.</li> </ul>  <p style="text-align: center;">Figure 27. B4 element distribution concept [HYP-46]</p>

Proposals	Description
Microsoft SWAN [HYP-47]	Microsoft main resources are set in distributed datacentres all over the world. SWAN project is a SD-WAN implementation for inter-datacentre networks that centrally controls traffic and re-configures the network data plane to match the current demand. SWAN routes the update of the switch in a congestion-free manner by taking advantage of a small amount of scratch power on the links.

Switching with Bloom Packet Filters (SiBF) transform the DCN into a software problem that introduces an army of rack managers acting as distributed controllers, containing all the flow configuration settings, and requiring only topology information [HYP-48]. To mitigate interconnection challenges in a cloud DCN and to support live and offline Virtual Machine (VM) migration without interrupting VMs during the mitigation process, there are other proposals in the literature [HYP-49] [HYP-50].

### 3.1.2.2.5 Systems & Products

An OpenFlow switch is a software program or hardware device that forwards packets in an SDN environment. It supports OpenFlow protocol for communication and management and consists in a flow table to lookup packet and forwarding. This communication is secured through a TLS or SSL channel between switch and controller.

There are several SDN software switches available that can be used when developing services on top of SDN. Mainly, the OpenFlow vSwitch is a stack used as a virtual switch adapted to various hardware platforms and currently supports multiple virtualization environments including Xen / XenServer, KVM, and VirtualBox [HYP-9]. The most relevant virtual switches are listed below:

*Table 6. OpenFlow-related software projects switches*

Product	Description
Contrail-router	Vrouter that implements the data-plane functionality that allows a virtual interface to be associated with a VRF.
LINC	OpenFlow software switch implemented in operating system's user space as an Erlang node.
ofsoftswitch13	OpenFlow compatible user-space software switch implementation in C/C++.
OpenFlowClick	OpenFlow switching element for Click software vrouters.
OpenFlowJ	Source code implementation of OpenFlow protocol. Both Beacon and FlowVisor incorporate this code.
OpenFaucet	As a pure Python implementation of OpenFlow protocol, OpenFaucet can implement both switches and controller.
Pantou/OpenWRT	Turns a wireless router into an OF-enabled switch.
Switch Light	Thin switching software platform for physical/virtual switches.
XorPlus	Switching software for high performance ASICs.
Indigo	Open source OpenFlow implementation in C that runs on physical switches and uses the hardware features of Ethernet switch ASICs to run OpenFlow
Pantou	C programmed software that turns a commercial wireless router or Access Point into an OpenFlow-enabled switch

Some commercial products develop their own communication protocol between the controller and the switch. With respect to those compatible with OpenFlow, products such as:

*Table 7. OpenFlow compatible commercial switches*

Company	Series
Hewlett-Packard	HI Switch, FlexFabric and FlexNetwork series
Arista Networks	Arista 7150 Series
Extreme Networks	ExtremeSwitching
Huawei	CX600 and S-Series

Company	Series
Juniper	EX4600, EX9200 and QFX5100 switches
Brocade	MLX Series
NoviFlow	NoviSwitch
IBM	RackSwitch G8264
NEC	PF5200 series and PF5820
Pica8	P-3290
Alcatel-Lucent	Omniswitch

### 3.1.3 Edge/fog computing

Cloud Computing (CC) has dominated the arena of IT world during the past decades. Despite having faced some challenges and fine-tuning (such as the CDNs, the client-server vs subscription or non-state approaches, REST vs SOAP in the web field, etc.), CC has remained the reference in the vast majority of modern IT deployments. Supported by high reliability thanks to backup possibility, virtually unlimited storage capacity, cost savings due to centralization, among other...altogether with the scarce availability of true alternatives, CC grew uncontested. However, the advent of the new generation of internet (NGI), characterized by ever-increasing demands of bandwidth, latency and computing power has brought to light some flagrant shortcomings of this paradigm.

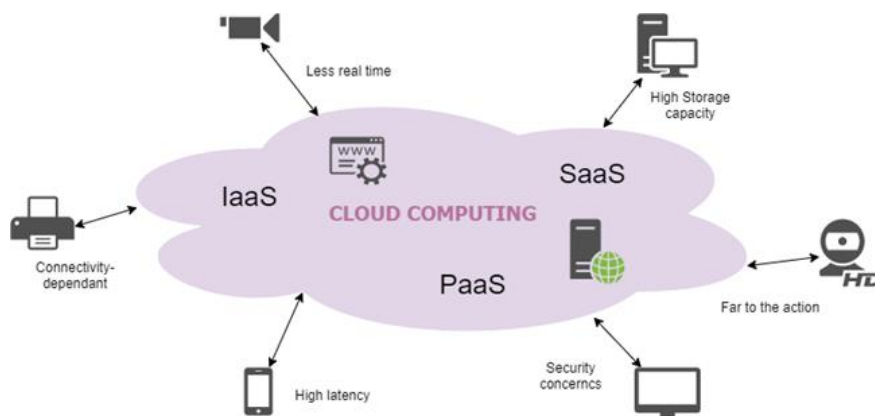


Figure 28. Classic processing and analytics approach, where the computation is mainly done at cloud level

Looking at the most evident flaw -latency-, the context is clear: in CC, computation of the data (anything else than simple forwarding) is done usually millions of kilometres away from the actual course of the action. From a study by K.Ha [EDGE-1] it can be easily checked that the difference of requesting image analysis by CC taking place in different remote locations (e.g. West Coast USA, Europe, Asia) may mean delays of 200 to 500 milliseconds in the response. In case of critical applications (like factory automation, clinical surgery, intelligent transport systems [EDGE-2]), where similar information is managed, such delays may have catastrophic consequences.

On the other hand, the flaw about bandwidth seems to be a prominent issue to be tackled for the sake of future applications. Wearable devices, hand-held devices, drones, surveillance cameras and other type of data-generators are proliferating in almost all verticals. Transmitting video streams through the network at acceptable rates becomes unaffordable for many applications [EDGE-3] considering the bandwidth those take. However, not only multimedia applications are currently posing a threat to bandwidth availability. Web pages [EDGE-4] and sensor streams are so data-rich that already suffocate transmission margins.

Another major concern in CC is privacy. With the current CC model, data must travel to cloud servers located significant kilometres away, usually passing through several networks and intermediate elements, where data



security may be in question. Following the previous rationale, as more data will be encapsulated in the messages, the more risk exposed. A solution could be found allowing some data reduction or filtering before going to CC. Even better, some reasoning capacity might be installed to act just as a network firewall letting only minimum necessary, secured, reduced data to fly over, keeping sensitive data under control.

Last but not least, the dependability on network quality connection and cloud services provider availability [EDGE-5]. If some of the ISPs intervening in the process suffer a network breakdown or if the connection is lost for any other reason, delays will be experienced, and the loss of substantial information will exist. Caching systems partially cope with this problem not reaching to completely solve it.

On top of this, all the previous issues are just at their birth. The same (and further) problems will be enlarged as aftermath of the new wave of emerging technologies. According to the Gartner's hype cycle for 2021 and beyond [EDGE-6], some of the most popular technologies in the forthcoming years will be Augmented AI, Explainable AI, Data Fabric, Augmented Reality, Adaptive ML and private 5G. Cognitive applications (like the ones listed) have strong computing requirements, which are often carried out in remote locations. It will mean a huge need of available hardware to enable AI pervasiveness in all industries [EDGE-7]. When analysing Augmented Reality, Virtual Reality and private 5G, another whirlwind of actors appear: wireless sensors, IoT data providers, wearables and other end devices. It is currently estimated that about 45% of the world's data will be moved closer to the network **edge** by the end of 2025 [EDGE-8]. That 45% looks scary when looking at their very forecasts of total data to be generated by devices, which would be almost 80ZB coming from more than 40 billion devices [EDGE-9]. Realising both rationales, the conclusion was: many more new devices will be generating increasingly reach data that should be used as soon as possible for the sake of user experience and industrial benefit.

At that point, it was automatically inferred that the answer to all the previous might be moving the **CC capacities closer to the place where the action takes place**. As classic IT deployments diagrams contemplate data origins, data forwarders, networking elements and centralised processing units, in a bi-directional flow, **the concept chosen in ASSIST-IoT** to refer this new paradigm is “**edge-cloud computing continuum**”. This term (that can be paired with just “edge computing”) was born to define the fact of spanning the resources for running applications throughout diverse locations ranging from the cloud premise (distant from the action) to the edge (closer to the data source). In this context, **edge computing** offers new possibilities. It means carrying out the same kind of computation (and with more room for improvement) but moving more of it to the edge of the network. In other words, closer to “things” that produce and consume data.

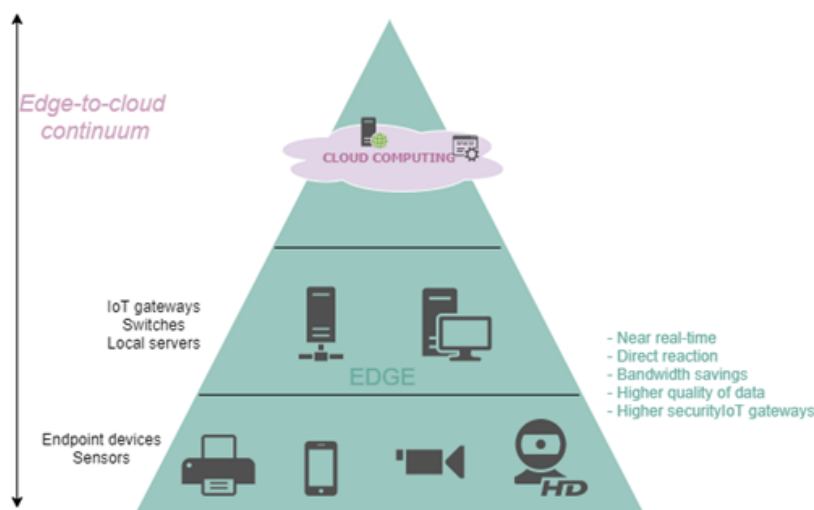


Figure 29. Edge-to-cloud computing continuum approach and its advantages [EDGE-10]

As it can be seen in Figure 29, the bird's eye structure of edge computing can be separated in three main levels:

- **The front-end level**, consisting of endpoint devices like sensors, actuators, mobile equipment (smartphones, tablets, wearables, etc.), personal computers, among other data-generator elements (e.g. cameras, Bluetooth). This layer cannot meet much computing requirements, if any, in most deployments. Therefore, components here act mostly as data forwarders.

- **The near-end level** is actually the key introduction in the edge computing paradigm. This level, that can be materialised in different ways (see below in Scientific Review - 3.1.3.1), will carry out the assigned tasks to alleviate the traffic towards the cloud and will help achieve the aforementioned benefits. Usual tasks allocated are filtering, pre-processing, aggregating, caching content, device management and privacy protection.
- **The back-end level** corresponds to the classic CC centric element, where bulk operations of processing and storage take place. This layer, either taking place in one remote location or multiple, also hosts the main workload of the associated cloud services. This level may act, sometimes, in the edge computing environment, as a centralized controller.

This structure (especially in the near-end level) relies heavily on the concepts of edge/fog, that are normally leveraged for reducing latency, optimizing bandwidth use, improving privacy and security, and alleviating network congestion and traffic in general [EDGE-11]. Pushing data processing as close to the edge as possible can bring serious benefits answering the previous questions, particularly where communication costs are high or where instant action is needed (*priority for many industrial processes*). Collecting and analysing information close to endpoints means that (re)action can take place in (near) real time. Furthermore, only selected information needs to be forwarded to cloud for storage and analysis. In addition, if input data originates from multiple heterogeneous streams (with extreme data volume), complexity of managing that information in (near) real time becomes a change-maker challenge. Therefore, more benefits can be **gained** by architecting for computing at “edges” of ecosystems.

There is a huge discussion about terminology in the field of edge computing. In the pursue **of a formal definition of edge computing**, some examples can be found in the literature. Although some discrepancies about technicalities – mainly due to the lack of a reference entity or clear standard, all agree on certain key points: edge computing refers to moving CC capabilities closer to the data source.

The Industrial Internet Consortium defines it as follows: “*Edge computing is a decentralized computing infrastructure in which computing resources and application services can be distributed along the communication path from the data source to the cloud*” [EDGE-12]. For Mostafavi, [EDGE-13] “edge computing” is “*the practice of processing data near the edge of your network, where the edge computing is a distributed and open information technology architecture. That may span from end users, to the edge, to core and up to the cloud*”. According to M. Satyanarayanan, an authoritative voice in the field, edge computing is “*an approach to efficient contextual data analysis in which computation is performed on sensing devices (sensors, actuators, controllers, concentrators), network switches or other devices (concentrators) instead of transmitting the whole data to a centralized computing environment/cloud*” [EDGE-14].

Regarding ASSIST-IoT’s Grant Agreement, the scope of our project is clearly aligned with the latter definition. The proposed approach is focused on the **edge-fog-cloud continuum model**. Although the word “edge/fog” was used in the preparation of the proposal (currently, Part B of the GA) to capture all generic situations in which data processing takes place in the appropriate location within the IoT ecosystem, the members of the team realise that an arbitrary use of the concept edge/fog, edge computing, edge node, etc. could lead to confusion. Such a divergence in terminology is very common in ever-evolving areas like edge/fog computing [EDGE-15]. That is why we have decided to include here below a brief outline of the terms, how we used them in the Grant Agreement text, how they could appear in the future in the project and what we really mean by them:

*Table 11. Glossary clarification about edge/fog computing*

Term used in the GA	Concept – what we mean to express
Edge/fog computing	<b>Edge computing</b> as a paradigm, meaning data-processing completed away from the “central processing location” (e.g., a cloud), and as close as possible, and as reasonable, to the data-generating elements.
Edge computing	
Edge node	<b>Fog node</b> . The node specifically selected, within the continuum, to perform given function(s).

The “edge computing” draws from concepts like CDNs, that have been long used in the web field. However, it was first used in 2012 when F. Bonomi (CISCO) defined “fog computing” as part of the edge computing. One

year later, the Mobile Edge Computing was defined and another year later (2014), the concept of “cloudlets” appeared. Despite being a recent field of research (8 years), this concept has been gaining more and more attention both at academic (more than 100 papers in 2013-2020 in prominent journals) and at industrial commercial plane (Google [EDGE-16]), Cisco, Amazon [EDGE-17], INTEL [EDGE-18], ...). This increasing interest is already being reflected in the continuous research landscape. Not only new innovative projects are being advertised (e.g. via H2020 calls ICT-12-2018 [EDGE-19], ICT-51-2020 [EDGE-20]) but several initiatives such as OpenFog consortium [EDGE-21], OpenEdge computing initiative [EDGE-22], and Multi-access Edge Computing [EDGE-23] (MEC - promoted by ETSI) have been created aimed at establishing reference architectures and standards in this field.

To sum up, edge computing is identified as a trending solver to some of the issues inherent to cloud computing - like providing closer processing units to users, less delay, and no bandwidth limitation. However, what does the scientific evidence say about this? Is the edge/fog computing already a reality in the current IoT deployments? Is there a clear reference to build upon? Which one does apply to ASSIST-IoT?

### 3.1.3.1 Scientific review

While, conceptually, edge computing has been rapidly gaining traction over the past years, many different examples can be found in the literature of mixed definitions, varied approaches, heterogeneous implementations, proper business models, adequate technologies, etc. Endless number of use-cases are arising through all sectors [EDGE-24] that can hugely benefit of edge computing characteristics. In those use-cases, there is an incredibly wide variety of infrastructures. Some, relying on legacy equipment, other, leveraging former IoT devices or introducing new resourceful machines at various locations. Additionally, diverse actors intervene whenever thinking of an edge deployment [EDGE-25]: Network Operators with their public network, ISP providers with powerful hardware, wide area access machinery put in place by companies, application developers and data integrators and, finally, users with their personal devices. Stretching the “**edge-to-cloud-computing continuum**” in a horizontal plane, the computing spots are everywhere. From the “things”, passing through IoT Gateways, personal computers, tablet, smartphones, local servers, switches, cell towers or ISP centres up to the cloud [EDGE-26].

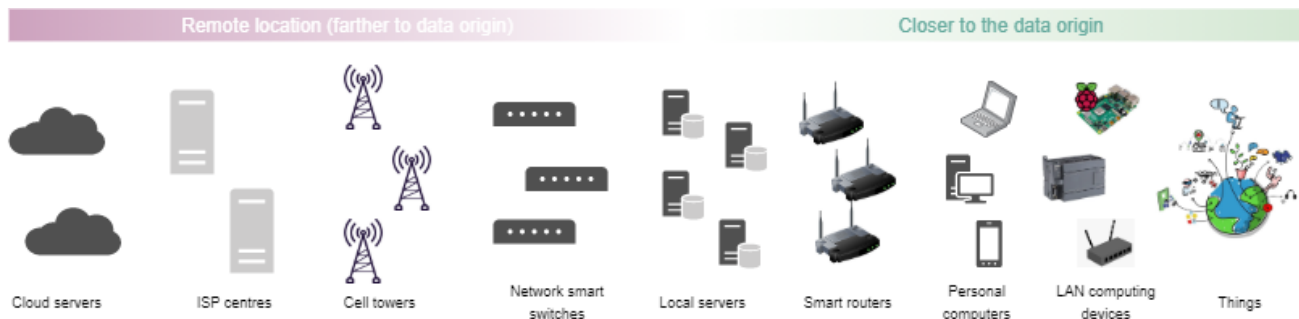


Figure 30. Wide spectrum of potential edge-to-cloud continuum devices.

All the previous form an extremely complex environment which makes **technically impossible the creation of a one-size-fits-all solution** for the “edge computing”.

Since the beginning, “edge computing” has been divided in three main categories of implementation: mobile edge computing. Cloudlets and fog computing [EDGE-27]. All of them share the vision of edge computing (see Figure 29) and strongly rely on mechanisms such as virtualization, containerization, safety resources management and metering. However, the three present clear differences in configuration, characteristics and scope which tear them apart.

In few words, **multi-access (formerly, mobile) edge computing (MEC)** is associated to Radio Access Network (RAN), where the Edge node is always located at a cell tower – base stations, covering mobile devices in its range. This implementation is oriented to ISP providers and leverages techniques of 4G-LTE and 5G such as function virtualization (NFV [EDGE-28]) to achieve edge computing benefits. **Cloudlets** can be understood as “replicas” of the cloud capabilities but closer to the edge of the network, thus reducing latency, round-trip time and backhaul bandwidth consumption. Cloudlets are conceived as “cloud in a box” acting as cloud running over one or a cluster of resource-rich servers following literally the canonical three-levels edge computing structure. **Fog computing (FC)**, instead, aims at leveraging the flexibility of IoT to perform edge computing functions.

Via the usage of “fog nodes”, that can be spanned through the edge-to-cloud continuum creating 1 to N “near-end” layers, fog computing orchestrates their functioning to take advantage of wide range of devices in the continuum spectrum (see Figure 30).

The “edge nodes” in MEC and cloudlet approaches are always one logical step away from end devices, which certainly might improve latency and context awareness. These two approaches also have more resourceful nodes to provide computing power through. On the other side, fog computing nodes might be located several hops away from end devices and are clearly scarcer in resources, having to cope usually with legacy equipment with hard restrictions. Nonetheless, fog computing allows accepting non-IP based access protocols (such as MQTT [EDGE-29]) and actually provides the more flexible approach for dynamic, scalable, growing environments. In contrast, fog computing implementations will require a higher level of fine-tuned design, needing to map particular application requirements and available equipment prior to proceeding with the deployment [EDGE-30]. From another point of view, without consolidated enough cloudlet equipment and examples, there is little chance for creating new applications for such deployments, while the IoT arena is plenty of fresh contributions.

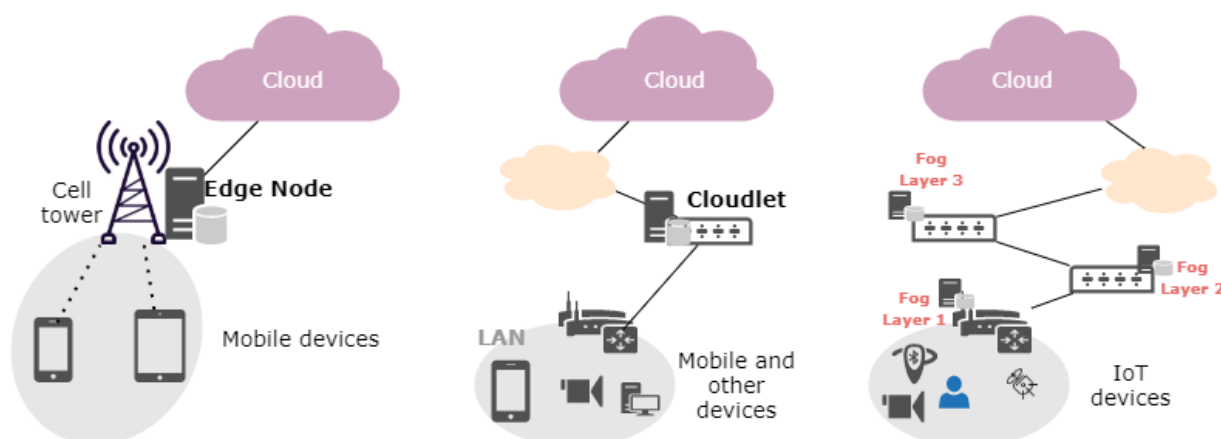


Figure 31. Main differences between edge computing implementations. From left to right: MEC, Cloudlet and FC.

In [EDGE-31] can be found an outstanding review of the differences among them, including advantages and disadvantages. As a tiny reference, we are including a simple conceptual comparison. In the same study, authors aimed at defining a decision tree for IT managers to select one or the other depending on: proximity, access mediums, context awareness, power consumption and computation time. According to the writers, they came up with a valid and sound reference, however, they concluded that “edge computing” implementation options are diverse and differently interpreted by customers. This is mainly due to the lack of standardization [EDGE-32].

Table 12. Summary of edge computing implementations comparison

Feature	Multi-Access (MEC)	Cloudlet	Fog computing
Node location	RAN Controller -cell tower	Local/outdoor installation	Any edge-to-cloud continuum spot
Proximity	One hop	One hop	One or multiple hops
Node HW device	Server at the base station	Data center in a box	Router, IoT GW, switch, RPi...
Management	Mobile orchestrator	Cloud Agents	Orchestration or Federation
Context awareness	High	Low	Medium
Access mechanisms	Mobile networks (e.g. 4G)	WiFi	BLE, WiFi, ZigBee, mobile...
Acquisition cost	Medium	High	Low
Reliability	Medium	Medium	High

Apart from those three main divisions, some new concepts have emerged during the last few years to catalogue specific/creative edge implementations. Here below there is a little reference of those, while in Figure 32 we are depicting an illustrative Venn diagram which spots the different concepts (extracted verbatim from [EDGE-33]).



**Mist computing** [EDGE-34] is used to denominate a fog computing deployment with the minimum expression of data processing as close to the data creator as possible. This definition was created to represent a “lightweight fog layer” just above endpoint devices, acting as the most peripheral computing element possible. Mist nodes are normally micro-controllers (e.g., Arduino [EDGE-35]) with the ability to forward IoT data upwards.

**Dew computing** [EDGE-36] is an architecture that extends the classical client-server architecture from CC, leveraging content backup at the edge to allow devices to work without connection for a period of time [EDGE-37]. For IoT, dew computing is different to cloudlets as it conceives a local “server” [EDGE-37] that collects weak signals from nearby IoT devices, store, process data and results to higher-level servers while may act as an IoT device controller.

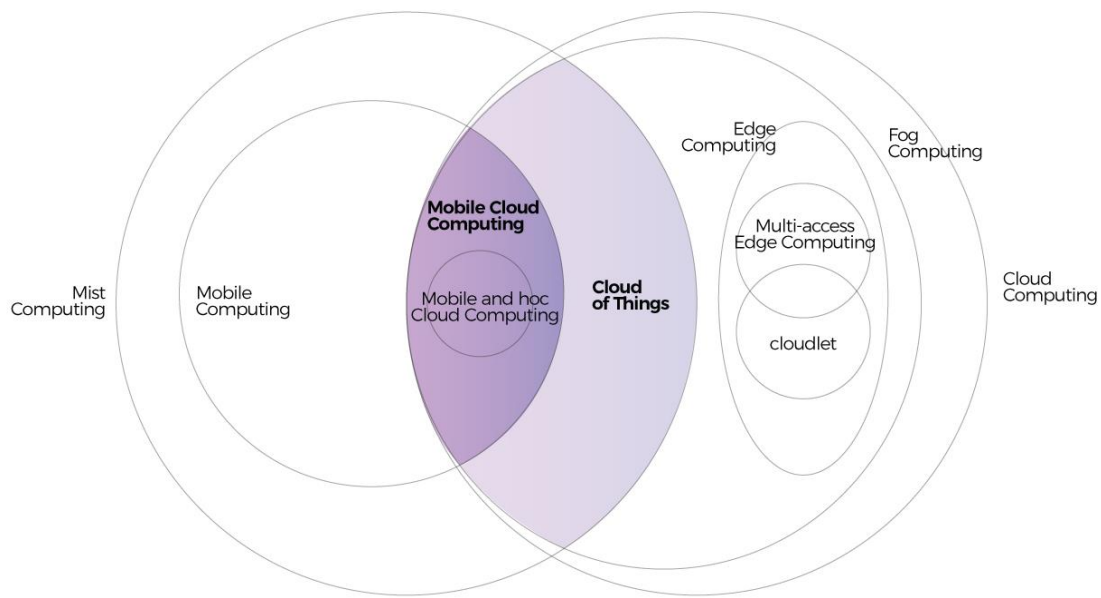


Figure 32. Venn diagram about paradigms, orientations and naming in edge computing [EDGE-31].

In the following pages, we aim at covering the basics of the three main implementation paths of edge computing. After a brief description, some technical details are included, accompanied with relevant deployment examples:

#### 3.1.3.1.1 Mobile -or Multi-access- Edge Computing (MEC):

The concept of Mobile Edge Computing has existed since 2013, when Nokia and IBM introduced the Radio Applications Cloud Server (RACS), an edge computing platform to be run by the servers in the base stations in 4G/LTE cellular networks. The new name (Multi-Access Edge Computing) has been recently adopted due to the enormous standardization efforts being done by the ETSI through one specific Industry Specification Group. As a relevant note, ETSI indicated as relevant the application of MEC to IoT scenarios in their whitepapers [EDGE-38], [EDGE-39] and [EDGE-40].

The basis behind MEC is to allow computation in cellular networks to be performed closer to the mobile device (at the edge), allowing thus to reduce latency in a highly location aware environment. In 3G networks, the MEC takes place at the Radio Network Controller (RNC), whereas in 4G networks it is encapsulated in eNodeB stations and, in the almost-ready 5G landscape [EDGE-41] in the gNodeB nodes. One of the main advantages of MEC is that the edge server (when deciding the offloading) will have accurate, real-time information on all network parameters including load and capacity while being at the same time aware of the end devices characteristics.

The first architecture reference for Mobile Edge Computing was delivered in [EDGE-42] in 2014. From then one, the most relevant initiatives that have been detected are: FemtoClouds [EDGE-43], REPLISOM [EDGE-44] and CloudAware [EDGE-45], all of them leveraging 4G edge and backhaul infrastructure.

Afterwards (2015), the concept of Central Office Rearchitected as a Datacenter (CORD) appeared [EDGE-46]. It consists of a solution suited for telecom operators for leveraging new technologies like SDN and NFV in their base stations for providing mobile edge computing capabilities. The reference architecture of CORD bases on three pillars: commodity hardware (servers at the MEC equipment in the base station), and SDN kernel to



control the underlying devices and a virtualization management platform to control the virtualized functions being executed in the edge of the cellular network. One of the main promoters of this approach is Telefonica, which with their initiative OnLife [EDGE-47] putting together CORD and open compute concepts and validating them in real pilots. Valuable lessons learned are being extracted that ASSIST-IoT will be observing.

Despite the recent advent, no proper demonstrators have been found on the MEC-IoT deployments in 5G. According to the specifications by the ETSI group [EDGE-48], a MEC has **an accessible API through which application developers can interact to put in place MEC deployments in their 5G networks.**

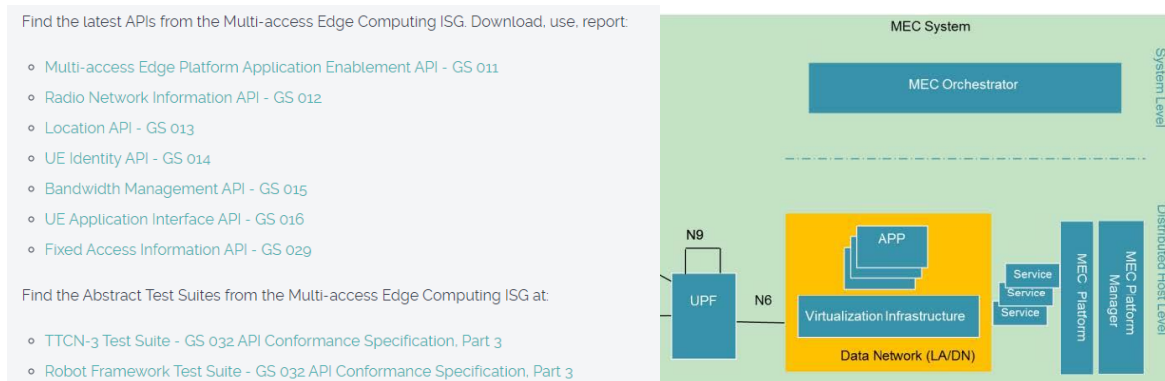


Figure 33. ETSI specification architecture and API for MEC in 5G.

In the context of ASSIST-IoT, Multi-access Edge Computing will only be tackled in one specific scenario of the Automotive pilot, when different cars (ECUs and other information included) will connect **via 5G** to an experimental base station. Therefore, **the reference architecture (T3.5) will consider** the mechanisms and implementations used in MEC **from a pure IoT point of view.**

### 3.1.3.1.2 Cloudlets

This term, coined by Prof. M. Satyanarayanan from Carnegie Mellon University in 2014 [EDGE-48], refers to those implementations that **create small data centres at the edge of the network** (cloud in a box) [EDGE-49]. The cloudlets aim at working exactly the same way than the classic clouds do (e.g., AWS, Azure, OpenStack), being articulated as a second level -closer to the data source- with cached stated imitating the cloud level but geographically dispersed. Cloudlets appeared to respond the needs of edge computing for mobile applications **without being constrained to run only in cell towers.**

Cloudlets represent the middle layer of a three-layer hierarchy (following literally the edge computing overall approach) that includes data-generators (in the case of ASSIST-IoT, mainly IoT sensors), cloudlet and centralised cloud-computing facilities. The design of the cloudlet approach spots this middle-layer to be materialised in servers (or cluster of servers) co-located with WiFi-Access Points (APs) or Smart Routers in surrounding physical environment.

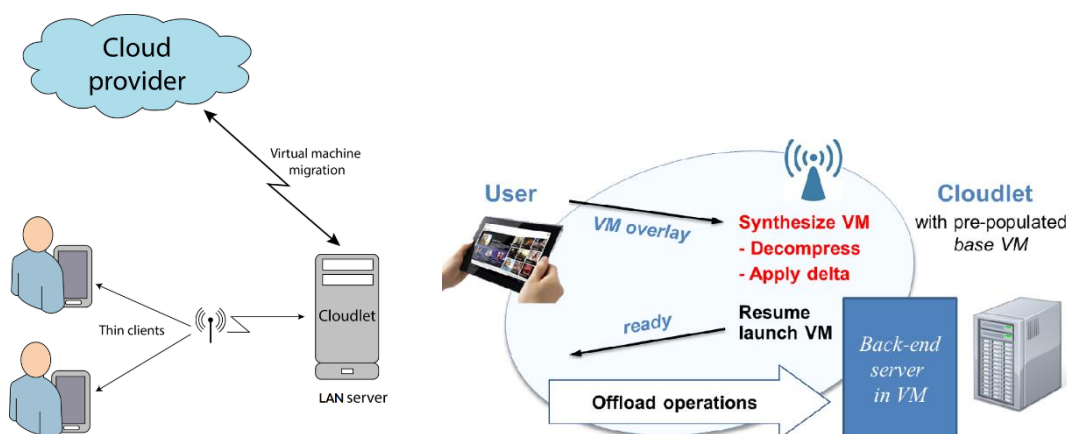


Figure 34. Left: Cloudlet illustrative diagram [EDGE-127].

Right: Offloading basics in a cloudlet schema [EDGE-126]

The objective of the cloudlets is to offload part of the work from the centralized cloud computing servers by replicating the capabilities of those (VM machines provision, on-demand pay as-you-go business models, availability, scalability, resource efficiency, multi-tenancy, and energy efficiency) in a logically and physically near trusted, resourceful local server acting on their behalf [EDGE-50].

To do so, the cloudlet is paired with the cloud server in the sense that, whenever a mobile device requests a service, part of the workload is offloaded to the cloudlet to improve latency avoiding end-to-end roundtrip as well as improving security. That way, devices requiring computation-intensive applications (e.g., Augmented Reality, face recognition) will seamlessly have better QoE than if relying in a traditional CC approach.

This type of implementation is modelled by the following attributes:

- (i) A cloudlet exists at physical, and foremost logical (one-hop) proximity to a mobile device, accessible via WiFi - high speed wireless connection.
- (ii) A cloudlet is a dedicated server (or cluster of servers) considerably rich in computation resources.
- (iii) Cloudlets are designed to be standalone devices connected to the cloud.
- (iv) A cloudlet uses pre-populated virtual machines (VMs) to provide resources for the end devices in real time. After receiving the request, the cloudlet decrypts the information, applies the base VM (Cloudlet agent) and launches the proper VM to perform the offloading. **Computation offloading and data caching** are the key technological concepts in this process [EDGE-51].
- (v) It is soft state only, which means that it is installed and thereafter it is self-managed, without the need of intervening further. This implies establishing contracts with cloud services providers and relying on them to hold the service.
- (vi) The cloudlets take a robust and powerful internet connection for granted. Being more in the “ISP side” rather than on the “user side”, a wired connection to the backhaul network is present in the “northbound” of a cloudlet.
- (vii) Each cloudlet has functionality that is specific to its cloudlet role.

The strongest **advantage** that the cloudlet model has against CC is avoiding the pitfalls of WAN latency. About this latency reduction, some evidence has been found that, depending on the cloudlet system setting, 20-times better performance can be reached. For small size entities, a cloudlet solution can be an optimal pick also with regard to deployment cost [EDGE-52]. Another advantage of the cloudlets is damage minimization of loss of data, considering that the information transferred to the cloudlet is soft state cached from the CC. It has been documented that cloudlet system show good performance in hostile environments [EDGE-53]. In similar studies, it was reasoned that using cloudlet approaches the energy consumption of the end-to-end process for computing a cloud application decreased considerably, having as well positive effects on the associated carbon footprint. As of today, commercial servers that can be attached to APs and even Smart Routers still have a considerable computing advantage against mobile devices (e.g., smartphones, tablets), thus the cloudlet-based schema (computation offloading) hold great potential to cover computer-intensive emerging applications in the mobile computing landscape.

On the other hand, cloudlets present some **disadvantages**. This approach entails the establishment of complex mechanisms of computation and data offloading, implying the need to negotiate with the CC provider the specific service scope that can be derived to the cloudlets. Additionally, because the cloudlet provider’s (which will range from on-premises IT departments to off-premises data centres, passing through ISP providers [EDGE-54]) budget is limited, it is very difficult to have a solid, consolidated global infrastructure of cloudlets in all locations of a network, which should be the objective to ensure “seamless latency experience” to the mobile users.

The main promoter of cloudlets since their infancy was the Carnegie Mellon University (CMU [EDGE-55], [EDGE-56]), which has been conducting research through the Open Edge Computing Initiative [EDGE-57], formed by several relevant industrial and academic members. Since their first proposals were published [EDGE-58], **two main architectural approaches** for cloudlets can be distinguished: transient cloud and mobile cloud (or mesh) [EDGE-59].

- Transient cloud architecture [EDGE-60] (see Figure 34) is the most common approach, in which one (or a cluster of) server (s) form the cloudlet that oversees offloading CC work before the centric computing element. In this architecture, a mobile device connects to the Cloudlet within the WLAN which takes care of providing requested resources.
- Mobile cloud (or mesh) architecture [EDGE-61] relies on a mesh network of cloudlets (each of them with its OS and capabilities) that can be fixed servers (as in transient) or mobile devices (e.g., a tablet). Those cloudlets (see Figure 35) are physically spread and might be working in Manager or Worker node modes, taking charge of the caching and load balancing among them allowing a distribution of the offloaded tasks. This architecture has gained popularity over the past few years due to the increasing computing capacity of modern mobile devices.

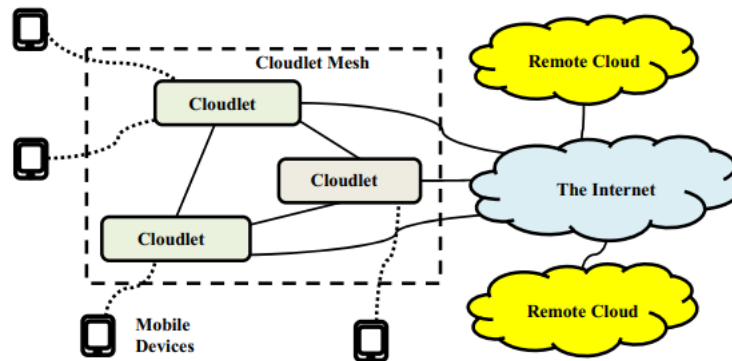


Figure 35. Mobile cloud (or mesh) architecture [EDGE-127].

Exploring the literature, many frameworks have appeared over the last years for the deployment of cloudlets to cover CC services. The first reference back from 2012 is MOCHA [EDGE-62], which bases on a transient architecture that just tested tiny processing in the three computing levels (lightweight processing, dynamic partitioning and parallel processing correspondingly). A test of this framework took place in the so-called Cloud-Vision [EDGE-63] that was based on custom development in all levels over a client-server application and almost trivial selection and task offloading algorithms over a Windows-7-personal-computer cloudlet. MAUI [EDGE-64] advanced the same line of work by introducing sophistication in the offloading mechanisms, reaching great levels of performance and energy consumption decrease, but with the problem of being only valid for applications running in .NET. CloneCloud [EDGE-65], instead, solved the problem of application-language-dependency by creating a “clone” of the mobile device in the cloudlet, synchronised periodically with the CC service. However, the issue of multithreading remained. Later, Pocket Cloudlet, which consisted of a cloudlet element that cached content (data) from cloud services close to end users according to their historic behaviour, drawing from previous ideas [EDGE-66]. ThinkAir [EDGE-67] was the first framework driving towards mesh-oriented architecture of cloudlets, dividing the offloading problem calculation into sub-problems to be executed in different VMs hosted in the own mobile devices. CACTSE [EDGE-68] follows a similar structure than CloneCloud but based on ThinkAir’s structure, rooting its functioning on a peer-to-peer interaction between mobile devices for specific content staging with the help of a Service Manager. OPENi Cloudlet [EDGE-69] framework was created out of a European research project in 2014 with special purpose of data staging in a near-end location. However, this line of advance was not followed as it required the existence of an adaptable, dynamic protocol for data exchange between the cloud and cloudlets. Afterwards, in 2015, GigaSight was proposed [EDGE-70] consisting of a transient-type architecture powered by virtual machine (VM)-based cloudlets. The approach followed was to assume that all cloudlets have VirtualBox [EDGE-71] and a guest OS installed so that they would be able to be managed as a distributed set of VMs to execute computing.

Drawing from the previous frameworks and making use of varied base technology and offloading algorithms, several (not many though) **actual implementations of cloudlets** can be observed in the **research/open-community field**. Two of those implementations of cloudlets came out of Prof. Satyanarayanan’s lab through a tight cooperation with OpenStack [EDGE-72]. The most relevant official outcome of Open Edge Computing initiative is Elijah [EDGE-73] (also known as OpenStack++) which has been created based on extensions of OpenStack including cloudlet discovery, just-in-time provisioning, and VM hand-off. Gabriel [EDGE-74] is a PaaS (Platform as a Service) based on the implementation of Elijah cloudlets for specific services related to

wearable cognitive assistance. Another example of using Elijah is QuiltView [EDGE-75], a crowd-sourced video response system. The second one is Meghdwar [EDGE-76], which instead of replicating and tailoring CC performance, follows the VM-synthesis approach also building upon OpenStack components. Another relevant implementation found was Pytos [EDGE-77], which builds on MAUI framework to provide libraries and software artefacts to run single-server cloudlets following a client-server model.

As a side note, although not exactly falling under the cloudlet's category, a current trend to bring CC capabilities to the edge, some interesting initiatives are emerging based on allocating specific functions execution in any capable hardware along the near-end network. Two relevant examples of this approach are Amazon AWS Lambda functions [EDGE-78] and OpenNebula [EDGE-79] (coming from the H2020 project OneEdge [EDGE-80]). These technologies rely on the capacity of such hardware to run containerised software.

However, to the best of our knowledge, **only one company** has shown a strong commitment in delivering a **serious commercial offer of cloudlet software**: Akamai [EDGE-81]. As mentioned in the characteristics list, one cloudlet is just designed to cover the specific role assigned to it. Aiming at covering a wide range of pre-CC services, Akamai offers a suite of nine different cloudlets to provide different services like visitor prioritization, application load balancer, API prioritization or audience segmentation.

As it has been outlined before, cloudlets are designed to run at resource-rich, one-hop locations from endpoint mobile devices. In the experiments, equipment like personal computer and Ubuntu servers close to WiFi hotspots have been the most common instantiation hosts of cloudlets. Other creative equipment used to explore cloudlet approach have been cluster of single-board-computers, like the one proposed in [EDGE-82] using Raspberry Pis and using modern Smart Routers like Xiaomi [EDGE-83], [EDGE-84].

According to the ASSIST-IoT WP3's team, the most worrying obstacle hindering cloudlet massive deployment is the overwhelming variety of implementations (most experimental) without a clear reference. The lack of a "killer app" for cloudlet-based mobile computing is preventing this paradigm to permeate the "edge computing" environment [EDGE-85], [EDGE-86].

Open research points in cloudlets are (among others), how to properly allocate resources (VMs) for received requests to optimize latency and efficiency [EDGE-87], how to properly pick cloudlet deployment spots [EDGE-88], how mobility affects the cloudlet handoff – when a mobile user shifts network connection – or how to enhance the questioned security of cloudlet deployments.

There is **no need to apply cloudlet schemas to solve ASSIST-IoT use-cases**. Hence, initially, this approach will not be considered to be part of ASSIST-IoT. However, the mesh distribution and the overall concepts of data and computation offloading in cloudlets **will be considered in T3.5** to be part of the reference architecture (RA) to be delivered out of the project.

### 3.1.3.1.3 Fog computing

This term was firstly introduced by F. Bonomi – from Cisco- in 2012 [EDGE-89]. The roots of this definition are the **implementation of "fog nodes" across the edge-cloud-computing continuum** to improve CCs shortcomings in IoT applications. According to NIST, "*Fog computing is a layered model for enabling ubiquitous access to a **shared continuum of scalable computing resources***" [EDGE-90]. Another interesting definition, which ASSIST-IoT team feels comfortable with, was outlined in [EDGE-91]: "*we envision fog as a bridge between the cloud and the edge of the network that aims to facilitate the deployment of the newly emerging IoT applications*". The objective is to deploy computing power in (potentially more than one) closer locations to the source while applying IoT concepts to upper layers in the network architecture, thus enhancing IoT infrastructure scalability.

As indicated in the first page of ASSIST-IoT proposal, this project focuses on the edge-fog-cloud continuum model applied to IoT scenarios. In that context, ASSIST-IoT will be using the word "edge" to address related ambitions, more specifically **via the "fog computing" approach**.

In contrast to the other implementations (see above), fog computing is associated to IoT scenarios and applications, evolving considering requirements thereof. Such architecture requires that processing to be embedded both directly within endpoints - "things"- (e.g., sensors), controllers or other equipment in nearby aggregation locations such as gateways/hubs. Hence, fog computing tends to be diagrammed as a multi-level scenario where data processing can be (dynamically) stretched through multiple locations along the network.



In the fog computing approach, the “edge workload” is always executed by **fog nodes deployed in one or more heterogeneous hardware** (e.g., laptop, Raspberry Pi [EDGE-92] local server, etc.) **that must be orchestrated** according to node resources and other. Each fog node is a highly virtualized software component tantamount to an IoT node that acts as gateway and a local computing resource. The “fog node” reduces the workload of computing to be carried out by the central element, depending on its resources and availability [EDGE-93]. This implementation type also characterizes for scarcity of computing resources in those fog nodes (vis-à-vis CC or cloudlets).

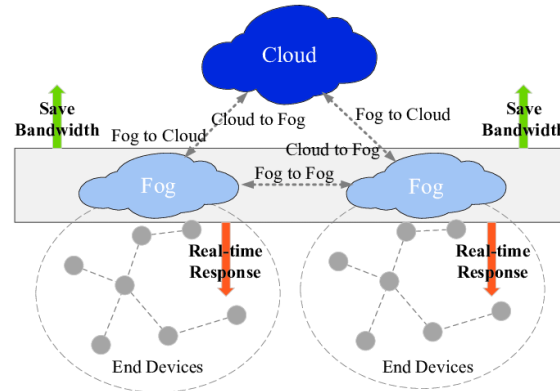


Figure 36. Fog computing structure basis [EDGE-127].

Besides, fog computing presents a key difference with the rest of “edge computing” approaches. Apart from the classic upwards-downwards communication among device-edge-cloud levels (in FC, fog-to-cloud, and cloud-to-fog), fog computing allows fog nodes (near-end level of the architecture) to cooperate and communicate with each other forming a network (fog-to-fog) [EDGE-94]. Thus, a fog computing deployment can be working in a centralized or de-centralized manner, having the nodes configured as stand-alone (the former case) or federated (the latter case), interacting among them thus providing horizontal scalability.

Like the review done for cloudlets, fog computing has a series of features that make this approach easily recognizable:

- The actual edge computing is carried out by fog nodes, that can be located anywhere between the device and the cloud layer
- FC is not constrained to a resource-rich server. It is designed to leverage any available computing resource along the edge-to-cloud-continuum.
- It can work in a centralized (fog-to-cloud) or decentralized (fog-to-fog) mode.
- It supports varied access networks, not constrained to mobile or WiFi, but allowing classic IoT protocols like Zigbee or Bluetooth to be extended to.
- It is the approach with less dependency to specific, purpose-devoted hardware. A fog node can run in a wide variety of devices leveraging virtualization techniques.
- Fog nodes are prepared to support many communication protocols, including mobility considerations like LISP [EDGE-95].
- There is a predominance of wireless access. Being designed to support IoT cases, wireless sensors will clearly benefit from FC traits.

Using fog computing against traditional CC services **provides substantial advantages**. Among the most relevant traits, the latency outstands. The FC offers the best **latency** in comparison to the rest of approaches as it does not need to rely on resource-rich computing components to be performed, in FC the “edge node” might be found in a **geographically close** computing device (e.g., Arduino, RPi) nearby the IoT endpoint, being usually co-located with them [EDGE-96]. This physical proximity also allows, in the lowest fog layers, to highly perform location-aware computing. Not being constrained to specific servers (like cloudlets or MEC in base stations), makes FC able to cope with the current **heterogeneity** of equipment in Industry and other sectors (e.g. Smart City). In one FC deployment, there may exist and interact data coming from multiple sources, in multiple



formats and passing through motley equipment (from legacy to well-equipped machines) making use of various communication standards (e.g., MQTT, ZigBee, BLE, TCP, HTTP, WiFi). Different from cloudlets (which are focused on data and computation offloading associated to batch operations), fog computing is specially oriented to deal with stream data flows, attaching therefore to the **real-time processing mechanism**. Other essential traits of fog computing are **scalability, modularity, and flexibility**. According to the different references, a “fog node” makes use of virtualization and containerisation technologies (e.g., Docker [EDGE-97]), leveraging a smooth deployment of ad-hoc components on-the-fly. This flexibility is also expressed by the capacity of FC to create specific deployments depending on available hardware, software, and communication protocols [EDGE-98]. Moreover, the flexibility is also present in the time axis, being dynamically adaptive to re-formulate fog-to-fog interactions, elastic computation, resource pooling and data-loads to be taken by each node depending on network conditions or other requirements. Last but not least, **security** is clearly enhanced with FC, which deployment may include specific security rules to be applied in each node, falling under authentication, encryption, filtering and others.

Reviewing the literature, many works on fog computing architectures are found, increasing since 2015 on. Two fabulous articles were published in 2018 [EDGE-99] and 2020 [EDGE-100] reviewing the different proposals outlined in the literature. The most remarkable were: (i) the Cisco-Bonomi reference architecture, which is the seed of the fog computing definition, just provided a bird’s eye look of potential FC materialisation, hugely relying on APIs between layers. (ii) the CLOUDS lab architecture [EDGE-101] which defines five layers (access, network, cloud services, vertical applications, and software-defined resources management), clearly focusing on the resource management from a centralized location. (iii) The AUT RA [EDGE-102] is a recent proposal that tries to align FC with the NFV (ETSI) and SDN (ONF) standards, including the interfaces based on OpenStack open APIs. (iv) SORTS [EDGE-103] is a very comprehensive reference that will be taken into account for ASSIST-IoT, which functioning is based on several managers (Communication, Security, Status Planner, Resources Orchestration) divided in three layers of fog instances.

However, despite existing a wide variety of approaches, **one reference architecture prevails above the rest**: the OpenFog RA [EDGE-102] proposed by the OpenFog Consortium [EDGE-104]. According to their definition: “*The OpenFog RA describes a generic fog platform that is designed to be applicable to any vertical market or application*”, in which Smart Cities, Transportation, Visual Security and Surveillance and Smart Buildings are included as representative examples. The OpenFog RA is structured in pillars (security, scalability, openness, autonomy, programmability, reliability, agility, and hierarchy) which can be roughly mapped to all FC traits described above.

The OpenFog RA structures a FC deployment as an N-tiers of fog nodes that interact together to form a complete system. Depending on the requirements of the use-cases, the number of layers must be determined according to the available resources. The reference architecture includes several layers, perspectives or cross cutting concerns, and views to enable a FC implementation. The OpenFog RA is illustrated in Figure 37.

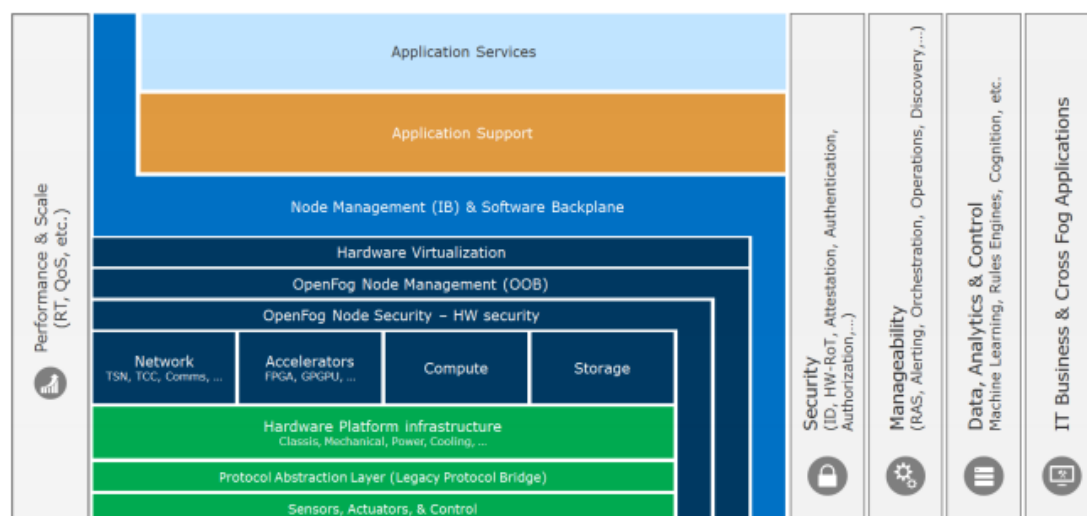


Figure 37. OpenFog Reference Architecture. Extracted verbatim from the official specification [EDGE-102].

According to OpenFog, a FC system is composed by a platform (including all layers, functionalities and modules in Figure 37) that is instantiated (with modular flexibility) differently in various fog nodes. Whereas a fog platform includes transversal software like manageability, application specificities, security control and data analytics, the basic fog node implementation just needs to include network capacities, accelerator, computing ability and storage capacity, as well as basic security mechanisms and a node management interface for interacting with the centric element (fog-cloud) or other nodes (fog-fog). This way, the **fog platform** (to be instantiated in a fog node or in the centric element) coupled with the fog software basics form the OpenFog reference fog node. One or more fog nodes compose the global FC system [EDGE-105].

The image below represents an abstraction of a fog node basic software as provided by the OpenFog reference architecture:

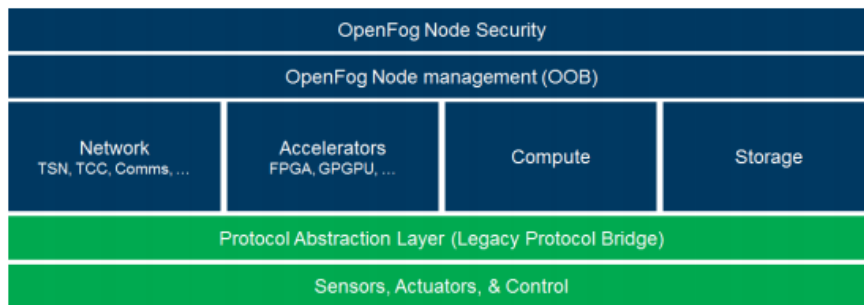


Figure 38. Fog node basics software according to OpenFog RA.

The concept of “**fog node**” is not original nor unique of the OpenFog RA. All FC approaches and deployments rely on the creation of fog nodes that carry out the fog computing workload. In all found implementations, the fog nodes always meet a clear set of requirements: (i) they have the capability of being autonomous, making local decisions at the node level, (ii) they are modularly heterogeneous, being able to implement all or some modules of a fog platform, (iii) they are always structured in a hierarchical way, that can be vertical or horizontal, (iv) they mandatorily include manageability capabilities, namely resources orchestration and/or federation, (v) high programmability level, as they can be addressed to solve specific problems that may need custom development from diverse actors.

According to the NIST [EDGE-106], the fog nodes can be classified in four “deployment modes” looking at their situation in the network and other characteristics:

- (1) Private fog node, existing within organizations to provide specific services that can only be leveraged for and by business’ purposes (e.g., an industrial edge node processing data from a manufacturing lane).
- (2) Community fog node, which usage and configuration are shared among a closed community with specific purposes (e.g., smart gateways pre-processing video at a football stadium).
- (3) Public fog node, which usage and access are open to the general public. It is normally managed by one public organization that afterwards allows using associated data and capabilities (e.g., computing unit placed in a light post for Smart City purposes).
- (4) Hybrid fog node.

The deployment of fog computing is gaining traction as paramount objective for covering the needs of the next generation of IoT applications. Reviewing the literature, we have found many examples of (mostly, experimental) fog deployments. Additionally, research projects (see section 3.1.3.2) are increasingly focusing on this approach.

Here below, we list the most relevant **fog platforms (including fog node) implementations and examples of fog computing deployments** that will be observed for the work in ASSIST-IoT (WP4). Other might be related but for the sake of conciseness those have been dismissed:

- Cisco IOx [EDGE-107]. The first fog computing platform put in place in the reality was IOx by Cisco, defined by them as “an application enablement framework for the IoT”. The basis of this

implementation was to host execution of services in Linux-based computing equipment along the network continuum using a host OS and Virtual Machines to run specific functions.

- ParaDrop [EDGE-108], coming from the University of Wisconsin-Madison [EDGE-109], was one of the earliest open software deployments of fog computing, initially designed to run within WiFi Access Points. It proposed a very modular specification to be leveraged by multiple actors via APIs. Like Cisco IOx, Paradrop required Linux OS hosts but building on top of native Linux container deployment instead of VMs. Another difference is that ParaDrop (in later versions) includes fog-to-fog capabilities as well.
- The Linux Foundation is currently in the phase of unifying some projects into the frame of “LF Edge” [EDGE-110] initiative, which aim is to establish an open, interoperable framework for edge computing to be hardware independent. This approach aims at decoupling the traditional separation in order to become the reference for open edge implementation.
  - EdgeX Foundry [EDGE-111] is the framework being created by the Linux Foundation to all-encompassing deploy fog computing services. According to their website: *“Is a highly flexible and scalable open source framework that facilitates interoperability between devices and applications at the IoT edge”*. In the reality, EdgeX Foundry is composed of a suite of open-source tools that aim to tackle specific functionalities that, together, form their fog computing platform architecture.

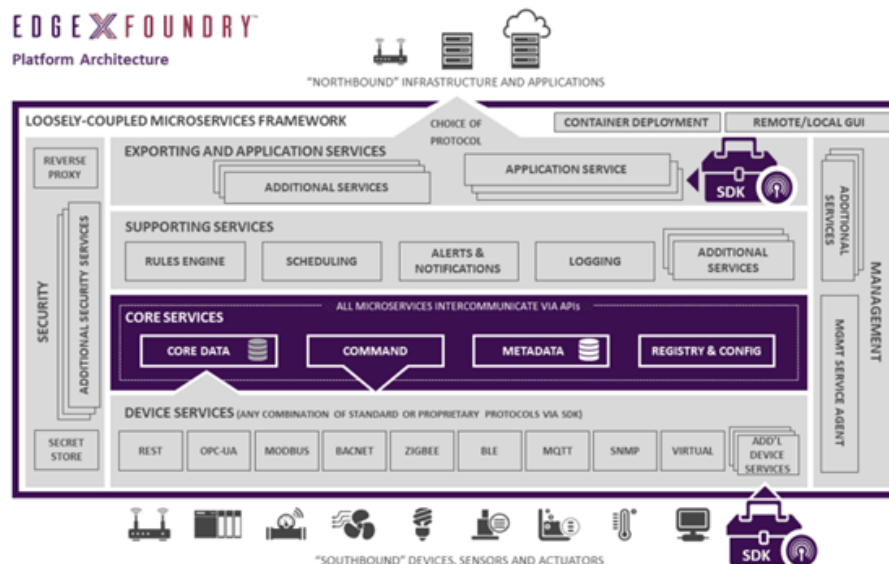


Figure 39. EdgeX Foundry fog computing platform.

- FogLAMP – Fledge [EDGE-112] currently named Fledge after adhering to the Linux Foundation initiative just mentioned. Fledge aims at being the **“basic fog node” implementation** preferred to comply with the EdgeX platform specification. According to their own definition: *“Fledge is an open source framework and community for the industrial edge focused on critical operations, predictive maintenance, situational awareness and safety”*. It bases functioning on fog nodes that can be managed and used by applications through an API and can grow on their capacities by adding specific northbound, southbound or inner processing plugins. Fledge will be one of the references to be considered prominently for ASSIST-IoT deployments.

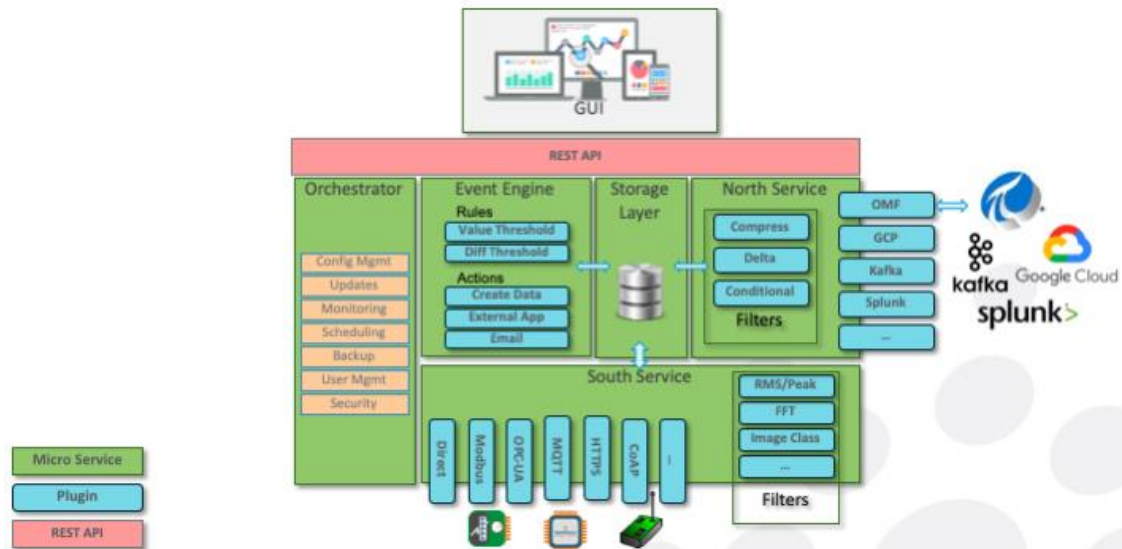


Figure 40. Fog node implementation for EdgeX: Fledge [EDGE-112]

- FogAtlas [EDGE-113] (coming from the former FoggyPlatform) is a framework for fog computing implementation oriented to provide “zero-touch” (plug-and-play) in edge devices when aiming at IaaS and PaaS service provision. installation). In contrast to the previous examples, FogAtlas does not aim to provide a “fog node basic software implementation”. Instead, what FogAtlas provides is an unambiguous software for orchestrating fog nodes, managing them as virtualised resources. The FogAtlas specification is divided into modules relying on open source technologies like OpenStack, Docker, Kubernetes and Ansible, Prometheus and Grafana. FogAtlas will be carefully observed in ASSIST-IoT as it is being positioned as the reference tool to be using in European research projects.

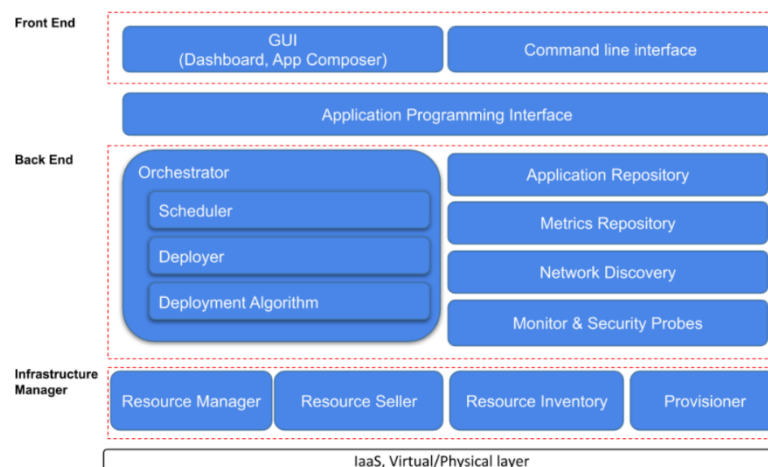


Figure 41. FogAtlas platform architecture.

- Fog05: As a recent contribution (May, 2020), Eclipse launched the first release of its “fog05” solution [EDGE-114]. This contribution will be carefully observed by ASSIST-IoT as this open-source community has been lately providing successful prototypes for fog computing in 5G. Like Paradrop, is based on LXD containers and integration with Kubernetes but following only the decentralized approach mode. It aims at providing Infrastructure-as-a-Service (LXD containers running in Linux machines) close to the source of the data. The fog05 nodes include capabilities for Infrastructure Management and Resources Provision.
- INTER-IoT edge node as part of an IoT Gateway. One of the partners of ASSIST-IoT (UPV) was in charge, in the project INTER-IoT [EDGE-115], to develop an IoT gateway capable of attach functions close to the IoT data source that should be executed in a physical light-weight computing device (e.g., RPi). This product is especially relevant as it introduced a new paradigm for IoT Gateways that adjusts to this new communication pattern: the dual Physical-Virtual IoT Gateway, communicated via web

sockets. While the virtual part is placed in the “cloud” layer of an “edge computing structure”, the physical capabilities fit exactly the role of fog nodes. A picture of its structure is depicted in the following figure:

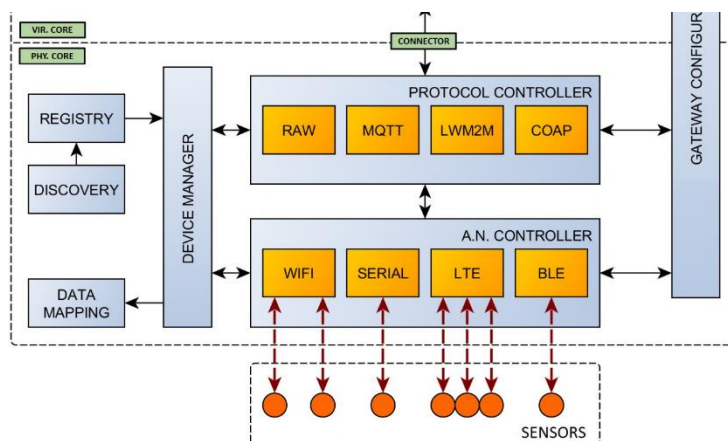


Figure 42. Physical IoT gateway from INTER-IoT as potential fog node.

Finally, as fog computing will be the approach to mostly consider in ASSIST-IoT, we have included below some hints on the current research challenges and other relevant aspects that the WP4 team will need to consider.

A limitation commonly presented in all the previous is the impossibility of creating a hybrid cloud-fog services scheme, as currently there is a lack of consolidated frameworks for fog federation [EDGE-116]. In this sense, it has been noted that the dispersion inherent in fog computing creates added difficulties in the management of data and processing in the nodes. To achieve scalability and interoperability in this regards, open APIs, ontologies and standard description languages need to be worked over at this point.

Another observation in the state of the art is the lack of an established framework to enable **fog resource management and monitoring** [EDGE-117] and scalable multi-objective dynamic fog system re-configuration (bandwidth, waiting time, availability, security, energy and bandwidth). Achieving this would mean an advance in the state of the art. Some actions in the past have suggested as an option to build upon OpenStack components incorporating enriched semantic reasoning and filtering. Another useful concept to achieve the previous is the SDN application in fog nodes. The current SDN open-source implementation (OpenFlow [EDGE-118]) does not natively support fog computing. Fog Federation [EDGE-119]. Building upon Kubernetes stack, it has been lately identifying the need here to advance for enabling computing sharing possible, considering that fog nodes must not be limited to one vertical/service thread, being able to simultaneously host several applications from several vendors/consumers. In this regard, although new initiatives are being published in the literature relying on Kubernetes CRD [EDGE-120], like StarlingX [EDGE-121], KubeEdge [EDGE-122], and Kubefed [EDGE-123], this line of work has seemed not to be evolving too much since 2018.

### 3.1.3.2 Relevant initiatives

About standardization entities:

Table 13. Edge/Fog computing standardization entities.

Standardization Entity	Reference Number	Implementation type	Comments
ISO/IEC	JTC-1 SC-41	Fog computing	Recent advent, following a mixed approach, not widely spread. To be observed.
ETSI	MEC 003	Mobile Edge Computing	ETSI MEC “MEC-in-NFV” reference architecture in ETSI Group Specification MEC 003.
ISO / IEC	JTC-1 SC38	Cloudlets	Based on the definitions by CMU.
NIST	NIST SP 500-325	Fog computing	American reference, it does not specify a clear architecture but just describes global concepts.



About relevant products, industrial alliances and open source initiatives, those have been mentioned during the previous text. With summarising purposes, the crucial references to be observed are:

*Table 14. Edge/Fog computing alliances.*

Company / Alliance	Business orientation	Comments
Linux Foundation	Open source	LFEdge initiative, tackled by the EdgeX Foundry ecosystem.
Open Stack [EDGE-124]	Open source	OpenStack++ initiative aims at creating an open ecosystem in which investments might be put on to establish enough cloudlets infrastructure to actually permeate the IT landscape.
OpenFog Consortium	Industrial (CISCO, Microsoft, DELL) and Academia (Princeton)	Focus on open models for fog computing across the entire IoT ecosystem, generating a relevant reference architecture.
OpenEdge Consortium	Industrial (NTT, CMU, Verizon) and Academia (CMU)	Focused on the advance of Cloudlets. Creators of Elijah, Gabriel and QiltView. Offering a Living Edge Lab for testing cloudlet applications [EDGE-125].
Edge Computing Consortium	Industrial (HUAWEI, INTEL)	Focused on MEC. Aligned with ETSI specifications and working on the APIs provided to leverage RAN base stations.
Industrial Internet Consortium	Industrial	Aligned with the MEC concepts. Involved in the CORD initiative mentioned.

Finally, there is a lot of movement in the public-funded research field in the edge computing area. Finished activities might provide an outline of what is still to be achieved, establishing a base to build on. A set of very interesting actions are projected to end in 2021 (awarded out of ICT-12-2018 call and previous). Some of their objectives are pretty aligned with ASSIST-IoT goals concerning edge/fog computing, thus a special attention will be paid during the first months (task T3.5) to leverage results and learn from lessons. After, other relevant projects have been identified that will be running in parallel with ASSIST-IoT. WP3 team believes that positive synergies may be built and, whenever possible, cross-learning will be fostered via knowledge exchange.

*Table 15. Edge/Fog computing research projects.*

Project	Orientation	Pilot Domains	Comments
<u>LightKone</u> 2018-2021 GA: 732505	Aims at solving some of the problems in generic-purpose edge computing by combining synchronisation-free programming and hybrid gossip algorithms.	New industrial applications and a startup company	Based on OpenFog RA, LightKone will be observed carefully by ASSIST-IoT members. Specially relevant is the new approach designed for data management in fog nodes.
<u>CLASS</u> 2018-2021 GA: 780622	Definition of RA for Big Data stream and at-rest analysis anywhere in the continuum based on a development framework for programming applications in a serverless cloud computing approach.	Several use-cases (traffic, parking, air pollution) in the city of Modena.	Not focused on any particular edge computing implementation, seems interesting to explore the serverless functions using Apache OpenWhisk [EDGE-73] based components and their Container-as-a-Service paradigm.
<u>DECENTER</u> 2018-2021 GA: 815141	Creation of a fog computing platform for AI application-aware including orchestration, federation, resources provisioning and DLT with blockchain. Specific emphasis is put in SLA negotiation.	City crossing safety, Robotic logistics, Smart and safe construction site, ambient intelligence.	DECENTER has been an inspiration for this state-of-the-art. Focused on SLA and specific use-cases, ASSIST-IoT may take as basis the open-source components (FogAtlas, Kubernetes, Prometheus [EDGE-126] and techniques (complex graphs theory) used in DECENTER to implement the dynamic resources provision and orchestration of fog nodes.
<u>MF2C</u> 2018-2021	MF2C investigated an architectural approach to address the	Emergency in Smart Cities,	The approach based on fog agents is specially interesting for ASSIST-IoT.

Project	Orientation	Pilot Domains	Comments
GA: 730929	<b>management</b> of fog to cloud (F2C) computing systems.	Enriched navigation, fog'-hub for Telcos.	The technological details will be consulted in their GitHub for the development of task T4.2.
<u>FogGuru</u> 2018-2021 GA: 765452	A very practical-oriented project that aims at solving the issues on the resources orchestration and autonomous management of the current fog computing platforms.	Smart water management	Specially relevant for ASSIST-IoT will be the adaption of stream processing middlewares to fog computing environments based on Kubernetes and their guidelines on how to deploy a fog application.
PLEDGER 2018-2021 GA: 871536	The project provides toolkits to both the (infrastructure) providers and the application developers (adopters), bridging the chasm between their domain areas in an edge/fog computing deployment.	Mixed reality, vulnerable road, manufacturing	ASSIST-IoT will observe the technology used in PLEDGER to deploy the “black box” approach of the cloud applications in the edge on the eyes of the stakeholders using the system. The introduction of blockchain in the edge will also be realised.
ACCORDION 2018-2021 GA: 871793	The most relevant objective is to create an orchestrator that will be able to manipulate underlying edge VIMs and public clouds and network resources	-	ASSIST-IoT will analyse the deliverables of current orchestrators, its shortcomings and how to overcome them, reviewing the proposals by ACCORDION and looking for implementing a suitable orchestrator for the NGIoT requirements.
BRAINE 2018-2021 GA: 876967	BRAINE aims at developing an Edge MicroDataCenter to be the reference for cloudlet-based edge computing deployments. Specific focus is put in the security, data privacy and sovereignty.	Healthcare assisted living, smart city, robotics in Factory 4.0, and supply chain Industry 4.0	Being participated by key partners in the sector (NEC, vmware, windtre, Sant'Anna (leaders of FogAtlas), DELL...), the outcomes of BRAINE might be standard-caliber quality. Despite not being 100% aligned with ASSIST-IoT approaches, this Project will need to be observed carefully.
FORA 2018-2021 GA: 767485	This MSCA action is forming PhDs in the field of edge/fog computing at 7 universities across Europe.	Robotics and Industrial automation	ASSIST-IoT will observe the results (intermediate outcomes, final theses) of the young scientists with specific focuses on our tackled verticals: automotive, maritime transport and construction.
ONEedge 2018-2021 GA: 880412	SME Instrument-funded enterprise ONEedge commercialises and advances the all-encompassing fog computing framework OpenNebula. It is supported by LFEde and GAIA-X.	-	OpenNebula is focused on cloud features provisioning for edge applications, falling under the “cloudlet” category. It seems to be supported by relevant stakeholders, therefore ASSIST-IoT will be willing to adopt some of their axioms to be applied to an open NGIoT environment without relying on AWS Greengrass platform.

### 3.1.4 Interoperability

Nowadays, there are a witnessing significant growth in data produced by IoT based sensors. The growth of volume of unstructured data, sent by IoT devices, exceeds that of structured data. For that reason, many existing applications do not benefit from opportunities and flexibility offered by the existence of multiple data sources. As data grows and heterogeneity, issues of interoperability become a rising concern [INT-1]. The previous introductory text is focused on one of the main challenges of ASSIST-IoT, the interoperability. The way to face this challenge converges in more specific aspects of the project as: (i) The core enabler design and development. It must attend objectives like to provide an infrastructure for guaranteeing interoperability among services exported by IoT platforms and to allow data sharing. (ii) The architecture planes. The interoperability will be needed in different planes, but with different features. It will be treated comprehensively within horizontal planes and between them. (iii) The need of translation mechanisms for data interoperability. (iv) The use of global ontologies and semantic interoperability (v) The project pilots. They need to deal with the data standardization and interoperability, to homogenize the information provided by each pilot.

As can be observed, IoT and interoperability are two of the main concepts involved in ASSIST-IoT Project. The aim of this section is to provide a summary of the concepts and an overview of previous researches and works carried out in interoperability, and specifically, in the field of IoT interoperability.

#### Interoperability concept

There are many different definitions about the term interoperability. A common explanation is defining it as the ability of two or more software components to cooperate despite the differences in language, interface, and execution platform [INT-2]. The previous definition can be extended as, the ability of a computer system to run application programs from different vendors, and to interact with other computers across local or wide-area networks regardless of their physical architecture and operating systems. Interoperability is feasible through hardware and software components that conform to open standards such as those used for internet [INT-3].

In order to be interoperable, two or more systems must be able to exchange, interpret, and present shared data in a way that is understood by the other. Focusing on the ASSIST-IoT expectations, it is important to highlight that there are two types of data interoperability: syntactic interoperability and semantic interoperability. Firstly, the syntactic interoperability involves adopting a common data format and common data structure protocols. It is a prerequisite to semantic interoperability and enables different software components to cooperate, facilitating two or more systems to communicate and exchange data. Secondly, the semantic interoperability which refers to the ability of computer systems to exchange meaningful data with unambiguous, shared meaning. It involves the addition of metadata that links each data element to a controlled, shared vocabulary. Within this shared vocabulary are associated links to an ontology, which is a data model that represents a set of concepts within a domain and the relationships among those concepts [INT-4].

#### IoT interoperability

Focusing on the Internet of Things (IoT) environment, it can be observed that the definition of the concept IoT considers the interoperability as a key element. For example, the International Telecommunication Union (ITU<sup>22</sup>), one of the main Standard Developing Organisations (SDOs) in the field, defines IoT as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies [INT-5]. Thus, to achieve interoperability is one of the main objectives of the IoT. It is all about connecting things and make them easily accessible just like the Internet today. For that reason, broadly speaking, interoperability can be defined as a measure of the degree to which diverse systems, organizations, and/or individuals are able to work together to achieve a common goal [INT-6].

Even though there are barriers to the full realization of the Internet of Things (IoT) vision, as the lack of interoperability between IoT systems and applications. Many companies offer IoT systems to their customers, without perceiving any need to make them communicate with other such solutions. From the commercial perspective, expenditure of resources needed to support interoperability, outside of the existing solution, is often

---

<sup>22</sup> <https://www.itu.int/es/Pages/default.aspx>

perceived as unreasonable [INT-7]. In addition, the plethora of sensors, protocols, platforms, and applications is increasing the complexity of integrating different solutions.

### Standardization role

Considering the estimated growth of the IoT ecosystem and the growing need for interoperability of IoT solutions, standardization will play an important role in this context by promoting best practices, integration and interoperability of systems, privacy, and security requirements [INT-8]. Common standards ensure the interoperability because they guarantee that technologies work smoothly and reliably together, and it foster research and innovation. Effective interoperability guarantees that connected devices can communicate seamlessly with each other, regardless of manufacturer, operating system, or other technical components [INT-9].

#### 3.1.4.1 Scientific review

The scientific research highlights a substantial development of solutions for a wide range of devices and IoT platforms over the past last years. However, each solution provides its own infrastructure, devices, APIs, and data formats leading to interoperability issues. To benefit from the full potential of the IoT, objects do not just have to be simply connected to Internet, they must also be found, accessible, managed and connected potentially to other objects. To allow this interaction, one degree of interoperability is necessary which goes beyond the simple interoperability protocol such as supplied by the Internet [INT-10]. The interoperability issues are the consequence of many critical issues such as vendor lock-in, impossibility to develop IoT application exposing cross-platform and cross-domain, difficulty in plugging non-interoperable IoT devices into different IoT platforms and prevents the emergence of IoT technology at a large-scale. To deal with these issues the efforts by several academia, industry, and standardization bodies have emerged to help in IoT interoperability.

### Interoperability categorization

As previously explained, interoperability is a complex concept with multiple aspects to consider. The first task from the point of view of analyzing the existing material in literature is to narrow down and classify the elements addressed by the interoperability. There are some different classifications of the different aspects of interoperability, also called levels of interoperability. The classification called LCIM (Levels of Conceptual Interoperability Model) [INT-11]. There are seven levels from no interoperability to conceptual interoperability and they are notated from L0 to L6. The classification, created in the context of simulation theory, provide the following levels of interoperability:

- **Level 0 – No interoperability.** No connection and no interoperability.
- **Level 1 – Technical.** Have technical connection(s) and can exchange data between systems. The premise are common communication protocols (such as HTTP; TCP/IP; UDP/IP etc.) and the domain network connectivity.
- **Level 2 – Syntactic.** Have an agreed protocol to exchange the right forms of data in the right order, but the meaning of data elements is not established. The contents clearly defined are the format of the information exchanged (XML, SOAP; JSON, etc.).
- **Level 3 – Semantic.** Interoperating systems are exchanging a set of terms that they can semantically parse. The information defined are the meaning of the data and the content of information exchanged.
- **Level 4 – Pragmatic.** Interoperating systems will be aware of the context (system states and processes) and meaning of information being exchanged. The information defined are the use of the data and the context of information exchanged.
- **Level 5 – Dynamic.** Interoperating systems can re-orient information production and consumption based on understood changes to meaning, due to changing context as time increases. The information defined are the effect of the data and the effect of information exchanged.
- **Level 6 – Conceptual.** Interoperating systems at this level are completely aware of each other's information, processes, contexts, and modeling assumptions. It is focused on the composability and the modeling abstraction domain. The information defined are assumptions, constraints, etc. and the contents defined are a documented conceptual model.

The European interoperability framework for Pan-European e- government services [INT-12] defines three levels: technical, semantic, and organizational interoperability. However, a more related with IoT classification is provided by ETSI and AIOTI [INT-13]. It defines four levels: technical, syntactic, semantic, and organizational interoperability.

- **Technical Interoperability.** It is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. It is often centered on communication protocols and the infrastructure needed for those protocols to operate. Some protocols in common use include: CoAP, HTTP, WebSockets, MQTT and AMQP.
- **Syntactical Interoperability.** It is usually associated with data formats. The messages transferred by communication protocols need to have a well-defined syntax and encoding. The content can be represented using high-level transfer syntaxes such as XML, JSON and RDF.
- **Semantic Interoperability.** It is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content being exchanged. Machine interpretable descriptions are applicable to different aspects of semantic interoperability, for example:
  - Data models and data types.
  - Models that describe how to interact with things.
  - Frameworks for describing different versions of devices and software.
  - Semantic descriptions of things.
  - Semantic descriptions of the context.
  - Privacy policies covering use of personal data.
  - Security policies.
  - Smart contracts and terms & conditions.

To minimize barriers for digital services that span different platforms, there is a strong need to encourage convergence on modelling frameworks and languages. Some relevant work includes:

- W3C's Web of Things which uses JSON-LD to describe things as object with properties, actions, and events, using JSON Schema for describing the data types.
- W3C's Resource Description Framework (RDF) using graphs with directed labelled arcs.
- W3C's Web ontology language (OWL) and RDF Schema.
- Chen's Entity Relationship Diagrams.
- OMG's Unified Modelling Language (UML).
- Object-Role Modelling (ORM).
- Organizational Interoperability. It is the ability of organizations to effectively communicate and transfer meaningful data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions, and cultures. Organizational interoperability depends on successful technical, syntactical, and semantic interoperability.

The previous layered approach is the most agreed classification for the description of the interoperability in the IoT systems. However, another interesting classification is based on the diverse elements comprising IoT (devices, communication, services, applications, etc.). It proposes that IoT interoperability can be seen from different perspectives such as device interoperability, networking interoperability, syntactic interoperability, semantic interoperability, and platform interoperability. This layered approach is interesting to clearly define which parts of the IoT architectures the market solutions are focused on and how their interoperability requirements are solved.



## Handling approaches

To improve the state of IoT interoperability, researchers have leveraged numerous approaches and technologies which they refer to interoperability handling approaches [INT-10]. The main approaches are the following:

- **Use of Adapters/gateways.** These components are focused on the development of an intermediate tool sometimes called mediators to improve interoperability between IoT devices. Their aim is to act as a bridge between different specifications, data, standards, and middleware's etc. Mainly, performing a conversion between the protocol of the sending device and the protocol of the receiving device.
- **Virtual networks/overlay-based solutions.** Focused in to create a virtual network on top of physical networks and thereby allow communication with other types of devices, including sensor nodes.
- **Networking technologies.** Different networking protocols and technologies can be used to provide networking interoperability in IoT. These approaches could be IP-based approaches, Software-defined networking (SDN), Network function virtualization or Fog computing.
- **Open APIs.** API is an interface provided by service providers that exposes data or functions to an application written in a high-level language. A well-documented open APIs provides developers clear access to functionalities and services.
- **Service oriented architecture (SOA).** It facilitates the syntactic interoperability between heterogeneous devices and across all systems, because it is built on top of the network layer and the information processed can be easily managed through different service components.
- **Semantic web technologies.** The Semantic Web technologies developed, like by the W3C such as Resource Description Framework (RDF), SPARQL and Web Ontology Language (OWL) can be used for describing resources on the Web. Currently, the same standards are used in many different areas including IoT. Ontologies in IoT are a set of objects and relationships used to define and represent an area of concern. They represent an abstraction technology which aims to hide heterogeneity of IoT entities, acting as a mediator between IoT application provider and consumers, and to support their semantic matchmaking.
- **Open standards.** A standard is framework of specification that has been approved by a recognized organization or is generally accepted and widely used throughout by the industry. Open standards are one significant means to provide interoperability between and within different domains.

## ICT Interoperability and Standardization Priorities

The European Commission outlines the essential role of standards in general and in IoT as well. In its Communication regarding the ICT Standardization Priorities for the Digital Single Market [INT-14] the following table shows a summary of the guidelines published:

*IoT landscape is currently fragmented because there are so many proprietary or semi closed solutions alongside a plethora of existing standards. This can limit innovations that span several application areas. Large-scale implementation and validation of cross-cutting solutions and standards is now the key to interoperability, reliability, and security in the EU and globally. The European Union needs an open platform approach that supports multiple application domains and cuts across silos to create competitive IoT ecosystems. This requires open standards that support the entire value chain, integrating multiple technologies, based on streamlined international cooperation that build on an IPR framework enabling easy and fair access to standard essential patents (SEPs). In detail: (1) Foster an interoperable environment for the Internet of Things targeting reference architectures, protocols and interfaces, the promotion of open application programming interfaces (APIs), support of innovation activities related to reference implementation and experimentation and the development of missing interoperability standards (especially in the cross-sector domain of semantic interoperability), (2) Promote an interoperable IoT numbering space that transcends geographical limits, and an open system for object identification and authentication, (3) Explore options and guiding principles, including developing standards, for trust, privacy, and end to end security, e.g., through a 'trusted IoT label' and (4) Promote the uptake of IoT standards in public procurement to avoid lock-in, notably in smart city services, transport, and utilities, including water and energy.*

### IoT interoperability framework requirements

One of the initiatives that has carried out detailed research, collected a lot of information, obtained clear conclusions, and provided some guidance on interoperability is CREATE-IoT<sup>23</sup>. This project aims are to stimulate collaboration between IoT initiatives, foster the take up of IoT in Europe and support the development and growth of IoT ecosystems based on open technologies and platforms. For example, they published some deliverables like Strategy and coordination plan for IoT interoperability and standard approaches<sup>24</sup>, Recommendations for commonalities and interoperability profiles of IoT platforms<sup>25</sup> or Assessment of convergence and interoperability in LSP platforms<sup>26</sup> summarizing the results of IoT Large Scale Pilots. To address interoperability and integration through open IoT platforms, CREATE-IoT project provides a list of the main requirements expected to define an IoT interoperability framework. The requirements are the following

- Support of common IoT communication protocols.
- Support for M2M communications.
- Standard protocols for device communications.
- Support of the main IoT middleware platforms.
- Extensibility for different sensor types.
- User Device Detection Capability.
- Syntactic interoperability.
- Semantic interoperability.
- Gateway Capabilities and Protocol Conversion.
- Unique Device ID / Naming.
- Standard protocols for device communications.

And some key elements to consider creating a complete interoperability framework:

- Reference Architectures
- Support of design and development
- Platforms and technologies
- Standards and pre-normative activities

#### 3.1.4.2 Relevant initiatives and solutions

This section is going to put the names on the table about the different initiatives and solutions that have addressed/are addressing the challenges of IoT interoperability. To show the information in a concise way, the following categories are going to be analysed: firstly, the main standardization organizations, secondly, the main IoT platforms that offer some functionalities to address interoperability issues, thirdly, the interoperability platforms aimed at achieving interoperability between IoT platforms and finally the large-scale pilots focused in to implement and demonstrate the fulfilment of interoperability needs.

#### Standardization

As previously explained, standardization across the IoT landscape is important because this reduces the gaps between protocols. Various initiatives are working on developing IoT standards majorly driven by government agencies, standards bodies, and industry giants. During the last decade more hundreds of standards are applying

---

<sup>23</sup> <https://european-iot-pilots.eu/project/create-iot/>

<sup>24</sup> [https://european-iot-pilots.eu/wp-content/uploads/2017/10/D06\\_01\\_WP06\\_H2020\\_CREATE-IoT\\_Final.pdf](https://european-iot-pilots.eu/wp-content/uploads/2017/10/D06_01_WP06_H2020_CREATE-IoT_Final.pdf)

<sup>25</sup> [https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06\\_02\\_WP06\\_H2020\\_CREATE-IoT\\_Final.pdf](https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_02_WP06_H2020_CREATE-IoT_Final.pdf)

<sup>26</sup> [https://european-iot-pilots.eu/wp-content/uploads/2020/06/D06\\_03\\_WP06\\_H2020\\_CREATE-IoT\\_Final.pdf](https://european-iot-pilots.eu/wp-content/uploads/2020/06/D06_03_WP06_H2020_CREATE-IoT_Final.pdf)

to IoT and the organisations that produce and maintain them. The main IoT standards activities related or interesting to ASSIS-IoT are the following:

*Table 16. IoT standard activities.*

Organisation	Description
ETSI <sup>27</sup>	ETSI, the European Telecommunications Standards Institute, produces globally applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. ETSI Smart M2M is currently focalized on: (i) participation and contribution to the EU initiatives in the M2M and IoT areas, (ii) Standardize a framework for an open ontology (SAREF) to that enables information sharing among IoT devices and servers using different technologies and (iii) Support to AIOTI Initiative. In addition, other ETSI activities are related to IoT, in particular by providing standards for Network interoperability
IEEE <sup>28</sup>	IEEE standards set specifications and best practices based on current scientific and technological knowledge. These standards span wired and wireless connectivity, encryption, data security, etc. IEEE P2413 is working with a top-down approach and follows the recommendations for architecture descriptions defined in ISO/IEC/IEEE 42010 which: (i) Provides a core ontology for the description of architectures, (ii) Specifies provisions that enforce desired properties of architecture frameworks, (iii) Can be used to establish a coherent practice for developing architecture frameworks and (iv) Can be used to assess conformance of an architecture framework
IETF <sup>29</sup>	It aims to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. IETF supports IoT since 2005 when it started with 6LoWPAN IoT related IETF working groups are: <ul style="list-style-type: none"> <li>• 6Lo (IPv6 over Networks of Resource-constrained Nodes);</li> <li>• ROLL (Routing Over Low-power and Lossy networks);</li> <li>• CORE (Constrained RESTful Environments);</li> <li>• ACE (Authentication and Authorization for Constrained Environments) (ACE);</li> <li>• CBOR (Concise Binary Object Representation Maintenance and Extensions);</li> <li>• 6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e)</li> <li>• IPWAVE (IP Wireless Access in Vehicular Environments);</li> <li>• IPWAN (IPv6 over Low Power Wide-Area Networks);</li> <li>• Detnet (Deterministic Networking);</li> <li>• LWIG (Light-weight Implementation Guide)</li> </ul>
ISO/IEC <sup>30</sup>	ISO and IEC have a joint technical committee called JTC 1. JTC 1 established a Special Working Group (WG10) on IoT in 2012 that was changed into a formal WG in 2015 and transitioned to a formal Sub Committee in 2017. Current works are: <ul style="list-style-type: none"> <li>• ISO/IEC 30141, Internet of Things Reference Architecture</li> <li>• ISO/IEC 20924, Definition, and vocabulary</li> <li>• ISO/IEC 21823-1, Interoperability for Internet of Things Systems, Part 1: Framework.</li> <li>• ISO/IEC PDTR 22417, IoT Use cases.</li> </ul>
ITU-T <sup>31</sup>	ITU-T develops international standards which act as defining elements in the global infrastructure of information and communication technologies (ICTs). ITU standardisation activities are managed

<sup>27</sup> <https://www.etsi.org/>

<sup>28</sup> <https://www.ieee.org/>

<sup>29</sup> <https://www.ietf.org/>

<sup>30</sup> <https://www.iso.org/home.html>

<sup>31</sup> <https://www.itu.int/en/ITU-T/Pages/default.aspx>

Organisation	Description
	in Study Groups (SG), two of them of particular interest: SG17 on security and SG20 on IoT and applications and Smart Cities.
oneM2M <sup>32</sup>	The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. OneM2M reaches to achieve interoperability through different standardisation efforts. The different working groups produce specifications for a reference architecture (ARC WG), a messaging protocol (PRO WG), a data management, abstraction, and semantics (MAS WG), but also interoperability testing (TST WG).
W3C <sup>33</sup>	The World Wide Web Consortium (W3C) is an international member funded community focussing on defining Web technology standards. W3C aims to counter the fragmentation of the IoT through a semantic interoperability framework that decouples applications from the underlying IoT standards, protocols, data formats and communication patterns, and enables discovery, composition, and adaptation to variations across devices from different vendors. The goal is to reduce the costs and risks for developing IoT solutions and create the conditions for unlocking the network effect for sustainable growth in open markets of services on a Web scale, just as we enabled through our standards for Web pages, which saw sustained exponential growth over many years. The Web of Things is based upon W3C's work on Linked Data and covers the interaction model exposed to applications in terms of the properties, actions and events for things, the semantic models describing the kinds of things and their relationships, and metadata relating to security, trust, privacy, service level agreements and other terms and conditions.

## IoT platforms

IoT platforms are considered as the most significant component of the IoT ecosystem. The Internet of Things cannot work without software, including middleware, known as an IoT platform. These platforms fill the gap between the device sensors and data networks. They connect the data to the sensor system and gives insights using back-end applications to create a sense of the plenty of data developed by the many sensors. An IoT platform can monitor, manage, and control various types of endpoints and, in addition, can enable connectivity and network management, data management, processing and analysis, application development, security, access control, monitoring, event processing and interfacing/integration.

We have selected the following classification, based in the information collected by UNIFY-IoT<sup>34</sup>, in order to analyse the most popular IoT Platforms and briefly summarizing its interoperability functionalities:

- Cloud centric IoT platforms. Fully managed service integrated into cloud offering. These kinds of platforms enable reliable and secure bidirectional communications between millions of IoT devices and a solution back end. Some platforms are Microsoft Azure IoT, Amazon AWS IoT platform and IBM Watson IoT platform.
- Industry centric IoT platforms. IoT connectivity extends to machines, sensors, devices and processes in the industrial sectors, and business outcomes produce increased manufacturing efficiencies, better resource utilization, and transformed support models that are driving adoption. In this context, the development of Industrial IoT platforms is driven by large manufacturing companies. Some platforms are: PTC ThingWorx, Bosch IoT Platform and GE Predix,
- Communication centric IoT platforms. They are focused in managing connected products and machines and implementing IoT and M2M applications. Some platforms are: Cisco/Jasper and Axeda IoT.
- Device centric. The device centric IoT platforms are developed as hardware-specific software platforms pushed by companies that commercialize IoT device components and have built a software backend

<sup>32</sup> <https://www.onem2m.org/>

<sup>33</sup> <https://www.w3.org/>

<sup>34</sup> <https://cordis.europa.eu/project/id/688369/es>

that is referred to as an IoT platform. Some Platforms are: Open Hab, Nimbits, IoT ToolKit and Chimera IoT platform.

- SME/Startup platforms. Platforms from SME and startups. Some platforms are Xively, Thingspeak or Carriots.
- Open-source platforms. Platforms from Open-Source projects. Some Platforms are: Fiware, OpenIoT, Universaal and Kaa.
- OneM2M based platforms (ETSI). OneM2M based platforms are M2M platform implementations that follow the OneM2M standard, an increasingly important IoT related standard in the Telecoms sector. Some Platforms are: Eclipse OM2M and Open MTC.

The table is focused in the main open-source application-oriented platforms:

*Table 17. Interoperability approach in IoT European Open Platforms.*

Platform	Interoperability Approach
universAAL <sup>35</sup>	IoT platform for the integration of open distributed systems of systems. The ontological model allows custom ontologies to be easily plugged in.
OpenIoT <sup>36</sup>	Its main objective is to enable flexible configuration and deployment of algorithms for collection and filtering information streams stemming from internet-connected objects. It provides ontologies, semantic data models and annotations for representing interconnected objects. The use of semantic open-linked data techniques, APIs and wrappers as methods for accessing the data services
FIWARE <sup>37</sup>	Middleware platform for IoT, supported by the European Commission. Union under the Future Internet Public Private Partnership Programme Public and royalty-free API specifications and interoperable protocols for the creation of new internet services and applications.
sensiNact <sup>38</sup>	A horizontal platform dedicated to IoT and particularly used in various smart city and smart home applications. sensiNact aims at managing IoT protocols and devices heterogeneity and provides synchronous (on demand) and asynchronous (periodic or event based) access to data/actions of IoT devices, as well as access to historic data with generic and easy-to-use API.
onesait <sup>39</sup>	Onesait Platform provides the flexibility so that developers can build their own solutions in a solid and agile way using Open-Source technologies. Provides unified view of business entities. The model describes the meaning of entities, relationships, and data.

### Platforms focused in providing interoperability between IoT platforms

The IoT European Platforms Initiative (IoT-EPI) is a European initiative for IoT platform development, interoperability and information-sharing, founded by the EU to build a vibrant and sustainable IoT ecosystem in Europe. Seven leading research and innovation projects (AGILE, bIoTpe, BIG IoT, Inter-IoT, symbIoTe, TagItSmart, VICINITY) supported by two coordination and support action projects Be-IoT and UNIFY-IoT make their technology accessible to third parties. The specific areas of focus of the research activities are architectures and semantic interoperability, which reliably cover multiple use cases. Their goal is to deliver dynamically configured infrastructure and integration platforms for connected smart objects covering multiple technologies and multiple intelligent artefacts. The table summarizes the results of a white paper that provides an insight regarding interoperability in the IoT platforms and ecosystems created and used by IoT-EPI. The document covers the interoperability aspects, challenges and approaches that cope with interoperability in the current existing IoT platforms.

<sup>35</sup> <https://www.universaal.info/>

<sup>36</sup> <http://www.openiot.eu/>

<sup>37</sup> <https://fiware.zone/>

<sup>38</sup> <https://projects.eclipse.org/projects/technology.sensinact>

<sup>39</sup> <https://www.onesait.com/>



Table 18. IoT European Platforms Initiative.

Project	Description	Platforms Integrated
AGILE <sup>40</sup>	It builds a modular hardware and software gateway for the IoT focusing on the physical, network communication, processing, storage, and application layers. The AGILE software modules are addressing functions such as device management, communication networks like area and sensor networks and solution for distributed storage. The project considers all the modules needed to provide a robust security management solution.	Resin.io Eclipse IoT Node-RED
Big IoT <sup>41</sup>	It develops a generic, unified Web API for IoT platforms implemented. As part of the project, 8 partner IoT platforms are being integrated with the ecosystem plus several additional platforms are joining via the community building process. The project focuses on the upper layers of the IoT architecture by addressing the security management, APIs, service integration, external system services, applications, and the business enterprise.	Smart Data Platform Smart City Platform (Bosch) Wubby Platform OpenIoT Traffic Information Centre Bitcarrier/Sensefield/FastPrk BEZIRK Platform
BioTope <sup>42</sup>	It provides an architecture and recommendations for the use of open standards and use case implementations that enable stakeholders to easily create new IoT systems and services and to rapidly harness available information using advanced Systems-of-Systems (SoS) capabilities for Connected Smart Objects. bIoTpe also develops and provides standardised open APIs to enable interoperability. The project addresses all eight layers of the IoT architecture and validates the interoperability solutions in a cross-domain environment.	DIALOG Node-RED Warp10 FIWARE Open IoT Mist eAir Web
INTER-IoT <sup>43</sup>	The project addresses an open cross-layer framework, an associated methodology and tools to enable voluntary interoperability among heterogeneous IoT platforms by focusing on six layers of the IoT architecture with modules covering the QoS and device management, service integration, external system services, storage, and virtualisation. The project addresses all network communication layers and the full security management suite.	SEAMS I3WSN BodyCloud Node-RED OpenIoT FIWARE UniversAAL Eclipse OM2M WSO2 Microsoft Azure IoT suite Amazon AWS IoT
TagItSmart <sup>44</sup>	It offers a set of tools and enabling technologies that can be integrated into different IoT platforms using provided APIs to enable users across the value chain to fully exploit the power of	SocioTal FIWARE

<sup>40</sup> <http://agile-iot.eu/><sup>41</sup> <http://big-iot.eu/><sup>42</sup> <https://biotope-project.eu/><sup>43</sup> <https://inter-iot.eu/><sup>44</sup> <https://www.tagitsmart.eu/>

Project	Description	Platforms Integrated
	condition-dependent functional codes to connect mass-market products with the digital world across multiple application sectors	EVERYTHNG RunMyProcces Microsfot Azure
SymbioTe <sup>45</sup>	The project provides an abstraction layer for a unified view on various IoT platforms and sensing/actuating resources. Applications can use symbIoTe Core Services implementing a semantic IoT engine to find adequate resources offered by symbIoTe-enabled platforms and subsequently access platform's virtual resources directly for data acquisition and actuation. The project focuses on seven layers of the IoT architecture from physical to application layer and proposes a full security management suite	OpenIoT Symphony MoBaaS nAssist Navigo Digitale IoT platform KIOLA
VICINITY <sup>46</sup>	It is focused on a platform and ecosystem that provides "interoperability as a service" for infrastructures in the IoT and addresses the five-upper layer of the IoT architecture. The work considers the service integration, business logic, virtualisation, storage, APIs, tools, external system services, applications, data analytics and cloud services.	LinkSmart IoTivity SiteWhrere Eclipse Kura TinyMesh Gorenje Cloud Sevices

### IoT European Large-Scale Pilots

The IoT European Large-Scale Pilots Programme includes the innovation consortia that are collaborating to foster the deployment of Internet of Things (IoT) solutions in Europe through integration of advanced IoT technologies across the value chain, demonstration of multiple IoT applications at scale and in a usage context, and as close as possible to operational conditions. The projects involved are ACTIVAGE, MONICA, IoF2020, AUTOPILOT and SYNCHRONICITY. The following table summarize its main information:

*Table 19. Example table caption above table.*

Project	Summary of interoperability support	Platforms and Technologies Supported in Use Cases
ACTIVAGE <sup>47</sup>	ACTIVAGE has developed and implemented a High-Level Reference Architecture (HLA) This architecture is tailored to address the needs of AHA and relies on a layered model to ensure the intermediation between the applications and the sensor devices (edge) layer. Three main layers are involved: (i) AIOTES Services Layer is a set of software solutions, tools and methodologies in support of semantic interoperability, security, privacy and data protection. (ii) The Interoperability Layer is an abstraction layer in charge of ensuring interoperability through the ACTIVAGE platforms. (iii) IoT Platform Layer. The IoT middleware in charge of connecting all the "things" involved in ACTIVAGE use cases is complex and heterogeneous. The Platform layer will serve as an abstraction layer that will ensure that different platforms can be supported, and a given service can be replicated across different pilot sites.	FIWARE IoTivity OpenIoT SensiNact SOFIA2 universAAL

<sup>45</sup> <https://www.symbiote-h2020.eu/>

<sup>46</sup> <https://www.vicinity2020.eu/vicinity/>

<sup>47</sup> <https://activageproject.eu/>

Project	Summary of interoperability support	Platforms and Technologies Supported in Use Cases
IoF2020 <sup>48</sup>	<p>The project is formed by 19 use cases grouped in 5 trials with end users from the Arable, Dairy, Fruits, Vegetables and Meat verticals and IoT integrators that demonstrate the business case of innovative IoT solutions for a large number of application areas. The main resulting Interoperability Points of the project are: (0) a connectivity enabler for IoT Devices and agricultural machinery, (1) it enables the exposition of the data and services offered by IoT Devices through well-known programmatic interfaces, (2) it enables the transformation, aggregation, harmonization and publication, as context information, of harmonized data coming from IoT Devices, agricultural machinery or other sources of information (open data portals, web services providing contextual data, etc.). On the other hand, it exposes a unified way to send commands and to mediate with IoT Devices or agricultural machinery, regardless the interface exposed by the IoT Service Layer or the Physical Machinery, (3) it provides access to all the data (real-time and historical data or analytics results) of interest to smart farming applications, (4) it enables the Application and Mediation Layers to consume public Geo-Services and (5) a cross-cutting interoperability point that facilitates the secure interchange of information between the different layers and actors.</p>	<p>365FarmNet  AgroSense  Apache Cassandra / Flink / Spark  Arvalis IoT Platform  Altland FMIS  Connecterra IoT  Cygnus  EBBITS  EPCIS  FIWARE  FIBSPACE  LinkSmart  MongoDB  OpenStack  Qlip (automatic calibration and validation)  ThingWorx IoT  VIRTUS</p>
MONICA <sup>49</sup>	<p>MONICA demonstrates a large-scale IoT ecosystem that uses innovative wearable and portable IoT sensors and actuators with closed-loop back-end services integrated into an interoperable, cloud-based platform capable of offering a multitude of simultaneous, targeted applications. It provides (i) an API layer, (ii) a Services layer where the intelligence of the platform is implemented, and processing modules are integrated. (iii) IoT layer which is in charge of interoperability using two Open-Source frameworks: LinkSmart (IoT middleware) and the SCRAL (IoT abstraction layer). (iv) Edge layer a set of processing modules that process real-time data directly from the Device Layer, (v) Network Layer allows the effective communication between the heterogeneous IoT wearables, IoT devices and the IoT platform modules and (vi) Device Layer includes all IoT wearables and sensors</p>	<p>LinkSmart middleware  SCRAL adaptation framework  GOST (Go-SensorThings) IoT  OGC SensorThings</p>
AUTOPILOT <sup>50</sup>	<p>AUTOPILOT develops new services on top of IoT to involve autonomous driving vehicles, like autonomous car sharing, automated parking, or enhanced digital dynamic maps to allow fully autonomous driving. Its interoperability framework is achieved based on: (i) OneM2M Interoperability Platform and Interworking Gateways. The proprietary IoT platforms are interconnected through interworking gateways and the oneM2M interoperability platform. (ii) Standardised</p>	<p>OneM2M  FIWARE  Huawei Platform  Watson IoT Platform</p>

<sup>48</sup> <https://www.iof2020.eu/>

<sup>49</sup> <https://www.monica-project.eu/>

<sup>50</sup> <https://autopilot-project.eu/>

Project	Summary of interoperability support	Platforms and Technologies Supported in Use Cases
	IoT Data Models. In order to specify the syntax and the semantics of the data.	
SYNCHRONICITY <sup>51</sup>	SynchroniCity is aimed to establish a reference architecture for the envisioned IoT-enabled city marketplace with identified interoperability points and interfaces and data models for different verticals. It provides: (i) A common standard API for context information management: the context data manager (Context Data Broker) is a key component of the SynchroniCity architecture and the implementation of its API (compliant with NGSI API) is considered an “interoperability point” to enable cities to participate to the SynchroniCity platform (ii) A common set of information models: semantic interoperability, achieved through the adoption of common data models, is introduced in the architecture as a basic requirement to enable reuse of applications in different cities and domains. (iii) A set of common standards data publication platforms: the role of data is crucial in SynchroniCity. For this reason, the reference architecture includes specific data management components that aim to provide, through standard interfaces, all the functionalities related to data life cycle management.	Mosquitto MQTT Fiware Stack

### 3.1.5 DLT and semantics

#### 3.1.5.1 Scientific review

IoT has gathered the attention of academics, businesses, and journalists over the past years as a technology that would bring a revolution [DLT-1]. Numerous sectors, such as healthcare, agriculture, or smart cities, have the potential of adopting the IoT applications. In [DLT-2], a view on the use of IoT in subsectors is presented where the most prominent places are held by smart cities, industrial IoT and connected health. Apart from sectors, rapid growth is documented in Internet-connected devices [DLT-3], as these devices are ranging from sensors to the more sophisticated cloud servers and smart objects. The communication between the devices is achieved via the implementation of communication protocols. Ammar et al. [DLT-3] refer to a concept in the IoT architecture that coordinates and manages the processes of the various IoT elements. Standardization bodies are working towards creating protocols for alleviating the issue of the heterogeneity in technologies and devices. Nikoukar et al. [DLT-4] have documented these standardization bodies, which are the following:

- IEEE Standards Association (ZigBee, Thread, WirelessHART)
- Internet Engineering Task Force (6LoWPAN, ROLL)
- European Telecommunications Standards Institute (3GPPTM)
- International Society of Automation (ISA100.11a)
- Internet Protocol for Smart Object
- Bluetooth Special Interest Group

Despite the promises and hopes for the opportunities that IoT could bring, the adoption is not flawless as challenges are documented. The existence of challenges should be evident from the standardization bodies that work on the technology. Sisinni et al. [DLT-5] have documented the following IoT challenges: Energy Efficiency; Real-time Performance; Coexistence and Interoperability; Security and Privacy. The research on the IoT is ongoing as the need for tackling these challenges is evident. The idea of the semantics is nothing new as it initially was a way to revolutionize the web with the Semantic Web [DLT-6]. The Semantic Web seemed to profoundly change the sharing of scientific knowledge. The web was constructed as an information space intended for human understanding, while the semantic web would allow machines to handle structured data.

<sup>51</sup> <https://synchronicity-iot.eu/>

The idea of applying semantics have not faded away as it has found ways of applying in many research fields. Naturally, the idea has been applied to IoT, where there is the apparent need that all the Things have to communicate with the rest of the world. For this reason, the following section aims to showcase some of the available suggestion from the literature review.

Ruta et al. [DLT-7] have proposed a service-oriented architecture which implements a semantic layer upon blockchain infrastructure. The semantic layer is built for the purpose of discovering resources and services. This is achieved by comparing the received request with the resource descriptions considering their semantic annotation. A shared ontology is used as a reference for the comparison of the request and the resources. The comparison outputs a distance score between the requested metadata and the available resources in the chain. The authors envisioned the adoption of such a paradigm in smart cities. The authors in [DLT-8] have proposed a Decentralised Interoperable Trust (DIT) model blockchain framework for healthcare IoT systems. The perceived architecture is composed of four distinct layers. The architecture is derived from the standard IoT architecture, but the third layer, that is dedicated to middleware, differentiates with the accommodation of blockchain as a sub-layer. The proposed system supports the annotation of edge devices and implements cryptographic algorithms for security reasons in various application layers. The blockchain creates trusted primary zones by validating primary and group IDs for edge devices and validates the transactions.

In a suggested architecture for a Semantic Web of Things platform, a six layered architecture is presented [DLT-9]. The basis of the architecture is the device layer, which exposed with IoT standards like OPC-UA, MQTT and Bluetooth. Data from different sources are consolidated in the cyber layer. The next layers are adding capabilities such as data analysis and machine learning algorithms on these data. The final layer is the one closest to the users who have different applications at their disposal to interact with the Things. Al Ridhawi et al. [DLT-10] have suggested a decentralized cloud solution with the application of fog computing and blockchain. The innovation of the suggestion is the execution of complex services at IoT objects in the edge of the network. Ontologies are contributing to the success of the suggestion as to the capabilities of a node, in hardware and software, are stored in ontologies. The selection of a node follows a three-stage process where the capabilities of a node, the node's willingness in cooperation and the service path are sequentially defined. The ontology is used for the comparison of a node's capabilities against the request of the service, while reinforce learning is assisting in the construction of the service path.

Blockchain researcher is ongoing and aims to mitigate issues and needs that sprung during the adoption of blockchain. Naim and Klas [DLT-11] have proposed a framework for a semantic blockchain that focuses on data persistence and represent the data in a graph. The data persistence is enhanced by adopting four additional steps in a block's creation. As the additional steps process, interlink and retrieve the data, the created block is transformed into graph data. The graph offers the opportunity for knowledge extraction and connection interrelations. The developed prototype has made use of RDF, but this would not exclude the adoption of other graph models. The suggested prototype seems to be agnostic to the data provided, as the authors have mentioned that IoT is a technology that could adopt the prototype as basic infrastructure. IoT could be implemented into the foodservice sector to assist in adhering with standards as HACCP. Markovic et al. [DLT-12] have worked on a system that harnesses the computational power in the devices and employs semantic provenance annotations. The system is focused on the last mile delivery and is tasked for compliance control after packaging the food. A delivery package is accompanied by an IoT logger that interacts with other devices to ensure food safety. As an IoT logger is assigned to a single delivery, the consumer could access his data via the interaction of a mobile phone with the IoT logger. The system requirements, that the system is built upon, are the IoT logger, the location beacons, the server, the private blockchain network and a mobile application. The components are tasks for compliance monitoring, semantic data representation and data storing. The semantic representation is handled in server due to the device's limitations and leverages the FD-PROV ontology. The communication between the devices and the server is done via the use of a RESTful API. The data storage component builds a blockchain business network by using the Hyperledger Composer and deploys smart contracts in Hyperledger Fabric. All in all, Markovic et al. [DLT-12] have suggested the use of semantics for controlling the food by using the data via IoT devices and the use of blockchain to create a marketplace.

### 3.1.6 Distributed intelligence

The term **distributed intelligence** has at least two meanings: (a) collective intelligence, and (b) distributed artificial intelligence. The first meaning also expressed in the term “collective intelligence” encompasses



shared/group intelligence that emerges from collaboration and competition of multiple individuals. As the main mechanisms of collective intelligence, (a) cognition, (b) cooperation, and (c) coordination are specified. Here, if understood in the “*most convenient way*”, e.g., when (a) cognition is seen as sensing, (b) cooperation is understood as multiple (semi-)autonomous entities exchanging data to (jointly) establish what needs to be done, and (c) coordination is conceptualised as mechanism crucial for realization of workflows, where specific actions depend on results of other actions, it is not very difficult to envision scenarios, in which collective intelligence can be claimed to materialize within IoT ecosystems. However, taking into account the scope of the ASSIST-IoT action, it can be stipulated that the collective intelligence is out of immediate interest, and focus of the proposed work, and could, instead, potentially appear as an emergent property of future concrete implementation of the ASSIST-IoT architecture. Therefore, let us direct our attention to distributed artificial intelligence. Nevertheless, the action remains open to pursuing inspirations rooted in conceptual frameworks and research conducted within the scope of collective intelligence.

Distributed artificial intelligence (sometimes also called Decentralized AI) is a subfield of AI research, dedicated to the development of distributed solutions for problems. Very often it is seen as a predecessor to the research devoted to software agents and (multi-)agent systems. While, in principle, this assessment is correct, one has to recognize that, over time, the field of research devoted to software agents has evolved on its own and, nowadays, is heavily loaded with domain-specific concepts, technical terms and results. As a matter of fact, one could also conclude that software agents/agent systems are also very closely related to the collective intelligence (as conceptualized above). It is also worth noting that within the scope of agent research, a large number of software platforms has been created [DI-1], leading to a reasonable assumption that agent systems should be implemented using agent-dedicated software. Obviously, such an assumption would be a strongly limiting one, from the point of view of research that is to be undertaken within the ASSIST-IoT action, as it would closely tie its undertakings to the specific set of tools. Therefore, we will not proceed in this direction and will not include further information about agent systems in this document. Nevertheless, a (relatively fresh) comprehensive review of use of software agents on the Internet of Things can be found in [DI-2]. Therefore, we will continue monitoring progress of research undertaken on the border between IoT and software agents.

This leads us to the area of most interest to the action, which is known as *distributed problem solving*. Here, the main idea is as follows. Let us assume that a computationally intensive task, related to some form of, very broadly understood, machine learning has to be undertaken. In this context, AI (or machine learning, in particular) can involve training neural networks, but the approach also applies to nature inspired optimization, data clusterization, etc. For (very) large datasets, completing such a task on a single computer/processor/node would require a substantial amount of time (hours, days, or even weeks). Let us now assume that multiple computing nodes are available (in the form of a tightly coupled parallel computer, or a network of workstations, or a cluster computer). In this case, research has been devoted to finding ways how the “work” can be divided (among nodes) to complete the task. It is easy to realize that, there, the main concerns are related to: how the main task can be decomposed, and how the knowledge, originating from multiple sources (individual nodes), can be combined (knowledge system) to complete the original task.

Considerations concerning task decomposition, and knowledge synthesis, has evolved with the whole area of machine learning. For instance, work of Cantu-Paz [DI-3] (from 1999), can already be seen as an attempt at task distribution and knowledge synthesis. Here, multiple instances of an evolutionary (genetic) algorithm run on separate computing nodes, and only from time-to-time exchange “*genetic material*”. This approach became, later, known as an island version of evolutionary computing. The main idea is simple; a task is divided into subtasks; each subtask is executed independently, and results are combined. Combining of results may occur at the end of the process, or can be repeated multiple times during the (iterative) process. This process matches what is typically named as “distributed (machine) learning” (DML). Note that such an approach can be applied to various machine learning (ML) algorithms, not only to genetic algorithms. More than 20 years ago the problem of how to scale up the DML algorithm have been discussed [DI-4, DI-5, DI-6]. Further examples of DML include transaction processing in large enterprises, on data that is stored in different locations [DI-7] or applying ML to astronomical data that is too large to move and centralize [DI-8]. There are multiple contributions, in which the common architectural framework for DML has been discussed. In the survey [DI-9] all these attempts have been summarized and a Reference Architecture for DML has been suggested.

Since this approach is (a) well studied, and (b) based on main ideas from parallel computing, which in itself is a mature research area, with 40+ years of development, we will not consider it further in this document. If

needed, existing results can be straightforwardly applied within the scope of the ASSIST-IoT action (see e.g., [DI-3]-[DI-8]).

However, reflecting on what has been said thus far, and what can be found in the literature, an important observation is in place. Methods and approaches, which stem from parallel (high performance) computing, typically, make the following implicit assumption. They are designed for a **single stakeholder**. In other words, the main idea is that a single “user” (e.g., a company) is the sole owner of all of the data. This data is used in DML, while remaining under full “control” of its owner. Of course, it is possible that some open source (public) data will be used (added to the mix) to augment the training. Nevertheless, the core data has a single owner. Obviously, this model can be easily adapted also to cloud computing, since it is possible to sign a contract with a cloud provider that will include appropriate guarantees concerning control over data (securing data from access by other users).

Until recently, this assumption, and the DML model that was based on it, was almost unquestionably valid. However, during the past few years, the situation has been rapidly evolving. Among others, the following trends brought about the change. (1) Proliferation of powerful handheld devices with multiple sensors (a.k.a. smartphones), which generate streams of data that users may want to control (e.g., to use them for their own “advantage”). Here, users have data, but lack capabilities of processing it. Moreover, their data covers only fragments of possible domains of interest. (2) Fast drop of price and size of sensors (and actuators), which can be placed “everywhere” and can belong to “anybody”. Again, data streams from individual sensors may not be enough to design and implement valuable services. (3) Proliferation of wireless networks with various (actual) bandwidth and range, which are used to establish communication channels between sensors, actuators, edge devices, computing nodes, gateways, cloud(s), etc. (4) Progress in research, development, and deployment of the Internet of Things ecosystems, in almost all areas of day-to-day activities. (5) Progress in methods, and their implementations, that can be used in various ML scenarios. (6) Development of ML-dedicated hardware, including extra small devices that can be placed “almost anywhere” (e.g., Intel Movidius pr NVIDIA Jetson Nano, are just two examples of this trend). As a result, the vision of a single owner of data that is being used to train model(s) to realize her/his/its own (individual) goals, starts to be supplanted by approaches that can facilitate coopetition<sup>52</sup>.

This brings us to one of the most recent developments in the area of, broadly understood, distributed machine learning, i.e., the **federated learning**. While, for all practical purposes, this approach is less than five years old (at least in officially published literature), it has generated substantial interest. Therefore, we will now focus our attention on this particular emanation of distributed intelligence.

**Federated Learning (FL)** is an approach to machine learning, where training of a model involves multiple datasets stored in “local nodes”, while the training itself proceeds without exchanging any data samples. In other words, there exists a central (shared) model, training of which is the goal of the process. However, during the training, each participating node is using only its local data to train its local sub-version of the model. Next, model parameters are “combined into the central model”. After the update is completed, the updated central model is redistributed (back) to the nodes that participated in the training. Here, the loop closes, and the process repeats, until the common model is considered to be “good enough quality” (using process specific criteria).

While this may seem like “canonical DML”, the underlying rationale is somewhat different. Rather than splitting single-owner data, and training the model in parallel, the focus is on the use of local data (without sharing it). In this context, it is easy to see that only local nodes have actual access to their own data (which is not shared), while the central (shared) model is updated on the basis of results delivered by individual nodes. It is important to note that, while the majority of currently published work focuses on the use of neural network-based FL, this is not necessary. In principle, FL can be applied to any form of DML. Saying this, let us now look in more details at the state-of-the-art in federated learning.

---

<sup>52</sup> Coopetition is the act of cooperation between competing companies; businesses that engage in both competition and cooperation are said to be in coopetition.

### 3.1.6.1 Scientific review

Let start from the summary of the number of papers related to the Federated Learning. In Figure 43 [DI-10] we see comparison of the number of publications related to three concepts, federated databases, federated cloud and federated learning. It is immediately clear that the interest in FL is an explosive phenomenon.

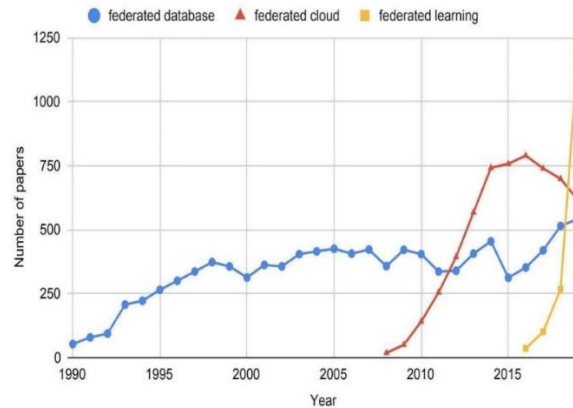


Figure 43. Number of published papers concerning federated databases, federated cloud, and federated learning

During desk research, we have preliminarily scanned 252 research articles found in journals (minority), conference proceedings, and arXive (majority). The results of our work have been summarized in Table 20. Here, the key observation is that majority of work is based on local simulations. Only very few contributions involve actual testing/experiments. This is a clear indication that this field attracts a lot of attention but is also very “immature” as far as real world, actual, experiments.

Table 20. Summary of considered papers.

Topic	Amount	Local simulation	Theoretical consideration	Testing/experiments as proof of concepts
All possible topics	250	214	21	15
Blockchain	6	3	3	0
Framework	40	38	0	2
Communication issues	30	28	0	2
Security and privacy	32	25	5	2
Using for IoT	12	9	1	2

Taking this into account, let us now present an overview of the most interesting ideas found in the surveyed literature. We start from the initial proposal, put forward by the researchers from Google.

#### FL foundations

In the blog post, and later in the articles [DI-11], and [DI-12], the foundations of FL, and an architecture of the system that enables FL, have been proposed. There, the machine learning software was TensorFlow, while the application area was related to word prediction and suggestion to be provided as a service when smartphone users are typing “messages”. It is important to note that, in work published less than three years ago, authors note that their work is in the initial phase and not all encountered problems have been solved. Based on our best knowledge, this remains the situation, regardless of the number of published contributions.

In the presented solution, phones send (to the server) initial messages that they are ready to “cooperate”. Next, they download a (shared) model (that is to be updated/improved) from the cloud. They refine it by applying training, based on locally available/stored data. In what follows, they send the proposed changes back to the cloud. Note that only the proposed model adjustments are communicated. The individual results (change suggestions) are used to update the shared (central) model. These steps form a single iteration. Interestingly, according to the proposal, only a limited number of devices should participate in each iteration. Moreover, an iteration is considered successful when a sufficient number of devices reports that changes (in the shared model) are needed. In other words, each device may establish that further training, based on local data, does not bring improvements to the obtained model. If a large number of nodes report that there was no need for central model

updates, all proposed changes in that iteration, are abandoned. Overall, iterations are repeated until the desired effect is obtained. Obviously, the FL process may be restarted at any time, if more data is accumulated in the individual nodes. Presented work states that a special security mechanism ensures that individual changes are not stored in the cloud. The latter is important as it is possible that such changes could allow an “attacker” to find something about the data that was used to propose them.

In the proposed approach, the server uses an actor approach [DI-13] that allows for easy scaling of the architecture. The main elements of the system are shown in Figure 44. Each *Coordinator* is responsible for managing one machine learning task. It receives information how many devices are connected to each *Selector* and decides how many devices should be accepted for training of the common model. The *Selector* is responsible for communication with (mobile) devices/computational nodes. More accurately, it accepts connections and redirects them to the *Aggregator*. Data is not saved to the persistent memory until information is collected from all nodes participants in the given iteration. This allows ensuring security and reducing delays associated with data recording. While in Figure 44 Selectors are connected to individual devices (smart phones), this approach naturally generalizes to any devices that perform training on local (private) data.

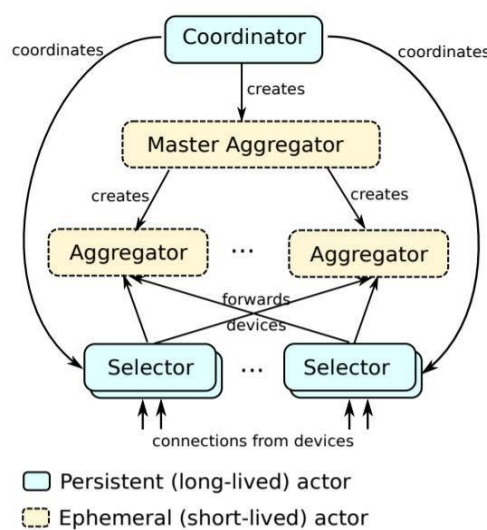


Figure 44. Schema of Federated Learning Architecture [DL-13]

Work reported in [DI-14] provides the basic algorithm, from the domain of DL that can be (and often is) used in FL. This is a popular synchronous algorithm, which utilizes Stochastic Gradient Descent (SGD). Here, each client performs one iteration of the algorithm, and sends a weight shift vector back to the server. The server averages the results from all clients that participated in the iteration and updates the model. This algorithm is referred to as FederatedSGD (FedSGD for short). As suggested in [DI-14] there exist multiple versions of FedSGD that may involve additional operations performed by each node. They are parameterized by three parameters: *C* – denoting the part of clients that takes part in each iteration; *E* – stating the number of epochs executed by the client in each iteration, and *B* – which describes the size of the batch. Operation of the proposed approach was tested on various types of architectures (convolutional networks, LSTM networks, multi-layer perceptron, and others). The most advanced version of the approach (the FedSGD) achieved 82% accuracy on the CIFAR10 dataset (containing photos of animals).

Designing an FL-based system requires solving problems that are (typically) not present in other well-known ML approaches [DI-15]. These problems are related to the fact that data is in multiple locations. This has two main consequences: (1) cost of communication needs to be taken into account, and (2) data can be unbalanced in a peculiar (very serious) way, different from the situation when all data is in “one place”. The latter means that the probabilities of appearance of different categories of data differ between nodes. This happens even if the combined data set, (virtually) consisting of all local data sets, is well balanced. Consider the extreme case when all images of digit 1 are stored on server one, digit 2 on server two, etc. To solve both of these problems, a special algorithm for deep learning has been proposed. It is claimed that it can reduce the cost of communication between 10 and 100 times, compared to the traditional approach. The main ideas of the proposed approach were: (a) to delegate more work to the nodes, to deliver higher quality model updates, and (b) to use



a compression mechanism to reduce the communication overhead. Note that the on-device learning used in [DI-15] was the standard Tensorflow library.

The article [DI-16] focuses on solving the problem related to the communication between the FL participating nodes and the global server. Observe that, after iteration, each device sends its update to the server. Since it is quite possible that they finish their work in a “similar time”, this may result in a bottleneck (especially if a large number of nodes participates in local model training). Authors of [DI-16] and [DI-17] propose an encoding, which allows to reduce the size of transferred data by up to 32 times. The error related to this encoding method is also analyzed.

Article [DI-18] deals with the fact that the data may be unbalanced. Here, the authors propose is to reduce the number of iterations. To be able to achieve this (and keep the quality of the resulting model intact), they propose to: (i) increase parallelism, and (ii) increase the client-side computation in each iteration. The authors also note that deep learning applications most often rely on the stochastic gradient descent (SGD) method for optimization. Standard use of SGD, results in the need to carry out many iterations (even despite the use of additional techniques to improve the solution). This is acceptable in the case of standard DL. However, increasing the number of iterations involves the need to exchange the data between the client and the server, which should be avoided. In the cited paper, the FederatedAveraging algorithm was introduced, which combines local stochastic gradient descent (SGD), on each client, with a server that performs model averaging. And upgraded version of SGD was also presented with some added client-side computation, to decrease the number of rounds (by increasing the amount of computation in a round).

A slightly different approach to FL has been proposed in [DL-19]. This solution uses, so-called, SplitNN, and is limited to the neural network-based models. Here, in the training process, the client propagates the network forward for the initial N layers. Next, the result for the N-th layer is sent to the server with the correct category (label). The server propagates data forward, across the layers, calculates the gradient on the result of the last layer and the category, and propagates data backward. After making these calculations, the server calculates the gradient of the N-th layer and sends it back to the client. The article shows that this method is equivalent to the traditional treatment of the neural network as a whole. Various modifications and extensions of the algorithm are also proposed. The main difference, vis-a-vis the original approach, is that the clients exchange the network model among themselves. The publication discusses ways in which it is possible (after some modifications) to proceed without revealing private data to the server. As can be seen, the modified approach requires a lot more communication between the server and the client. The results of training were compared for different data and network architectures. They were also compared with other algorithms, including the original one (from [DI-18]). In the described cases, the SplitNN algorithm gave better results than the other algorithms.

Article [DI-20] describes a solution that works well for non-convex problems with unbalanced data. The algorithm is compared with the FedAVG. The authors note that the FedAVG performs well only under certain conditions, and that this may be due to the fact computing the gradient locally is not always a good solution. In response, the FedPD algorithm has been proposed. It is based on the Primal-Dual method. Experiments have shown that the algorithm learns much faster than the FedAVG (60% accuracy was obtained about 10 times faster).

Finally, let us note that the very recent publication [DI-21] discusses ML from the theoretical perspective. It formally defines the following models: Centralized Learning, Distributed Learning, and Federated Learning. The aim of the article is to determine the error for data that did not participate in the training. It also attempts at determining how much the network is overtrained. The final goal of the paper is to investigate the privacy offered by these models. It is important to stress that these issues have been examined only theoretically (no implementation has been attempted).

After summarization of core issues that lay the foundation of FL, let us now focus our attention on main developments concerning FL in selected application areas.

### **FL in medicine**

In publication [DI-13]) one can find a description of a framework that enables the use of FL in IoT devices, in the field of healthcare. The authors state that the solution presented by Google will not work in their area of interest, because IoT devices that are used in medicine, have much less computing power and battery capacity, compared to mobile phones. Also, typically, the available link speed is considerably lower, when compared to



mobile devices. To overcome these limitations, the authors used a shallow subnet that is trained on the device and a deep neural network that is trained in the cloud. In their research they used this approach to predict arrhythmias. Conducted tests showed slightly worse accuracy results – around 2% performance decrease. The second considered aspect was the reduction of the network traffic. Here, savings of over 90% were achieved, as compared to other approaches.

Continuing the topic of FL in medicine, article [DI-22] describes a solution for classifying signals from the electroencephalogram (EEG). The authors emphasize that, due to the need for personal data protection, in the field of medical informatics, there exist multiple small data sets that, due to privacy policy, cannot be combined into one large (training) data set. An algorithm using the method of covariance, based on neural networks, has been proposed. The article describes how signals are processed to constitute an input to the neural network. Next, an averaging method is applied, and the model is updated on its basis. The achieved results are satisfactory, compared to other algorithms. The proposed algorithm achieved an efficiency of 63%, while the best of the compared ones reached 66%.

Another healthcare usage example is described in the NVIDIA blog article<sup>53</sup>. It describes an example of using FL to support medical diagnostics. The main motivation behind this approach is, again, protection of patient privacy. Servers in hospitals train the global model on local data. Local results are sent securely to the global server. The Nvidia Clara platform<sup>54, 55</sup> is used to implement the proposed approach. It is an FL capable platform designed to process medical images and genomes.

The authors of [DI-23] describe their FL solution for processing medical data. The proposed approach is tested using the MIMIC-III database. The authors do not describe, in detail, the used algorithms, but only the components that they consist of. The client consists of three parts: the first for training, the second for communicating with the servers, and the third for performance testing. For the given categories of data inputs, satisfactory results (accuracy of 89-94%) was reported.

### FL and blockchain

The solution described in [DI-24] combines FL with blockchain technology. This approach is compared with the solution proposed by Google. Here, authors try to solve two main problems of Google's solution. The first is the server's susceptibility to failures, and the second is the lack of rewarding clients for the work put into training the model. The authors note that clients with larger datasets may be less dependent on collaborative learning, which may have a detrimental effect on the ability to deliver highest quality solutions for the users. The operation of BlockFL can be summarized as follows:

- The client trains the model locally
- The client sends the model to the associated miner with its local compute time.
- Miners broadcast the obtained local model updates. At the same time, the miners verify the received local model updates from their associated devices, or the other miners. The verified local model updates are recorded in the miner's candidate block.
- Each miner begins computing Proof-of-Work (PoW) until it finishes or gets a different block.
- Miner that first computes the PoW sends the block to other miners.
- Clients get the generated block from the associated miners.
- Customers update their model based on the block they receive

The conducted research shows that the proposed algorithm leads to faster learning than the one proposed by Google. It also achieves comparable effectiveness (95% and 98% for various parameters).

### FL and security

In [DI-25], FL is considered from the point of view of attacks on FL systems. Three types of attacks are investigated: direct attack, indirect attack, and a combination of the two. A direct attack is when a device that

<sup>53</sup> <https://blogs.nvidia.com/blog/2019/12/01/clara-federated-learning>

<sup>54</sup> <https://developer.nvidia.com/clara>

<sup>55</sup> <https://blogs.nvidia.com/blog/2019/12/01/clara-federated-learning/>

can participate in the training, sends incorrect data to the server. An indirect attack is when an attacker accesses a device on the network and then sends incorrect data. The attack consists in selecting the network coefficients to disturb the learning process as much as possible. The article presents a method of determining such an attack vector. The conducted research showed that, when using the proposed method, the mean error increased more than 4 times, from 5% to 23.88%, when the amount of data that has been infected is 20% (which may be seen, for instance, as one out of five nodes being infected). To prevent issues of “malware client’s model” it is recommended several approaches. For instance, to calculate average weights (of client’s model) and to compare it with global weights. If the difference is too big, in comparison with the other clients, than this model should be discarded.

In [DI-26] the authors state that existing FL solutions do not fully assure data security. To deal with this issue, a Multi-Party Computation (MPC) solution is proposed. MPC is a set of cryptographic techniques enabling confidential calculations on sensitive data. Moreover, two models: Peer-to-Peer and Two-Phase are compared. The Peer-to-Peer model involves the exchange of data between every two node pairs. Hence, it is demanding, due to the computational complexity, and thus not easily scalable. To solve this problem, the Two-Phase model is introduced. Both models were compared, in terms of the number and size of messages. The Two-Phase outperforms the Peer-to-Peer one, and the difference increases as the number of participants increases.

### Other application areas and related issues

In [DI-27] an FL-based solution for keyword detection is described. The model uses the encoder-decoder architecture. A modified FedAVG algorithm was used, in which the Nesterov accelerated gradients were used for the server-side updates. Various methods of server-side optimization were also compared, inducing Adam, Yogi and LAMB. The conducted research showed that, when using Yogi optimizer, the false reject rate decreased from 8.76% to 1.39%.

In [DI-28] a system supporting maintenance of industrial machines is proposed. In the classical approach, machine learning is based on local data available within each machine. Use of FL, allows to use data from business partners, without the need to share the actual data. Obviously, as emphasized in the text, FL applied in this case requires appropriate data preparation. For instance, the issue of data interoperability must be solved, so that each client is able to participate in training of a common model. Separately, it was decided that it is necessary to use appropriate metrics to distinguish between different types of “customers” (e.g., with automatic, or semi-automatic, production). The article discusses in detail individual elements of the proposed system.

The publication [DI-29] discusses the possibility of combining FL with Generative Adversarial Networks (GANs). GAN networks are used to generate elements in various categories. They consist of two components: a generator and a discriminator. The generator learns how to create elements like a given category of “objects”. The discriminator, on the other hand, learns to distinguish between true (correct) and false (incorrect) “objects”. The authors present a system, in which each client has a generator and a discriminator module. Clients also update the global (shared) generator and discriminator, located on the server. It is claimed that, due to the system consisting of two modules, the problem of model synchronization is much greater than with the, above described, FedAvg algorithm. In the paper, four methods of synchronization: synchronization of the generator, the discriminator, both elements, and lack of synchronization are considered and compared. For the real-world cases, where communication costs are very high, it is suggested that generator-only synchronization should be used. In other cases, use of synchronization of both generator and discriminator is proposed. More precisely, synchronizing generator and discriminator both as well as synchronizing only the generator achieved accuracy of about 99%. Synchronizing only the discriminator, and skipping synchronization, has obtained accuracy lower than 80%.

## 3.1.6.2 Relevant initiatives

### 3.1.6.2.1 Platforms powered by Federated Learning

Federated learning can be applied to image processing, realized by the FedVision application<sup>56</sup>, which aims at recognizing objects in images. In this context, the main advantage of FL is the reduction of data transmission. Here, data (large images) can be stored locally, while it is only a model that is communicated. It is enough for

<sup>56</sup> <https://www.fedai.org/cases/computer-vision-platform-powered-by-federated-learning>

the images to be tagged using a common set of labels. It has been used by three large-scale corporate customers. The platform has helped the customers significantly improve their operational efficiency and reduce their costs, while eliminating the need to transmit sensitive data around.

Another example of applying FL into real application is described in <sup>57</sup>. WeBank, the first digital bank established in China, has developed its federated learning model for credit rating. Here, authors of the platform support the claim that companies need to cooperate, but they cannot share their own data. FL is a solution in that situation. Their model is restricted to measuring the credit risk of small and micro-enterprises. It is claimed that, so far, the model has halved the number of defaults among WeBank's loans to these customers.

Healthcare giants around the world aim at developing a personalized AI for their doctors, patients, and facilities, where medical data, applications and devices are on the rise, while patient privacy must be preserved. NVIDIA offers an edge computing platform, which uses deep learning for radiology. Participating hospitals label their own patient data and train the global model. Platform preserves privacy by sharing only partial model weights. There are already partners (mostly in UK and US) who use the described solution.

The last example is an application for drug discovery<sup>58</sup>. Major pharmaceutical companies agreed to build common platform in partnership with NVIDIA, Owkin, etc. Authors claim that fewer than 12% of all drugs entering clinical trials end up in pharmacies and it takes at least 10 years for medicines to complete the journey from discovery to the marketplace. FL can accelerate this process. Authors also mentioned that they reached the first-year objective (out of 4).

### 3.1.6.2.2 Tools for Distributed and Federated Learning

Finally, let us summarize tools available for DL and FL. Material presented in this section is mostly based on [DI-30]. First, in Figure 45 and Table 21 we present tools directly devoted to DL, and related ones.

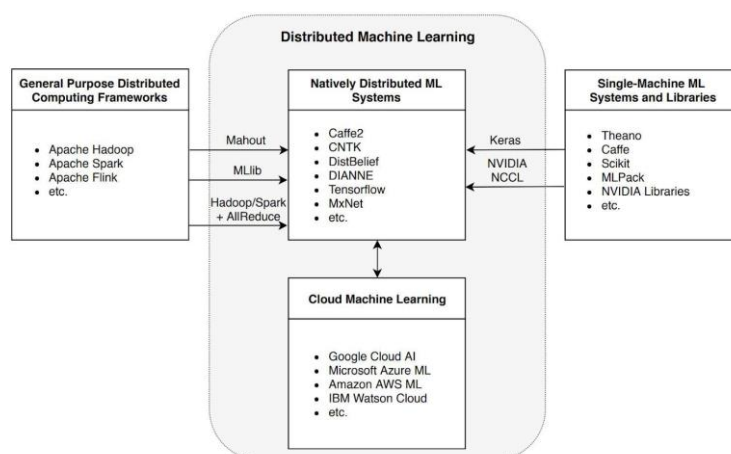


Figure 45. Tools for Distributed Learning

<sup>57</sup> <https://www.digfinngroup.com/webank-cluster/>

<sup>58</sup> <https://venturebeat.com/2020/09/17/major-pharma-companies-including-novartis-and-merck-build-federated-learning-platform-for-drug-discovery/>

Table 21. Known tools for distributed learning.

Tools for distributed intelligence	
Caffe2	pytorch api with multiple algorithms
CNTK	microsoft deep learning framework (cloud)
DIANNE	modular ML framework
Tensorflow	Google machine learning framework
MixNet	convolution neural network architecture, implemented in pytorch
Cloud Machine Learning	
Google Cloud AI	provides machines, cluster for ML on cloud
Microsoft Azure ML	more pyspark, some ready solutions, clusters, machines for ML on cloud
Amazon AWS ML	ready to train models or ready solutions, machines, clusters for ML on cloud
IBM Watson Cloud	ready to use ML algorithms and tools
Single-Machine ML Systems and Libraries	
Theano	python library and compiler to optimize math calculations
Caffe	ML framework
Scikit	python ML library
MLPack	c++ ML library
NVIDIA libraries	Rapids, cuBLAS, faster ML training
Tools for distributed learning <sup>59</sup>	
MapReduce and Hadoop	process data in a distributed setting
Apache Spark	loads to RAM memory
Baidu AllReduce	separate mini-batches of the training data
Horovod	adds a layer of AllReduce-based MPI training to Tensorflow Caffe2 - distributed machine learning through AllReduce algorithms
Apache Flink	tool for data streams processing working with AWS
Microsoft Cognitive Toolkit	data-parallel distribution

A slightly different, and more detailed, information about FL platforms can be found in Table 22, which is based on the same paper.

Table 22. Federated Learning Tools

Tools for federated learning	
syft.js	PyTorch and PySyft - javascript frameworks enabling to run visual training in browser
Threepio - PyTorch, TensorFlow.js, and TensorFlow	javascript library enabling to run visual training with Tensorflow and visualize it on browser
IBM Federated Learning <sup>60</sup>	python framework to build federated learning systems supporting Keras, PyTorch and Tensorflow
Federated Core	programming environment for implementing distributed computations, tensorflow federated
Federated AI Technology Enabler (FATE) <sup>61</sup>	distributed python framework with docker, k8s aligned to big data
KubeFate <sup>62</sup>	environment for distributed and federated learning using docker and k8s with python spark

<sup>59</sup> Many of the tools in this category use the Ring AllReduce under the hood

<sup>60</sup> <https://github.com/IBM/federated-learning-lib>

<sup>61</sup> <https://github.com/FederatedAI/FATE>

<sup>62</sup> <https://github.com/FederatedAI/KubeFATE>

Tools for federated learning	
Fate Cloud <sup>63</sup>	cloud infrastructure working with KubeFate
Fate serving <sup>64</sup>	high performance algorithms for FL working with KubeFate environment, wrote in Java (a lot of documentation is available in Chinese, only some in English)
Google TensorFlow Federated	python federated learning, tensorflow based framework created by Google
OpenMined PySyft <sup>65</sup>	python federated learning using pytorch 'A library for computing on data you do not own and cannot see' from github readme
Baidu PaddleFl	python, C++, GPU support library

Table 23. Comparison among existing Federated Learning Libraries

Supported features		FATE 1.3.0	TFF 0.12.0	PySyft 0.2.3	PaddleFL 0.2.
Operating systems	Mac	✓	✓	✓	✓
	Linux	✓	✓	✓	✓
	Windows	✗	✗	✓	✓
	iOS	✗	✗	✗	✗
	Android	✗	✗	✗	✗
Data partitioning	Horizontal	✓	✓	✓	✓
	vertical	✓	✗	✗	✗
Models	NN	✓	✓	✓	✓
	DT	✓	✗	✗	✗
	LM	✓	✓	✓	✓
Privacy mechanisms	DP	✗	✗	✓	✓
	CM	✓	✗	✓	✓
Communication	Simulated	✓	✗	✓	✓
	Distributed	✓	✓	✓	✓
Hardware	CPUs	✓	✓	✓	✓
	GPUs	✗	✓	✗	✗

### 3.1.7 Self-\*

#### 3.1.7.1 Context

With the growing scale of IT systems and amount of processed data, the need arises to introduce a new approach to computing called autonomic. Autonomic computing is a computer's ability to manage itself automatically through adaptive technologies which leads to (among others) reduced cost of ownership and maximized availability. The role of humans is then to manage the policy and not to maintain the mechanisms. Making intelligent decisions and self-management procedures based on data (including contextual) available within the ecosystem, close to the edge, allows deployment and execution of contextual applications. Self-awareness and semi-autonomy (extent of which is decided by a human) will allow the system to be prepared for, and react to, threats before they happen (e.g., a specific machine starts to fail) faster and with more accuracy, than possible in non-self-aware systems. The autonomic computing initiative (ACI) developed by IBM is inspired by the nervous system of the human body. In [SELF-1] IBM shows its idea about current computing vs autonomic computing.

IBM has defined the four types of property referred to as "self-star" (also called self-\*, self-x, or auto-\*) properties [SELF-2]:

- **Self-configuration:** automatic configuration of components,
- **Self-healing:** automatic discovery, and correction of faults,

<sup>63</sup> <https://github.com/FederatedAI/FATE-Cloud>

<sup>64</sup> <https://github.com/FederatedAI/FATE-Serving>

<sup>65</sup> <https://github.com/OpenMined/PySyft>



- **Self-optimization:** automatic monitoring and control of resources to ensure the optimal functioning with respect to the defined requirements,
- **Self-protection:** proactive identification and protection from arbitrary attacks.

Moreover, characteristics that every autonomic computing system should have include automation (being able to self-control its internal functions and operations), adaptivity (being able to change its operation) and awareness (being able to monitor its operational context as well as its internal state).

In papers by Poslad [SELF-3] or M.R. Nami and K.Bertels [SELF-4] another classification of self-\* capabilities is given that partially overlaps with what was defined by IBM:

- **Self-regulation:** maintaining some parameters, e.g., quality of service, within a reset range without external control,
- **Self-learning:** using machine learning techniques such as unsupervised learning which does not require external control,
- **Self-awareness** (also called **self-inspection** and **self-decision**): knowing itself, specifically the extent of its own resources and the resources it links to,
- **Self-organization:** structure driven by physics-type models without explicit pressure or involvement from outside the system,
- **Self-creation** (also called **self-assembly**, **self-replication**): driven by ecological and social type models without explicit pressure or involvement from outside the system; a system's members are self-motivated and self-driven, generating complexity and order in a creative response to a continuously changing strategic demand,
- **Self-management** (also called **self-governance**): managing itself without external intervention. What is being managed can vary depending on the system and application; self-management also refers to a set of self-star processes such as autonomic computing rather than a single self-star process,
- **Self-description** (also called **self-explanation** or **self-representation**): a system explains itself; it is capable of being understood (by humans) without further explanation.

In ASSIST-IoT we have decided to use the following classification (which may be affected by outcomes of SotA analysis):

- Self-learning
- Self-diagnose
- Self-adaptation
- Self-organization
- Self-configuration

Applying these capabilities should enable self-awareness and self-autonomy.

IBM has formulated eight conditions that every autonomic system should have [SELF-5]:

1. The system must know itself in terms of what resources it has access to, what its capabilities and limitations are and how and why it is connected to other systems.
2. The system must be able to automatically configure and reconfigure itself depending on the changing computing environment.
3. The system must be able to optimize its performance to ensure the most efficient computing process.
4. The system must be able to work around encountered problems by either repairing itself or routing functions away from the trouble.
5. The system must detect, identify and protect itself against various types of attacks to maintain overall system security and integrity.
6. The system must be able to adapt to its environment as it changes, interacting with neighbouring systems and establishing communication protocols.
7. The system must rely on open standards and cannot exist in a proprietary environment.

8. The system must anticipate the demand on its resources while keeping transparent to users. [SELF-6] is a good summary of available techniques for autonomic computing.

#### 3.1.7.1.1 Cognitive networks

In the field of autonomic computing well known is the concept of cognitive networks [SELF-7]. The concept comes from cognitive radio networks [SELF-8], which are based on self-awareness and context-awareness requirements that are motivated by complexity, especially of wireless networks. They can perceive current network conditions and then planning, learning, and acting according to set goals. Cognitive network elements (entities with reasoning capabilities) are involved in a cognition loop which aims at improving current performance based on past experiences. In the context of cognitive radio networks, the wireless communication system should be aware of the environment and its changes (sense unused spectrum in specific time and location) and adopt transmission parameters accordingly.

#### 3.1.7.1.2 Autonomic Internet-of-Things systems

The concept of autonomous Internet-of-Things systems is a design metaphor close to the paradigm of multi-agent systems (MAS). MAS [SELF-9] is a system composed of multiple interactive intelligent agents (software agents) that should be autonomous (at least partially independent, self-aware), with local view on the system, decentralized (no agent is designated as controlling). Recently, the MAS featured of self-steering and embedded intelligence generated a synergy between agent-based systems and biology-inspired paradigms of autonomic computing [SELF-10]. Authors give examples of four autonomic and cognitive IoT architectures: Cascadas [SELF-11], Focale [SELF-12], Inox [SELF-13], I-Core [SELF-14] with comparison. With respect to self-\* capabilities, they identified: Cascadas with self-organization, -adaptation, -protection, -healing, -configuration, Focale with self-adaptation, -governance, Inox with self-management, -healing, -organization, -protection, -adaptation, -configuration, I-Core with self-healing, -protection, -organization, -optimization, -configuration.

Authors of [SELF-15] treat the IoT system as MAS where the agent abstraction is a suitable paradigm to instill smartness and autonomy within a single object. They propose ACOSO (Agent-based Cooperating Smart Objects) middleware that should enable development of interoperable, autonomic, and cognitive IoT.

In [SELF-16] a paradigm of autonomic computing is introduced for dynamic secure management use in IoT.

*“Autonomy in IoT can be realized by implementing self-managing systems. Self-management is the property of a system to achieve management and maintenance of its resources intrinsically and internally. Management and maintenance is realized through many levels of decision making. In IoT, the management scope extends to access management, device management as well as service management.”*

The adoption of the autonomy in IoT architecture can prove to be a valuable addition to IoT systems.

#### 3.1.7.1.3 Organic computing

Organic computing [SELF-17] [SELF-18] is an emerging paradigm with emphasis on self-control and self-awareness that can be considered an extension to IBM's vision of autonomic computing. The field of organic computing aims at translating well-evolved principles of biological systems to engineering complex system design [SELF-19]. Organic computing systems adapt dynamically to exogenous and endogenous change. Examples of applications include robotic systems. It is characterized by the properties of self-organization, self-configuration, self-optimization, self-healing, self-protection, self-explaining, and context awareness. An OC system typically consists of a potentially large set of autonomous and self-managed entities, where each entity acts with a local decision horizon. Each entity in an ensemble implements a multi-layered observer/controller (O/C) system design concept that allows for local, and coordinated, global optimization of the ensemble's behavior [SELF-20].

### 3.1.7.2 Scientific review

#### 3.1.7.2.1 Autonomic architecture

In this section different approaches to realize architecture supporting autonomic capabilities are outlined.

To achieve autonomic computing, IBM has suggested a reference model for autonomic control loops, which is sometimes called the **MAPE-K** (Monitor, Analyse, Plan, Execute, Knowledge) loop [SELF-2]. The MAPE-K autonomic loop is similar to, and probably inspired by, the generic agent model proposed by Russel and Norvig, in which an intelligent agent perceives its environment through sensors and uses these perceptors to determine actions to execute on the environment. In the MAPE-K autonomic loop, the managed element represents any software or hardware resource that is given autonomic behaviour by coupling it with an autonomic manager. Sensors collect information about the managed element, whereas effectors carry out changes to the managed element. The data collected by the sensors allows the autonomic manager to monitor the managed element and execute changes through effectors. IBM has developed a prototype implementation of the MAPE-K loop called the Autonomic Management Engine, as part of its developerWorks Autonomic Computing Toolkit.

In **Autonomic Control Loop** [SELF-2] the complete system can be described as a graph of interacting feedback loops. Feedback loops can interact in two main ways: (1) where both loops affect interdependent system parameters, i.e., they interact through their environment, (2) where a loop manages another loop, i.e., the first loop continuously adapts the policy implemented by the second loop. In both cases, the system's global behaviour depends on all the feedback loops taken together.

**LRA-M** stands for learn-reason-act-model. It is a high-level description of a self-aware and reasoning system. To better understand this, we will use graph coming from [SELF-21].

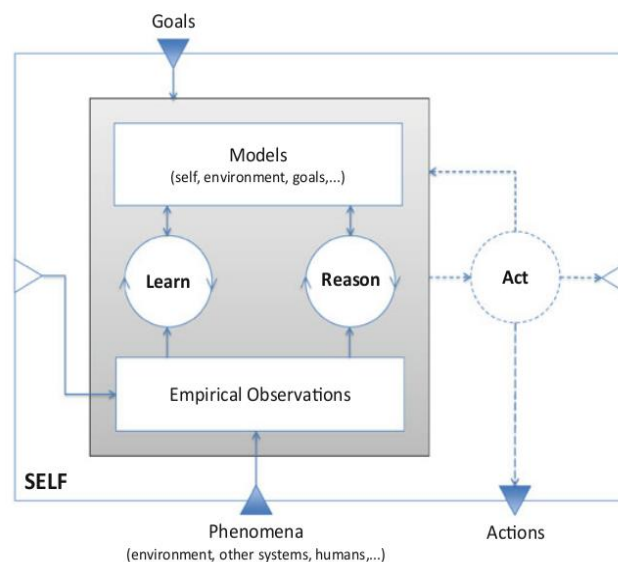


Figure 46. LRA-M architecture

The idea behind this architecture is general enough that it is almost necessary to address all the elements mentioned during creating a self-aware system. Authors of [SELF-22] describe elements of the system as follows. System collects external *phenomena* and *internal observations* that then is used to produce *models* according to the high-level system *goals* via *learning* and *reasoning* processes. High-level goals might change during life- and runtime of the system. Based on the built knowledge system may decide to *act* both on itself internally and on the environment externally. It is worth noting that authors of [SELF-23] also include architecture elements and concepts represented by UML to propose a tool for architecture modelling.

Kramer and Magee [SELF-24] proposed a three-level architectural model for self-managed systems (**Kramer and Magee's Three Layer Architecture**). The three layers are: Component Control, Change Management and Goal Management. Component control layer is responsible for the interconnection among components to facilitate the information about components statuses. In this layer occurs deployment, undeployment and interconnection of the system components. Change management layer is responsible for the execution of plans, i.e., actions that address context changes. The actions taken in this layer might include the introduction of new components, changes in the interconnection or even in the operational parameters. Goal management level produces plans needed from the layers. In this layer the introduction of new goals takes place as a consequence of the changing environment that may require behaviour modifications in order to achieve its goals or modify goals.

In development for 30 years, **Soar** [SELF-25] (originated from state, operator, and result) is a cognitive architecture for developing systems that exhibit intelligent behaviour that specifies fixed building blocks necessary for general intelligent agents. Soar integrates knowledge-intensive reasoning, reactive execution, hierarchical reasoning, planning, and learning from experience, with the goal of creating a general computational system that has the same cognitive abilities as humans. The latest version of Soar includes extensions such as adding reinforcement learning, semantic memory, episodic memory, mental imagery, and an appraisal-based model of emotion. Soar is divided into three levels: memory, decision, goal.

The **Autonomic Computing Reference Architecture (ACRA)** [SELF-26] provides a reference architecture to organize and orchestrate autonomic systems using autonomic elements, where an autonomic element is an implementation of the MAPE-K model. ACRA-based autonomic systems are defined as a multiple-layer hierarchy of MAPE-K elements, which correspond to orchestrating managers and resource managers, controlling managed resources. Whereas other models are based either on a single MAPE-K loop element or on a three-layer structure of MAPE-K loop elements, in ACRA each layer adds autonomic control over the layers below it. Another difference to other models is that ACRA defines generic responsibilities for its layers instead of specific responsibilities for each layer.

**DYNAMICO** is a Reference Model introduced in [SELF-27]. Authors identifies that for system to be context-driven and self-adaptive it must consist of at least three parts: a *control objectives manager* – responsible for regulation of systems requirements both functional and non-functional, *adaptation controller mechanism* – responsible for achieving adaptation goals and preserving system properties in changing environment; and *context manager* which is responsible for dynamic context monitoring. They realize this design by introducing three feedback loops: *control objectives feedback loop* (CO-FL), *adaptation feedback loop* (A-FL) and *monitoring feedback loop* (M-FL). By effectively separating three types of system concerns they allow each component to adapt in an independent way. This allows identification of components when building adaptive systems - as according to authors - systems monitoring feedback loop of that type must realise all three of those loops.

**DEECo** Component Model (Distributed Emergent Ensembles of Components) was developed in ASCENS EU project (within FP7) [SELF-28] focused on self-aware, self-adaptive systems from components. The proposed model addressed the problem of the dynamic and changing environment of massively distributed ad-hoc networks. The component is an independent autonomous unit responsible for computation and sensing/actuating with local knowledge executing processes (periodic or event-based) performing computation over the local knowledge. Ensemble is a group of components cooperating for a common goal that may be formed dynamically and synchronize knowledge.

Usage of DEECO framework is popular when creating autonomous components as in [SELF-29-31]. Unfortunately, the jDEECO Java-based implementation of the model has not been updated for 4 years.

**models@run.time Systems** core characteristic of model@run.time architecture defined in [SELF-32] is a clear separation between two systems: manager and managed.

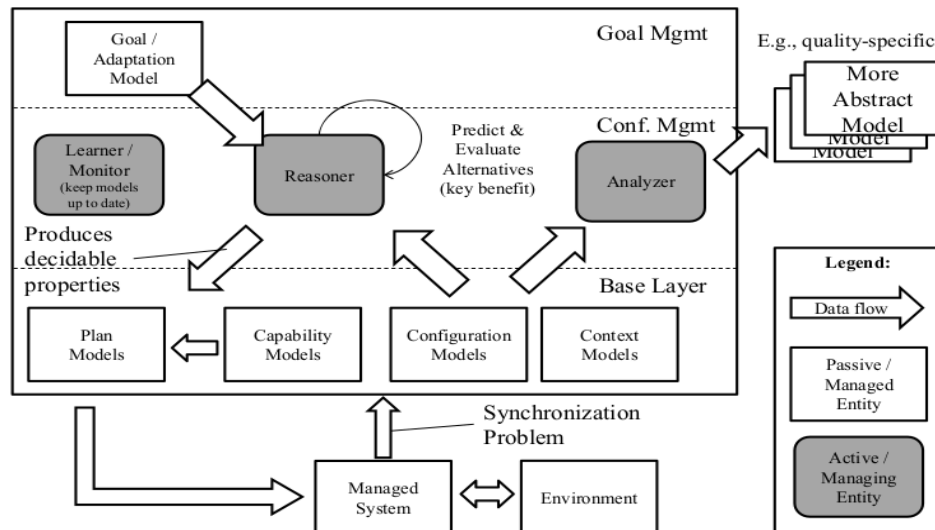


Figure 47 model@run.time architecture.

Brief description comes from [SELF-33]: *The managing system, [...], can often be subdivided into three layers [...]. The bottom layer, interfacing with the managed system, is comprised of models covering different concerns of the underlying managed system. The configuration model, often also simply called runtime model, reflects the current state of the underlying system. Additional models cover the managed system's capabilities (e.g., for adaptation, but also for use), not only context models focusing specifically on the managed system's environment, but also plan models constituting specifications of how to act upon the managed system. The middle layer consists of three active entities: a reasoner, an analyzer, and a learner. The learner is responsible to keep all models of the lower layer in sync with the managed system. The analyzer provides means to further abstract (i.e., decompose) the managing system, which enables a hierarchical decomposition of models@run.time systems. Finally, the reasoner is in charge of processing the models from the lower layer with the aim of decision making. The reasoner also takes the third layer into account, which typically comprises requirements and goal models.*

**Cyberphysical-System-on-Chip (CPSoC)** is an architecture that “combines sensor-actuator-rich C3-centric paradigm with that of and adaptive and reflective middleware to control manifestations of computations on the physical characteristics of the chip itself and the outside interacting environment” [SELF-34]. The architecture itself consists of three main parts: sensor-actuator platform, Introspective Sentient Units (ISU) and an adaptive and reflective middleware. Moreover, this architecture is divided into five abstraction layers: applications, operating system, network/bus, hardware architecture, device/circuit architecture. Each of the layers is equipped with a set of sensors and actuators to enable self-aware features for each layer separately. This architecture supports following concepts: Cross-Layer Virtual and Physical Sensing and Actuation, Simple and Self-Aware Adaptations, Online Learning, Multi- or Cross-Layer Interactions and Interventions (for more detailed discussion please see [SELF-35]). It is worth mentioning that authors also developed a smart linux load balancer SmartBalance [SELF-36].

**SOTA** [SELF-37] stands for “State of The Affairs” is a robust and powerful framework providing conceptual support for self-adaptive systems. Idea behind this model is to represent a system using n-dimensional complex dynamic system tools. Each dimension of SOTA space represents either internal software or external environmental parameters. Then the behaviour of the system (including self-adaptive behaviour) can be modelled as a movement in aforementioned space. Goals are related to areas that the system must reach, non-functional requirements could be represented as trajectory and self-adapting behaviour is an ability of a system to “come back” to proper trajectory in case it diverged from it.

### 3.1.7.2.2 Self-\* capabilities

#### Self-adaptation and self-configuration

The systematic literature review done for self-adaptation in cyber physical systems is presented in [SELF-38]. Results are: *“The primary concerns of adaptation in CPS are performance, flexibility, and reliability. 64% of*



*the studies apply adaptation at the application layer and 24% at the middleware layer. MAPE (Monitor-Analyze-Plan-Execute) is the dominant adaptation mechanism (60%), followed by agents and self-organization (both 29%). Remarkably, 36% of the studies combine different mechanisms to realize adaptation; 17% combine MAPE with agents. The dominating application domain is energy (24%).”*

Authors of [SELF-39] describe the framework for self-managing devices, comprising measurement-based learning and adaptation to changing system context and application demands. The framework supports agent-based adaptation capabilities.

Another direction in self-aware systems presented in [SELF-40] where authors add another dimension of self-adaptivity - Field Programmable Gate Arrays. FPGA is a circuit that can be dynamically modified during runtime. This means that not only software can be adaptive, but also the hardware itself. They introduce the *Elastic IoT platform* which is relatively mature (compared to projects presented in other papers).

### Self-awareness

Self-aware computing systems [SELF-41], [SELF-42], [SELF-43] are a subclass of autonomic systems that maintain knowledge about the applications state and environment and then use this knowledge to reason about and adapt behaviors (referred also as self-expressive capabilities). Self-aware computing has received attention in application areas such as: security, IoT [SELF-44], cloud, automotive and robotic. Authors of [SELF-45] introduce self-aware computing as a design approach for IoT applications which is centered around a self-aware architecture for IoT nodes.

It is worth noting that [SELF-46] provides alternative (to [SELF-47] and [SELF-48]) definition of self-aware system:

*“Self-aware computing systems are computing systems that:*

- learn models capturing knowledge about themselves and their environment (such as their structure, design, state, possible actions, and runtime behavior) on an ongoing basis,*
- reason using the models (e.g., predict, analyze, consider, and plan) enabling them to act based on their knowledge and reasoning (e.g., explore, explain, report, suggest, self-adapt, or impact their environment) in accordance with higher-level goals, which may also be subject to change.”*

Notion of *higher-level goal* is introduced to emphasize that those goals are not under direct control of the system, hence the abstraction level is higher than that of a system.

In [SELF-49] following properties of self-aware systems are proposed: introspective, adaptive, self-healing, goal-oriented, approximate. It represents a different level of control to one that we describe in the introduction.

Authors of [SELF-50] propose a conceptual framework that consists of three main concepts:

- Levels of self-awareness (pre-reflective, reflective, meta-reflective),
- Aspects of reflective self-awareness (scope and span),
- The domain of self-awareness (type of objects system works with).

Authors of [SELF-51] propose an interesting set of metrics for self-aware systems.

Goal fulfillment	Monitor	Analyze	Plan	Execute
Proportion of time the system is in a goal fulfillment state	Levels of self-awareness	Number of input sources utilized	Proportion of “correct” decisions made per time unit	Proportion of time the system is in an oscillating state
Duration/amount of goal violations per time	Number of monitored internal and external properties	Sophistication of the learning mechanism	Sophistication of the reasoning processes	Duration of an adaptation action
Severity of goal violations	Granularity/precision of sensing the environment	Accuracy of the learned models w.r.t. reality	“Precision and recall” of the selected adaptation actions	Correctness of the adaptation actions
Level of goal fulfillment	Size/length of the historically stored properties	Duration of altering the learning process upon changing goals	Extent/granularity of traceability for reasoning	
	Monitoring frequency			
	Monitoring overhead			
	Completeness of the collected and required information			
	Number of required user inputs per time			

Figure 48. Metrics for self-aware systems [SELF-51].

### Node-level and Network-level self-awareness

In paper [SELF-52] authors base their work on reference architecture defined in [SELF-53], the difference authors introduce is clear separation between *node-level* self-awareness and *network-level* self-awareness.

Node level self-awareness concert is limited to a single device and its immediate environment. Example provided by the authors is being able to select different algorithms based on external stimulus (e.g., lighting), internal stimulus (low battery) or changing goals while trying to overcome some obstacle. Network level self-awareness handles interactions between devices - it focuses on data incoming from many devices rather than local knowledge. It helps devices by being aware of the state, capabilities, and goals of other devices - to ensure that each node is able to make more complex decisions based on other devices' intended actions. Network-level self-awareness generates knowledge based on state, capabilities of many devices taking into consideration local objectives and constraints. Authors of [SELF-54] also performed an experiment in Cooperative Multi-robot Observation of Multiple Moving Targets using the SimTool camera network simulation tool. They defined node-level self-awareness as the ability to “*make an individual decision whether to follow an object of interest or not*” and whether to request help from others - that decision is also individual. Authors define network-level self-awareness tracks current engagement of all the cameras. Having this knowledge allows a particular node to respond to received help requests. Moreover, the network keeps information about what object each camera is currently observing.

### Self-diagnose

#### Fault classification

To talk precisely about the ability to diagnose issues within any system it is reasonable to first define faults that can occur in it, as in Table 24. Fault classes below were defined at [SELF-55] and are still used in latest surveys [SELF-56]. It is worth noting that [SELF-57] classifies faults in many more dimensions than those mentioned here.

Table 24. Fault classes levels

First level fault class	Second level fault class
Phase of creation or occurrence	Development
	Operational
System boundaries	Internal
	External
Phenomenological cause	Natural
	Human-made

First level fault class	Second level fault class
Dimension	Hardware
	Software
Objective	Malicious
	Non-Malicious
Intent	Deliberate
	Non-deliberate
Capability	Accidental
	Incompetence
Persistence	Permanent
	Transient

Authors of [SELF-55] also introduces three types of faults which all of the above classes can give even more precise classification:

- Development faults - were introduced during development
- Physical faults - all faults that are caused by messy, physical nature of hardware
- Interaction faults - various faults that can be introduced during interacting with the system during runtime

It is rather clear that any break-through design should address all of those faults. Authors of [SELF-56] give detail survey of fault-detection techniques.

#### Redundancy based fault detection

If a system has a redundant, additional source of data that allows techniques that are based on comparing actual data sources with information coming from the redundant ones. That includes techniques like majority voting, lockstep execution or Triple Modular Redundancy. We are currently used to the fact that most cloud systems are designed with redundancy in mind as users are expecting constant and low latency access all the time. This is not so trivial when it is within the context of IoT as we cannot expect or guarantee that everyone will have multiple copies of the same device.

#### Specification based fault detection

Those techniques are based on system specification - expected and defined behaviors using models like hybrid systems. Of course, using a model of a system will always introduce approximation error, moreover exhaustive verification of a hybrid system is in general undecidable and is usually used during system design.

Another technique is specification-based runtime monitoring - also based on hybrid system models. Given both continuous and discrete variables characterizing systems we can monitor and decide whether runtime system behaviour is in accordance with our expectations.

*Falsification-based analysis and parameter synthesis* is an approach, which given a system model one can try to synthesize inputs that will falsify that model.

Signature-based intrusion is based on a priori knowledge of system behavior (called signature) that is then compared with runtime behavior. This approach requires calibrating signature, which is a non-trivial task. Moreover, if there is a new type of fault - signature-based detection will not be able to detect it.

#### Anomaly-based detection

Most natural approaches for anomaly-detection are statistical based. If a system generates a behavior instance that is highly unlikely to be generated, the system can claim that it is an anomaly. If distribution parameters are not known, then either estimation or machine learnings techniques have to be deployed. Those techniques are nowadays replaced with neural networks which are more robust tools for multivariate and non-linear data.

Machine learning/data mining techniques - various machine learning techniques can be deployed to classify data point as an anomaly, to just name a few: Neural Networks, SVM, Bayesian Networks, KNN. One of the advantages of this approach is no prior domain knowledge of the system is required, another is ability to re-train models on constant inflow of data.

Information-theoretic techniques are usually based on the entropy of the information. When information content exceeds a threshold then system can mark that data point as an anomaly.

### Graph theory-based detection

Graph based techniques are ubiquitous in network analysis and that of course includes IoT networks. One of the most popular techniques for diagnosed networks was introduced back in 1967 [SELF-57], where concepts of  $\kappa$ -diagnosability and *diagnostic graphs* (although there were not named like that in the paper itself). a  $\kappa$ -diagnosable network can identify all faulty nodes of a network as long as the number of faults does not exceed  $\kappa$ . Authors of [SELF-58] generalize this model to include temporal dimensions and heterogeneous outputs of the network by introducing *temporal diagnostic graphs*. It allowed them to introduce *PerSys* - framework for fault diagnosis in perception systems (implemented in python). PerSys framework was then used in autonomous vehicle simulation which improved results as compared to regular *diagnostic graphs* by 60% compared to SotA open-source autonomy stack (Apollo Auto). Another important result in [SELF-58] is the observation that adding edges to the temporal diagnosability graph can only improve overall  $\kappa$ -diagnosability.

### Fault localization

Truly self-diagnosing system should be capable of localizing faults. Two most common approaches are root-cause analysis. A lot of literature is available on the topic, mostly coming from software engineering. Other approaches usually are based on statistical techniques, for example spectrum-based fault localization which provides ranking of most probable faulty components.

### **Self-security**

A definition of self-security could be found in Tahir et al. [SELF-59] where it is described as the capability of an IoT system to self-heal and self-protect. System malfunctions are detected by the self-healing components triggering corrective actions that are based on policies without any disruption to the IoT environment. The difference between the two security mechanisms, self-heal and self-protect, are discussed in Ashraf et al. [SELF-60] work. Self-protection is the adoption of cryptographic techniques against studied attacks to pre-emptively prevent the attacks. While the self-healing adopts is easier to accomplish as it occurs after the attack detection. Finally, there are hybrid techniques that bridge the two notions together.

A comprehensive taxonomy on the threat mitigation has been unveiled in Ashraf et al. [SELF-60] based on the layer, actor, and approach. The layers on the approach are in common with the IoT environment as they cover machine-to-machine communication, network, and cloud infrastructure. The following figure visualizes the aforementioned work in a descriptive way.

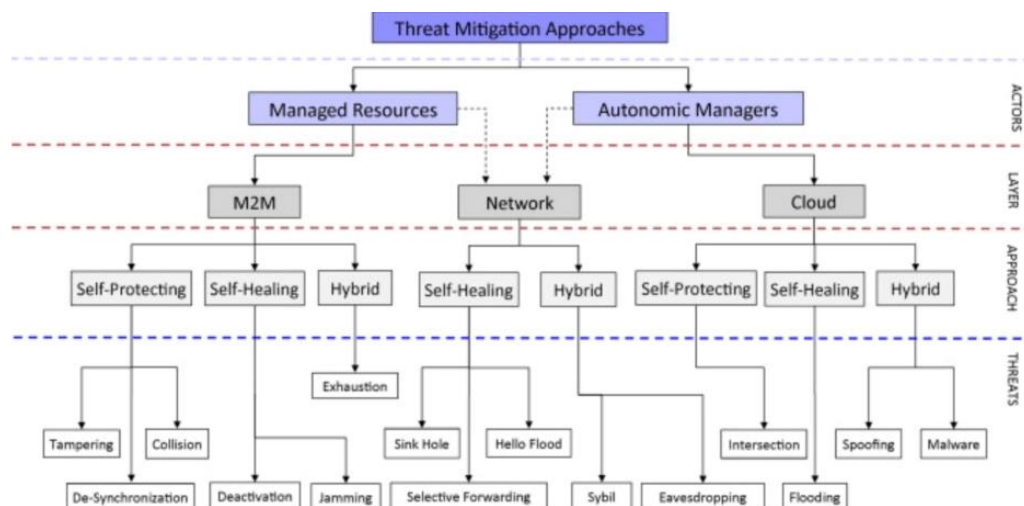


Figure 49. Self-security taxonomy [SELF-60]

In an attempt for a more trustworthy IoT, Msadek et al. [SELF-61] have suggested a solution named Trust-Enabling Middleware (TEM). The proposed middleware architecture goal is to provide trust to the self-\* capabilities by refining the distributed Observer/ Controller architecture. The refinement of the architecture is achieved by the abolishment of the benevolence assumption. The Observer's task is to track the IoT node and

measure the trust based on the information from the trust data. Self-\* properties are implemented onto the trust data for accomplishing the system's overall goal in a trustworthy manner. Different metrics for measuring trust could be applied. The suggested in this work incorporate direct trust, reputation, and confidence. Tweaks and changes are, also, suggested to the controller in order to achieve a self-organization process between the nodes. The nodes are not considered definitely as benevolent, but the design adopts self-\* properties to lead to the robust operation in all the environments. The controllers in this design take into account the observer's trust data to make decisions. The global system is affected by the controllers as rules are executed by following the self-\*properties. These properties are trustworthy self-configuration, trustworthy self-optimization, simultaneous self-optimization, and trustworthy self-healing.

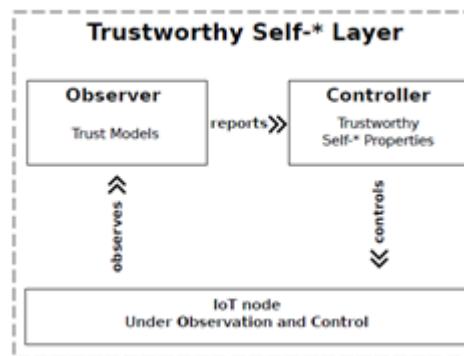


Figure 50. Observer/Controller architecture used for the trustworthy self-\* layer [SELF-61]

A framework has been proposed by Ge et al. [SELF-62] for automatic security analysis. The framework's goals are to pinpoint potential attack paths and to alleviate the attacks' impact. The framework is based on extending the Hierarchical Attack Representation Model (HARM) for pinpointing the paths and on the Symbolic Hierarchical Automated Reliability and Performance Evaluator (SHARPE) for the analysis. The framework is divided into 5 distinct phases which are: the data processing; the generation of the security model; the visualization of security; the security analysis; and the update of the model. In the first phase, the security decision maker provides system information and security metrics as inputs for IoT network construction. In the next phase, the data are fed to the extended HARM model. The third phase is the visualization of HARM model. The fourth stage is the security analysis where the attack path acts as an input to the Security Evaluator. The Security Evaluator could export the file into the SHARPE which sequentially computes the security analysis. The final stage, the security decision maker makes a choice on the appropriate defence strategy based on the results.

Notable research has been performed in the radioactive material sector as the materials call for ensuring security. Self-security is a notion that has gathered the interest and found its place in applications. The first work in the radioactive material sector is done by Zeng et al. [SELF-63] who propose a four-layer defence. The self-security is done by attaching a device on the containers of the materials with numerous capabilities. One of the capabilities of the node is the ZigBee communication that will flag any node that is compromised to the network as the node will disconnect from the network due to its movement.

Another work on radioactive materials has been researched in Zeng et al. [SELF-64] on the swarm self-security intelligence system. The container is equipped with a security device that is considered as a decentralized node. The network permits the communication between adjacent nodes which consequently allows a node to communicate with up to six other nodes in the network. In essence, a group of parallel computing is formed between the nodes. There are two modes for the state of nodes: the silent and the alert mode. The nodes in the silent state communicate with the rest of the network to confirm their existence. In this state, a node is recognised by the network via its name. The node recognition swifts to a node's unique number once the state changes to alert. The network's security is ensured by imposing identity authentication and encryption in the transmitted data.

### 3.1.7.2.3 Software Engineering aspects of self-\* and IoT systems

Author of [SELF-65] introduces a principled software engineering approach for the systematic development of IoT systems and tries to frame the key concepts around the design and development of IoT systems and IoT



applications. In the article it is pointed out that one of the more natural approaches is to consider IoT in terms of Web Services which allows taking from the great body of knowledge in that area. Articles define “IoT System” as “*overall set of IoT devices and to the associated middleware devoted to manage their networking and interactions*”. The author introduces all necessary abstractions that are required for defining and designing IoT systems. Please see below various elements that the author introduced in the paper.

Logically system could be divided into two types of elements:

- Services – means to enable users to access and use individual Things and control their sensing/actuating as well as coordinated services that do the same for a group of Things.
- Applications – means to regulate functioning of (parts of and overall) IoT system to ensure overall consistent behaviour of the system, access to the system itself and configuring it.

Three high level types of actors in the system are defined, which are aligned with the usual approach of modelling authorization:

- Global Managers – owners, can control configuration, access, overall usage of services and applications. Interesting question is about the existence of a global manager for a big enough IoT network - does the Internet itself have a global management?
- Local Managers – owners of a subset of IoT infrastructure. Usually control some specific application of the system.
- Users – people that access and use IoT applications and services.

Overall functionalities defined by IoT system are classified as follows:

- Policies – describe desirable permanent configurations or states of functioning of an overall IoT system and call them global policies. In turn local policies describe the above for a subset of the system. Aim of those is to regulate the IoT system. Policies can target both software and hardware configurations.
- Goals – express desirable situations that can or should be activated. Activation of goal might be triggered by some specific event or configuration or might be activated on user request.
- Functions – define the sensing, computing and actuating functionalities of individual or grouped resources. Functions can be made available via a service which might include usage and coordination of multiple functions.

Basic abstraction that is introduced is called Avatar. Avatar is one of the unifying abstractions for “things” in the IoT system. “*Avatar is a general abstraction for both individuals and groups of things that logically define a unique concept*”. Abstracted Avatar is not concerned with the specific characteristic of things they represent as well as how they are internally coordinated. In turned Avatars are identified by:

- Identity – every avatar has a unique identity and is addressable. If avatar represents group of things, then it is not necessary to hide addresses of components.
- Services – services are means of using the particular capabilities of avatars.
- Goals – goals can be optionally linked with Avatars and represent desired state of the affairs.
- Events – events are published by an avatar and might be detected and used by the same or other avatars.

Avatars might be grouped into a Coalition - which might be temporary or permanent - that coordinate each other's activity to either reach a goal or enforce policies. As opposed to avatars, coalitions do not have to define an identity or provide services. Also, a coordination scheme is introduced, which defines minimum requirements for defining coalition. Coordination scheme includes:

- Rule for membership
- Coordination pattern
- Coordination law

This gives quite a comprehensive set of abstractions which make thinking and reasoning about the IoT system more concrete.

Another approach presented in [SELF-66] is named Fluidware. Authors propose an idea to represent groups of IoT devices (from smallest to largest) as “sources, digesters and targets of distributed flows of contextualized events, carrying information about data produced and manipulated over time”. Then they propose that services and applications can be represented as transformations of aforementioned flows by using a “funnel process” which should be specified in a declarative way that would be managed by Fluidware itself. It is a promising idea especially given the fact that event processing is a well-established and popular framework in software engineering.

#### 3.1.7.2.4 Other projects

The European government has funded autonomic computing research projects for several million euros via the FP6 and FP7 programs, and the US government has funded research in this field as well.

The concept of autonomic computing emerged in EU projects before 2009. EU FP6 CASCADAS [SELF-67] the project was driven by a clear research vision, which is to define a new generation of composite, highly distributed, pervasive services, with underlying technology, that addresses computing resources configuration and complexity problems. The objective was to identify, develop, and evaluate a general-purpose abstraction for autonomic communication services, in which components autonomously achieve self-organisation and self-adaptation towards the provision of adaptive and situated communication-intensive services. Similar concepts were investigated in EU FP6 Grid4All project [SELF-68] which aimed to enable domestic users and non-profit organisations to share their resources and to access massive grid resources when needed, envisioning a future in which access to resources is democratised and cooperative. The self-\* dynamic grid systems addressed p2p techniques for self-management/adaptability/dynamicity, on-demand resource allocation, heterogeneity, and fault tolerance. In general, the concept of grid computing acted as an enabler for autonomic mechanisms.

EU FP7 REFLECT project [SELF-69] aimed at developing new concepts and means for pervasive-adaptive systems. Research was done on sensing user moods and intentions in order to perform actions to optimize user comfort. A software framework with a set of practical tools was developed which can be used for building pervasive, adaptable, self-organized systems that seamlessly collaborate with users and control their environments. EU FP7 SafeAdapt project's [SELF-70] goal was to develop novel architecture concepts based on adaptation to address the needs of a new electric/electronic architecture for fully electric vehicles regarding safety, reliability and cost-efficiency. The context of studying autonomy in these projects is different than in ASSIST-IoT.

H2020 WearHealth [SELF-71] provided smart devices monitoring bio parameters for a workforce 4.0 in different manufacturing application domains. H2020 PLEDGER [SELF-72] provided a tool suite to validate and evaluate the performance of applications supported by edge computing architectures. These two projects however do not reference self-\* capabilities.

In 2004 IBM released Autonomic Computing Toolkit 2.0 [SELF-73] which is a collection of technologies, tools, examples, scenarios and documentation for those who want to develop autonomous behavior in their products. Unfortunately, it has not been updated ever since.

### 3.1.8 Human-machine interfaces for collaboration

The fourth industrial revolution has already started and is leading the way to an era where production systems, machines, operators, products, and services are all digitalized and conventional centralized systems are not required. The Industry 4.0 concept, which is based on cyber-physical systems, big data analytics and the Internet of Things paradigm, is already current practice for many companies, even though many of the enabling technologies have not yet reached the required maturity [HMI-1]–[HMI-3].

The IoT provides a framework for the development of hybrid solutions that combine digital services and physical products [HMI-4]. One of the most important aspects of human-centric IoT applications, with respect to building trust in intelligent systems, is the information exchange through human-machine interfaces [HMI-5]. From the user's perspective, human-machine interaction can be analyzed as follows; the physical aspect determines the interfaces and the mechanics of the interaction, the cognitive aspect deals with the user's understanding of the system and the affective aspect is concerned with the user's satisfaction and engagement levels [HMI-6]. The most suitable and widely used interfaces for IoT applications lie within the augmented

reality end of the virtuality continuum [HMI-7]. Whereas this continuum provides a taxonomy of visual-based mixed-reality systems, there exist other sensory modalities [HMI-6], namely auditory, somatosensory, taste and olfactory, which have been used in various application domains [HMI-8], such as:

- teaching, science, and healthcare
- training and safety management
- design and prototyping visualization
- construction, ship building and manufacturing
- quality control and predictive maintenance
- logistics operations and warehouse management
- visualization of the location of objects and hidden assets
- remote assistance for mechanical equipment maintenance, installation, assembly, etc.

### 3.1.8.1 Scientific review

There are three types of visual-based systems, which is considered the most powerful modality. In video see-through mode, which is suitable for remote applications, the user views the world through a portable or static, display and not directly; therefore, the experience is affected by the, usually low, resolution of the camera and the limited field of view. The optical see-through type provides a direct perception of the real world that is combined with computer-generated content superimposed through head-mounted semi-transparent mirrors (monocular, biocular or binocular). The main advantages are that the user has an unmodified view to the real world without any delays and it does not create discomfort after long use. The projection-based technology allows the projection of digital content directly on the real object and can accommodate more than one user, but these setups are usually not mobile and are susceptible to self-occlusions. The main technical challenges and selection criteria for a particular application are the latency, resolution, field of view, scene fidelity, eye-point matching, ergonomics and comfort, power consumption, processing power, connectivity, memory and cost [HMI-9]–[HMI-12]. Achieving high fidelity collaborative augmented reality applications is currently prevented due to bandwidth limitations and latency which could be mitigated by 5G networks [HMI-1].

The digital content that augments the user experience is usually displayed as animated or static 2D or 3D graphics, including geometric models, text, or annotations. In the past, this content was manually developed for each application. Several authoring tools and methodologies have been proposed [HMI-12] for authoring AR content; within an IoT ecosystem a connected AR system should be able to display information about every connected object in the vicinity. Even though the provision of information within the user's field of view is invaluable for certain applications, as it can enhance or even replace manuals and textbooks during maintenance and training [HMI-11], it may have negative effects on the user's attention during safety critical procedures; for example, inattention blindness has been reported during AR-guided medical procedures [HMI-13], [HMI-14].

The most important function of an AR system is real-time tracking of its absolute position and orientation or relative pose, with respect to an object or scene of interest. This is particularly challenging for portable devices due to the requirements on processing power, especially if the scene is not static, but essential in order to accurately superimpose the digital content. Sensor-based tracking techniques utilise GNSS and INS systems. AR can support identification services by retrieving a digital identifier of a smart or tagged physical object in order to enable control services by connecting to the object and change or read its state; visually recognising a plain object that is not connected could also allow the retrieval of any related information. Visual-based tracking techniques rely on the detection and identification of markers, either artificial or natural markers [HMI-15] and 2D features; or even 3D features, if depth cameras are used. Model-based tracking can also be achieved if a 3D model or a feature map of a previously visited scene is available [HMI-12]. Several recent review articles indicate the extensive use of industrial augmented reality in manufacturing [HMI-16], from products to shipbuilding [HMI-17], for the provision of information to operators on assembly lines [HMI-18].

With the advent of wearable sensors, humans are no longer only the operators or the receivers of information, in the context of human-machine interaction, as the users' cognitive, emotional, physical and behavioural state and patterns are also measured and acted upon through AR technology [HMI-4]. Wearable thermometers [HMI-19] and heart rate, oxygen saturation, blood pressure [HMI-20] or exposure to UV radiation [HMI-21], [HMI-

22] monitors are commonplace nowadays with many off-the-shelf products available. Still, even more sophisticated sensors are being developed. Kim et al. [HMI-23] introduced a wireless, stretchable, adhesive electronics device which deforms naturally with the human body while maintaining the functionalities of the on-board electronics. It has capabilities for real-time physiological monitoring, signal abnormality automatic and a long-range wireless connectivity up to 15 m. The stretchable electrodes allow for intimate skin contact and can generate clinical-grade electrocardiograms, accurate analysis of heart and respiratory rates while the motion sensor assesses physical activities. Erkoyuncu developed of an olfactory-based AR system to help with the identification of maintenance issues by enhancing the sense of smell, as odours are made up of volatile compounds at low concentration [HMI-24].

### 3.1.8.2 Relevant technology and initiatives

Several software and hardware solutions are available for the development of AR applications. Unity [HMI-25] and Unreal [HMI-26] are among the most powerful frameworks; numerous SDKs also exist such as the Mixed Reality toolkit [HMI-25], ARKit [HMI-27], ARCore [HMI-28], Vuforia [HMI-29]. During the last few years numerous visual-based mixed-reality headset kits have been announced; and some of them were discontinued before gaining traction. The most popular optical and video see-through devices are HoloLens2 [HMI-30] and Oculus Quest/Rift [HMI-31], respectively. More devices are available on the market, e.g., Glass, MOVERIO [HMI-32], Vuzix [HMI-33], MagicLeap [HMI-34], Iristick [HMI-35], but not all of them have the required performance capabilities to support demanding applications which may lead to problems such as overheating [HMI-11].

Several research projects aiming to improve the state-of-art in AR have been (co-)funded by the Horizon 2020 programme. One of the barriers to wider use of AR/VR eyewear is the large size and complexity of the required electronics. Finnish SME Brighterwave developed an imaging component which could generate excellent image quality and is small enough to enable production of AR/VR eyewear that consumers are willing to wear continuously [HMI-36]. The objective of the VIMS (Virtual IoT Maintenance System) project is to allow operators, engineers, and managers to receive and experience the relevant information about the production process even at a different location using AR/VR technologies; in addition, they will be able to control remotely the manufacturing and maintenance processes [HMI-37].

The aim of VISCOPIC is to develop an accessible tool that makes it easy to learn how to create AR content within an hour - without any previous knowledge. In addition to individual information, multistep instructions can also be created in just a few minutes [HMI-38]. The AIM and LARA projects will develop system using hand-held devices and AR interfaces to render the complex 3D models of the underground utilities infrastructure such as water, gas, electricity, etc. in an approach that is easily understandable and useful for utility field workers [HMI-39], [HMI-40]. The aim of ImmerSAFE is to train multi-disciplinary experts, who understand the core imaging technologies, the requirements set to them by the safety-critical applications and who can account for the human user in the design of such systems. This can be achieved by Immersive Visual Technologies (IVT) delivering ultra-realistic and interactive visual experience [HMI-41]. The objective of the ARIESS project is the introduction of cutting-edge Human-Machine Interfaces (HMI) and the supporting infrastructure for indoor positioning and navigation, augmented reality techniques and real-time data integration to improve the productivity, competitiveness, and sustainability of the final assembly of an aircraft [HMI-42].

### 3.1.9 Vertical applications of the Tactile Internet

Tactile Internet is a natural evolution of the Internet that adds a new dimension to the interaction of humans and machines in a variety of different fields of application with impact on society. Fixed and mobile internet infrastructure is typically used to transfer information between two points and is optimized for streaming content, either static or in real time. In this sense, the latency on the existing infrastructure have been adapting appropriately for that applications. Furthermore, IoT increases more possibilities allowing mobile Internet communication between devices. This are low-power devices, and its interconnection is designed to transmit data at a low rate and with a degree of latency tolerance. A new dimension to the perception of the internet, improving availability, security, reliability, and latency is provided with the Tactile Internet, going far beyond data streaming over fixed and mobile networks, and even beyond allowing communication and collaboration



among things. Tactile Internet is designed to enable haptic communications and allow human-machine interaction [TI-1] [TI-2].

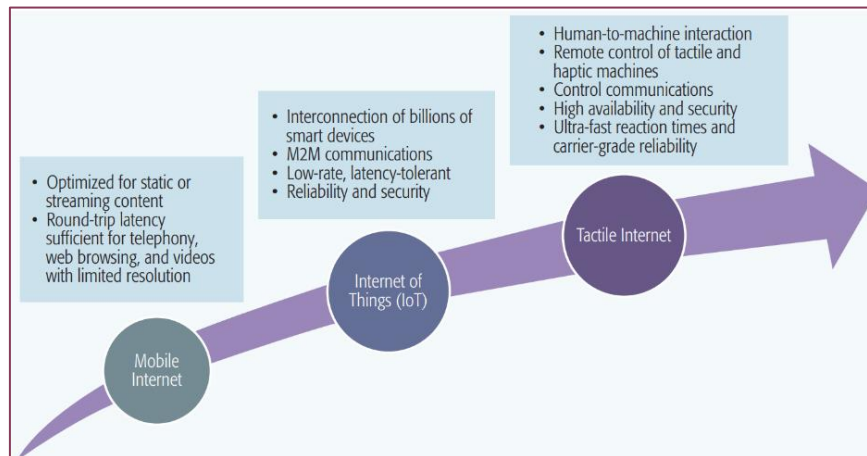


Figure 51. Tactile Internet context evolution [TI-3].

Fettweis mentioned the term “Tactile Internet” in his seminal article in 2014. In this first vision it was defined as a technology to allow the control and direction of real/virtual objects over the Internet [TI-4]. The ITU-T Technology Watch Report in 2014 defined its vision of tactile internet, as well as an analysis of its impact on society and potential applications. This document also analysed a first approach of the infrastructure requirements to support the technology [TI-2].

The IEEE P1918.1 Standards and Working Group was formed in 2016 with the goal of defining the Tactile Internet reference architecture. Some of the key use cases mentioned in IEEE P1918.1<sup>66</sup> are remote robotic surgery, autonomous driving, and haptic-enabled virtual reality, resulting in very low round-trip latency requirements. The P1918.1.1 project under development tries to define haptic codes for the Tactile Internet [TI-5]. In addition, the European Standard Institute (ETSI) has started a work item on IPv6- based Tactile Internet [TI-6]. The 3GPP has released the 5G New Radio (NR) specification that provides various enhancements pertaining to ultra-reliable low latency communication (URLLC)<sup>67</sup>.

Potential technology to support human senses interaction with machines is growing and requires high transmission speeds and low latency. Due to the technology needed to support Tactile Internet is still under development, it is still in a conceptual stage. This scientific review will address the state of the architectures and technologies that allow meeting the requirements of tactile internet, as well as the applications in which it is applied.

### 3.1.9.1 Scientific review

Due to the latency, availability, reliability, and haptic compatibility requirements of Tactile Internet, both the technology and the architecture have been developed in recent years so that they can support these requirements.

#### 3.1.9.1.1 Architecture

The architecture definition in a Tactile Internet environment is a key decision due to the strict limitations that the concept requires. For instance, the propagation delay limitation is imposed by the speed of light, so the distance between the endpoints of any given tactile application is upper bounded by 150 km to ensure the 1 ms round-trip latency requirement. In real-world implementations, this upper-bound becomes even smaller due to the overall latency of the transmission. The ITU-T warned this problem early on and, in 2014, proposed distributed service platform architecture to accomplish these objectives. The architecture is based on keeping the applications local, so that small clouds support a cluster of user devices [TI-2].

A multi-stage hierarchy of cloud platforms is proposed, with mobile edge-clouds at the level of the user devices, Mini Clouds at the local level, and a limited set of larger central clouds. The mobile edge-cloud is responsible

<sup>66</sup> [https://standards.ieee.org/project/1918\\_1.html](https://standards.ieee.org/project/1918_1.html)

<sup>67</sup> <https://www.3gpp.org/release-15>



for the tactile applications' network functions at the edge of the mobile access network, close to the user devices. The local cloud provides a complete functionality of a wireless network. These clouds include functional units as a cloud-based service platform, virtualized network control functions and the necessary interfaces.

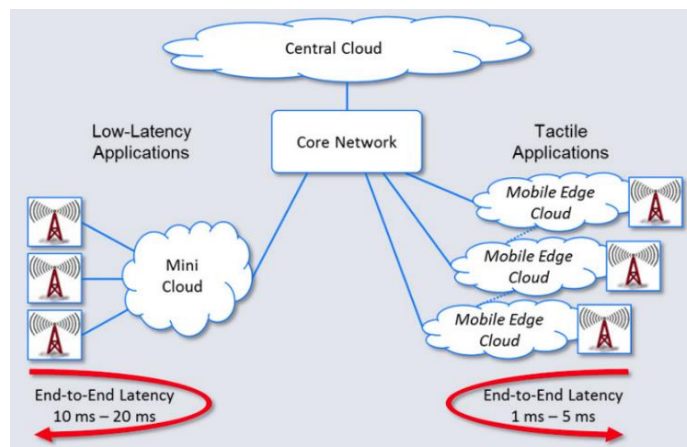


Figure 52. ITU-T multi-stage hierarchy proposal [TI-2].

The IEEE P1918.1 proposed an application agnostic architecture, adaptable to all types of connectivity. It is made up of network domains and edges domains, introducing the master-slave tactile edges and a network domain. [TI-5]

- The master domain consists of a human controller or a machine controller
- The slave domain consists of remotely controlled entities by the master domain

IEEE P1918.1 tactile internet reference architecture sets the gateway node and the network controller as part of the tactile edge or in the network domain.

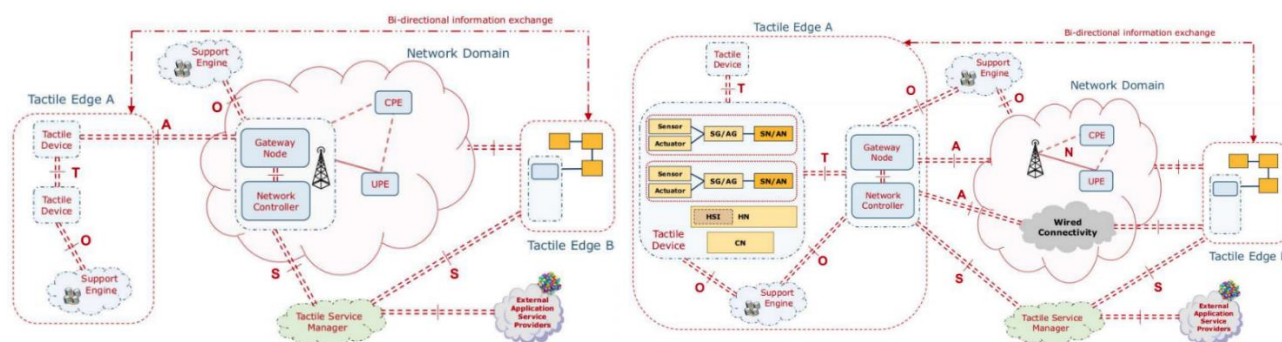


Figure 53. IEEE 1918.1 architecture with gateway node and network controller at the tactile edge (left) and at the network domain (right) [TI-5].

Tactile Internet aim is to upgrade some fundamental attributes in next generation networks. The challenges of realising the Tactile Internet span many domains that mainly include to develop an infrastructure that meets all ultra-low latency, ultra-high reliability, and high exchange rate requirements, as well as supports cloud/edge computing components [TI-2]. The ultra-reliable and low-latency communications (URLLCs) in Tactile Internet requires the most advanced technologies as well.

### Low latency

As discussed previously, latency plays a major role in Tactile Internet. A low latency is needed for seamless connectivity between the ends. In some activities, the required round trip delay implies the user interface processing, the radio interface transmission, and the server computing.

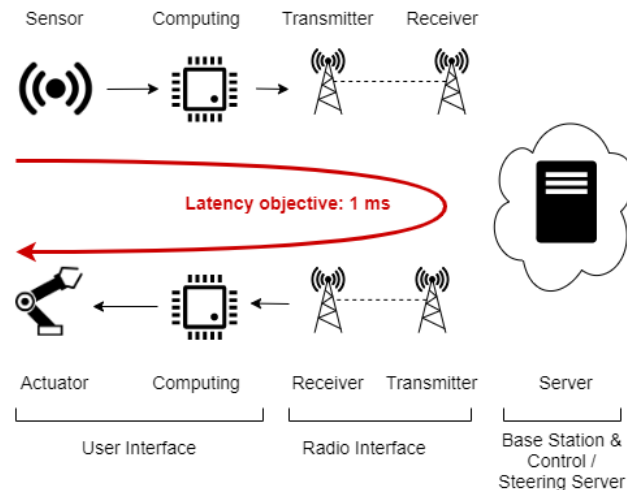


Figure 54. Tactile internet infrastructure elements that intervene in the delay of data transmission.

5G networks enable the Tactile Internet by allowing a round-trip latency in the millisecond range. As a consequence, new real-time interactive systems and physically tactile experiences can be experienced remotely. The Tactile Internet should not be restricted to the context of 5G, as there are several researches that aim to realize the implementation over other technologies (e.g., WLAN, sub-GHz technology, and combinations of these technologies) [TI-7] [TI-8] [TI-9] [TI-10] [TI-11]. Other technologies as Software-Defined Networking (SDN), with integrated network coding and a Virtualised Network Function (VNF) router can significantly reduce latency, in contrast with current packet-switched networks [TI-8]. Towards these goals, SDN and Network Function Virtualisation (NFV) have been adopted in recent proposals for future mobile networks architectures because they are considered critical technologies for 5G [TI-12] [TI-13]. While the above-mentioned methods can reduce the latency of the network domain, they cannot improve the lower bound of the latency that is a given by the speed of light. Artificial intelligence prediction algorithms are discussed that aim to deliver a seemingly real-time experience to the user (while the actual latency is still bound by the speed of light) [TI-14] [TI-15] [TI-16].

Linear predictor outputs a prediction that is a linear function of a fixed number of previously received values. In mathematical function-based algorithms, the prediction is calculated from previously received values. Additionally, a model-based algorithm can be used. When prediction algorithms become more and more advanced and computationally intensive, Mobile Edge Computing (MEC) brings cloud-computing services closer to the user, to be accessible with lower latency. Edge computing pushes computing and storage to the edge network offering a substantial reduction in communication latency. The concept has been addressed in the literature from several aspects; examples of edge computing paradigms include mobile-edge computing, fog computing, cloudlets, and mobile cloud computing.

### High reliability

In addition to the low latency, the system must be able to handle traffic at a high rate and remain reliable. To ensure the integrity of data in networks that require low latency, security mechanisms are needed. Securing a system with complex requirements, such as low latency, is difficult to implement. A drastic change in methodology and practice is needed to ensure that both data security and availability occur without hindrance. However, some security issues arise when haptic data is processed on a remote server, as the data must be sent from the device to the MEC server and vice versa. To solve this problem, encryption techniques are needed, considering that additional data implies additional delay in communication with the MEC server [TI-15].

### High data rates

To support high data rate Tactile Internet applications such as haptic-enabled VR/AR, a promising solution is to move towards higher frequency bands. The use of narrow beamwidth directional antennas, which is inevitable for reducing the high path loss at mmWave, may result in frequent link outages due to antenna misalignment. To support Tactile Internet applications, a hybrid radio access architecture is considered, where sub-6 GHz access is used for the transmission of haptic information, while mmWave access is used for the high data-rate transmission of audio-visual information [TI-17].

### Human interface. Human to Human & Machine to Machine communication

Conventional pre-5G mobile networks focused on enhancing human-to-human (H2H) communications, whereas the IoT relies on its machine-to-machine (M2M) communications [TI-1]. Tactile Internet involves the inherent human-in-the-loop nature of human-to-machine/robot (H2M/R) interaction. To support applications that requires human interaction, a master-slave architecture is needed. A master domain, that consists of a human operator and a Human System Interface (HSI) to encode the inputs into haptic inputs. The network domain provides the medium for bilateral communication between the master domain and the slave domain, and therefore kinaesthetic connection between the human and the remote environment. The slave domain consists of an operator that act as slave robot and is controlled by the master domain. The actions carried out by the slave are defined by instructions through command signals [TI-3] [TI-18].

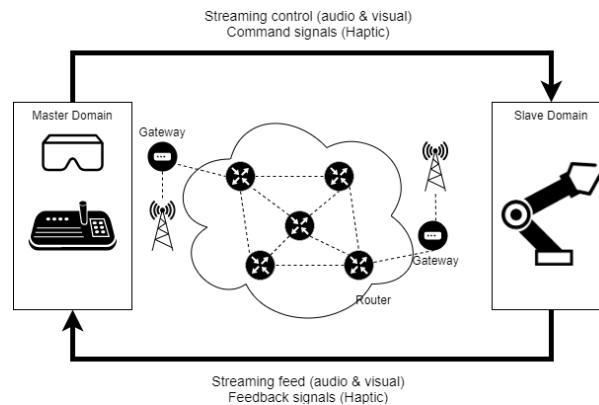


Figure 55. Tactile Internet main architecture.

### Haptic codecs

To support human-machine interactions and reduce data to achieve Tactile Internet requirements, Haptic Codecs are being defined by the 1918.1.1 task group of the IEEE. The codecs specify mechanisms and algorithms to reduce data, and a reference system for verification, evaluation, and cross-validation of the proposed codec designs [TI-5][TI-19][TI-20]. Kinaesthetic information within a closed-loop communication (feedback system). The data captured by the sensors typically consists of 3-D position, velocity, force, and torque data. Reduce update rate allows maintaining transparency of the system, so the user cannot distinguish between local and remote interaction.

- Delay intolerant. The communication does not tolerate delay, so the codec tries to reduce average number of packets transmitted bidirectionally using a mathematical model of human kinaesthetic perception to help with decision.
- Delay tolerant. In a communication with delay, the stable interaction cannot be guaranteed. An evaluation procedure to validate the communication requirements is needed.

Tactile information typically occurs within open-loop communication (non-feedback system) scenarios. This opens the opportunity for codec components such as block-based processing or frequency-domain models. The modality consists of several sub modalities such as vibrotactile signals.

- Single point interactions, such as 1-D vibrotactile signal requires the codec to split the signal into small segments and encode the segments independently.
- In multipoint interactions, the codec addresses simultaneous stimulations of the human skin at several points, to lead to more realistic experiences. Inter-channel or spatial correlation complements temporal correlation.

#### 3.1.9.1.2 Protocols

No protocols have been proposed so far by the IEEE P1918.1 standard, although interfaces have been identified [TI-1]. However, some protocols can be found in the literature to favour communication in Tactile Internet applications. An Agile Cloud Migration (ACM) protocol aims at providing fast migrations with zero downtime over MECs to ensure that applications (e.g., a control server for autonomous driving) are always close to users.

The key approach of this protocol is to transfer only the state of the application during migrations, thereby optimizing the amount of data transmitted. However, this protocol requires that applications be designed such that their engine is isolated from their state.

A handoff protocol for vehicular to infrastructure (V2I) communication. Defines which network vehicles should be connected to, in order to ensure that the vehicles experience a minimum delay. The LTE network provides better delay performance than the IEEE 802.11p network when V2I distance is large and vehicle density is high, thanks to its broader coverage and higher capacity. However, it is worse than the IEEE 802.11p network when the V2I distance is smaller and vehicle density is lower, due to its handshaking protocol during the channel access procedure. A haptic handshake scheme for orchestration between heterogeneous tactile devices with different specifications and requirements in terms of sensing and display, data compression compatibility, and application requirements, among others. Before a Tactile Internet application connection is set up, every node must be aware of the capabilities and requirements of other nodes. A messaging format to exchange metadata during haptic handshake is also developed.

### 3.1.9.2 Relevant initiatives

In its basic definition, Tactile Internet was conceived to support vertical applications that requires real-time communication and human-machine interactions. That is why the requirements for speed of reaction and response must be adapted to the context of a specific service or application. The initiatives under development and the proposals found in the literature are focused on fulfil those applications requirements. Fettweis defines a real-time interaction when the communication response time is faster than the time constants of the application and discusses four types of physiological real-time constants: muscular, audio, visual, and tactile [TI-4]. In this innovative vision, some application scenarios are proposed, mainly health care, education and sports, traffic, robotics and manufacturing, free-viewpoint video, and smart grids.

The ITU-T published shortly after its vision about the application fields where the Tactile Internet may take a decisive leap in its viability. This publication specifically mentions the requirements that the infrastructure that supports the applications must have, indicating not only the performance requirements, but also the architecture and the devices / sensors involved [TI-2]. The IEEE P1918.1 also summarized specific use cases and described the minimum value of latency and reliability to achieve acceptable performance, in addition to other traffic characteristics such as burst size and average data rate [TI-5]. The different applications can be grouped according to the type of communication, purpose of the applications or variety of scenarios. Regarding specific applications, there is a great variety of fields depending on the communication that is carried out.

- Audiovisual information provides the feeling of being present in a remote environment, but this immersion can be completed with the exchange of haptic information in the form of various parameters such as force, movement, vibration, and texture. Haptic applications bring a strict set of requirements in terms of latency, reliability, and security. Ultra-low latency is required to ensure timely delivery of control messages, with a high level of reliability to ensure message integrity [TI-1].


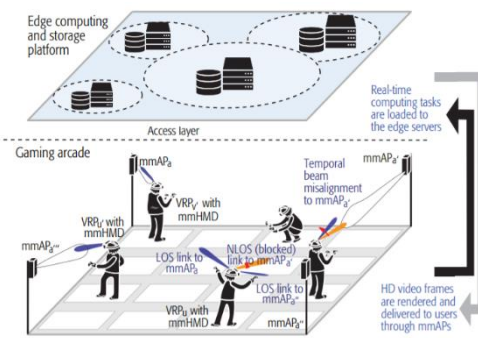
*Table 25. Tactile applications based on haptic information*

Domain	Proposals
Mechatronics	Real-time teleoperation allows human-machine (master-slave) communication into a distant or inaccessible environment. In mechatronics, the interaction provides a physical link between the virtual and real worlds and constitutes the remote body of the human being to execute various sets of skills. These techniques are widely used in industrial automation [TI-21]. Applications as monitoring do not need strong real-time requirements. Latency requirements are more usual in emerging industrial applications, as safety control and HMI applications where 99.99999% is desirable and 99.9999% is acceptable [TI-22]. Some design approaches set multi-robot applications allocating physical and/or digital human tasks to robots. In [TI-23] an integrated Wi-Fi multirobot network architecture is designed, coordinating local and nonlocal H2R task allocation.

- Some applications do not require haptic information, being audio and image the main content of the messages. Video transmission applications are developed in a wide variety of areas, being virtual reality initiatives mainly relevant.

Domain	Proposal
Virtual Reality	High resolution images and 3-D stereo audio in VR and AR applications demand the flow of massive information, and thus will introduce new design challenges in future networks in terms of improving several performance metrics such as network throughput, delay performance with less than 10 ms latency to avoid cybersickness. Some use scenarios, as free-viewpoint video, allows digital image processing to synthetically render the viewpoint of the viewer to another spot. A remote VR phobia treatment architecture is proposed in [TI-26] using MEC networks to reduce computation delay and mmWave communications to increase network capacity. These innovations provoke emergence of helmet-mounted VR devices such as Oculus VR, HTC Vive, PSVR, and Microsoft HoloLens.

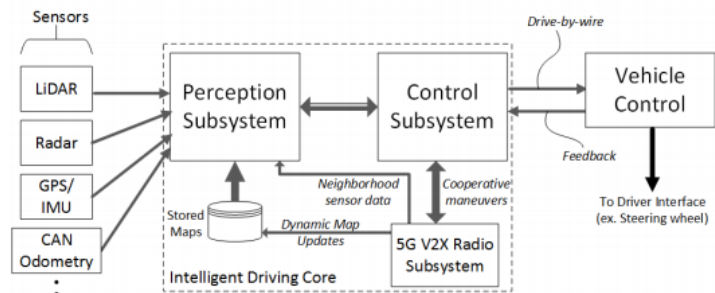
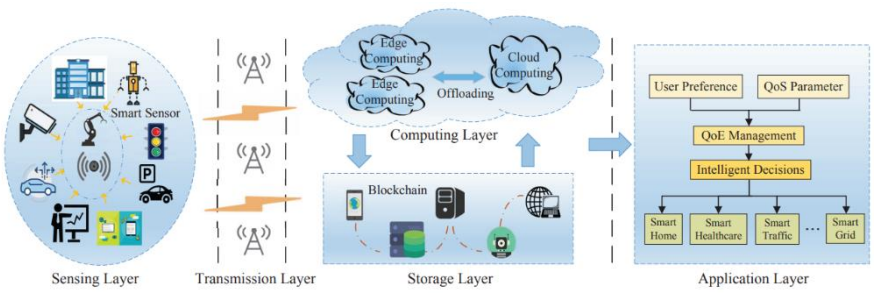


Domain	Proposal
	 <p><i>Figure 58. VR phobia treatment architecture concept [TI-1].</i></p>
Video surveillance	<p>A video surveillance application is proposed in [TI-27] to use on unmanned aerial vehicles with the computation capacity to perform local data processing close to sensors and actuators. The architecture of video surveillance systems requires these sensors and actuators to be installed on the ground, and cameras installed on board each drone. The data generated by these cameras cannot be sent to the cloudlet or MEC servers on the ground because this should take a long time to be transmitted, not compatible with actions that must be taken in times less than 1 ms. The particularity of this project lies on the installation of a microcomputer on board the drone that acts as a touch support engine to process the incoming data and decide, as soon as possible, if the alarm level is changed to send the activation message to actuators installed on the floor.</p>
Gaming	 <p><i>Figure 59. Interactive VR game proposal.</i></p>

- Other tactile internet applications do not require human interaction, and its implementation is based on data transmission optimisation. Different communication patterns are being developed in smart cities or autonomous vehicles: vehicle-to-vehicle, device, infrastructure, network, pedestrian (V2V/D/I/N/P).

*Table 27. Tactile applications based on M2M information*

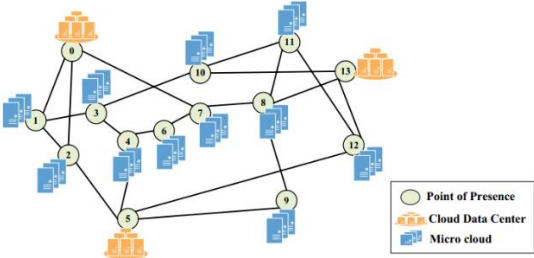
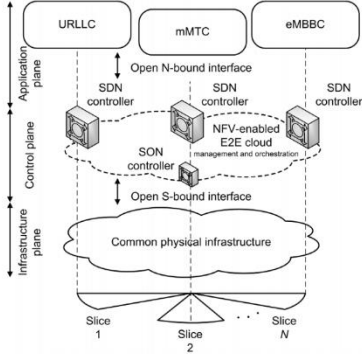
Domain	Proposal
Autonomous vehicles	<p>Detected data is used by the vehicle to make a better decision during driving events. Do to the possible tragical consequences of an accident, it must be transmitted in real time with almost zero delay. In-vehicular networks are currently standardized within the IEEE 802.1 (IEEE 802.1BA, IEEE 802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav). In [TI-29] a useful scenario, used for broadcasting purposes only, covers V2P and V2V patterns where either a vehicle or a pedestrian can receive or transmit the information of neighbouring vehicles or pedestrians. This information includes velocity and location of the vehicle by which one can calculate the relative position to avoid collision. Other large-scale propagation scenario is used for making the policy handle emergency situations, by communicating the information to remote locations. In [TI-30] testbed based on flexible and re-configurable software defined radio that is designed for cooperative automated driving. The system consists of re-configurable frame structure with fast-feedback, new Polar-Orthogonal Frequency Division Multiplexing (P-OFDM) waveform, low-latency multiple-access scheme and robust hybrid synchronization.</p>

Domain	Proposal
	 <p><i>Figure 60. Automated driving core subsystems [TI-30].</i></p>
Smart cities	<p>In [TI-31] a quality of experience (QoE)-driven five-layer Tactile Internet architecture is proposed, in order to improve smart cities performance.</p> <ul style="list-style-type: none"> <li>• Sensing layer. Collect big data from distributed sensors in smart city.</li> <li>• Transmission layer. Multiple uncorrelated links can be created through inter-band spectrum aggregation techniques and through coordinated multipoint transmissions.</li> <li>• Storage layer. Includes both data storage and security using blockchain techniques.</li> <li>• Computing layer. Osmotic computing handles the issue of computation offloading in the cloud and edge integration.</li> <li>• Application layer. Intelligent decision-making is performed, containing network optimization, demand response.</li> </ul>  <p><i>Figure 61. Smart city 5-layer architecture proposal</i></p> <p>Another application area is the synchronization of suppliers in a smart grid. As synchronous compensating of suppliers is necessary to minimize reactive power, this must be achieved within a small angle of phase.</p>

Other proposals are not defined to a specific application. The IEEE-P1918.1 architecture seen at the scientific review is defined as application-agnostic due to its generic configuration accessible to all types of connectivity.

*Table 28. Application-agnostic architectures for tactile internet*

Architecture	Description
FlexNGIA [TI-32]	In FlexNGIA an innovative vision of the future Tactile Internet infrastructure is proposed, including services, business model, management framework, and network protocol stack by leveraging the availability of computing to host advanced network functions that could support the network applications. It defines a business model where network operators could offer not only data delivery but also service function chains with stringent requirements in terms of performance, reliability and availability. FlexNGIA fully flexible packet headers that could be tailored to the application requirements, and a combination of transport and network layers allows the network to offer better congestion control and reliability services.

Architecture	Description
	 <p><i>Figure 62. FlexNGIA concept [TI-32].</i></p>
SDN/NFV dynamic slicing architecture	<p>The architecture in [TI-10] fulfils requirements of different vertical applications, including latency critical communications, by enabling flexible and dynamic slicing. A two-hierarchical control levels model integrates SDN and NFV with fog computing. SDN controller forms the higher level, while local controllers model the lower level.</p>  <p><i>Figure 63. SDN/NFV architecture for Tactile Internet [TI-10].</i></p>

These other architectures in [TI-1] are not specifically developed for Tactile Internet, but they can be configured to support different applications.

- MEC enhanced Cellular network architecture propose a multi-level cloud system to provide offloading capability in the cellular networks. This system aims to improve the latency and reduce the network congestion in the core network in Tactile Internet applications.
- FiWi-enhanced cellular network architectures aim to enhance LTE-A heterogeneous networks with FiWi access networks to provide high-capacity fiber backhaul and WiFi offloading capabilities.

EPON-based network architecture. Next-generation EPON (NG-EPON) allows transmission of traffic over multiple wavelength channels simultaneously, thereby increasing the network capacity.

### 3.1.10 IoT security and software development using DevSecOps on IoT ecosystems

The following statements could be considered as security requirements for an IoT deployment:

- IoT sensors in machines which provide data are assumed to be reliable,
- Workstations used to access collected data from machines are assumed to be reliable and able to operate properly,
- Software on server is reliable and continuously updated,
- Server is secured,
- Users of the application are authenticated and authorized, the owner of the service provided is considered as trusted at the client.

Secure software and firmware updates are a technical measure for IoT listed, associated with Authorization, as described in ENISA Good practices for IoT [IoTDSO-1] that will mitigate different threats associated to failures, malfunctions among others operational threats related to IoT devices.

Software distribution should be controlled in IoT environments, not only associated with Authorization but also on the software update process.

DevOps paradigm deals with the concrete above statements related with software distribution and secure operation.

### 3.1.10.1 DevOps definition

DevOps is, as defined [IoTDSO-2], a collaborative culture with a set of practices, ideas, tools, technologies, and processes that streamline the product development process. This huge cultural shift lays emphasis on effective communication, integration, and better collaboration among teams for delivering quality products. Basically, DevOps is a methodology that helps organisations build software - and their production teams - in a way that enables continuous rapid deployment.

DevOps initiatives aims at faster and easier delivery of better quality, more secure software.

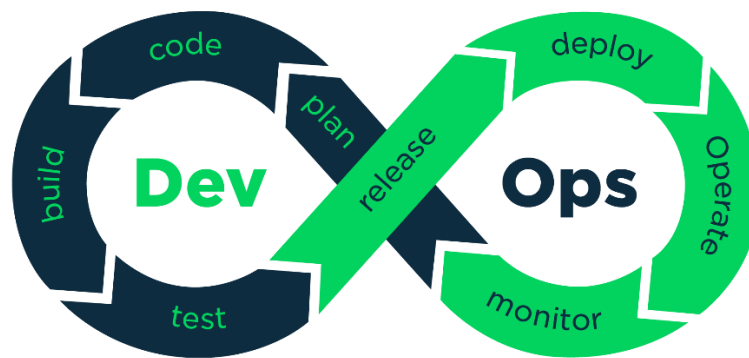


Figure 64: DevOps cycle

### 3.1.10.2 Purpose of DevOps

Historically, there has been a serious disconnect between the development and operations teams in software production. Lack of cooperation among teams often resulted in confusion and tons of challenges along the way. The culture focuses on merging the development and operations roles - and the processes involved throughout the production cycle - to achieve common business goals. Embracing DevOps helps to put together a more streamlined, agile, and efficient process of software production. It is all about maintaining a common, shared culture, enhanced collaboration, and shared business processes.

DevOps has four fundamental principles:

- Collaboration: Between project roles,
- Infrastructure as Code: All assets are versioned, scripted, and shared where possible,
- Automation. Deployment, testing, provisioning any manual or human-error-prone process,
- Monitoring: Any metric in the development or operational spaces that can inform priorities, direction, and policy.

### 3.1.10.3 IoT and DevOps

IoT software developers are constrained by imperfect IoT tools and platforms in terms of delivering their apps to end users. DevOps methodology can help IoT ecosystem to solve this issue, additionally and as mentioned before DevOps workflows will help to reduce threats on software delivering and operation on IoT environments.

To prevent the threats that IoT and M2M communications and devices may face, a set of security properties should be guaranteed. Below are grouped in three main levels:

- 1) Minimalized physical hardware interface exposure:
  - a) To reduce the surface of physical attacks, the hardware interface on IoT device should be minimalized, for instance, disable the unnecessary debug (JTAG) port, remove the unused USB ports and ensure that there is no open accessible console port.
- 2) Secure device identity
  - a) Device provision and identification: A proper identification method is the foundation of IoT. An ideal identification methodology not only identifies the objects uniquely, but also reflects the property of the object.
  - b) Device authentication: it may refer to either entity authentication or data origin authentication. More precisely, entity authentication enables communicating parties to check that the other entity is really which it claims to be whereas data origin authentication, as its name implies, ensures that a message really originates from a given entity.
- 3) Secure device communication channel
  - a) Confidentiality: it protects the content of gathered as well as exchanged information by preventing them from being read by unauthorized entities such as eavesdroppers.
  - b) Device and Data Integrity: it keeps devices as well as, transiting and stored, data from being altered by any illegitimate entity.
  - c) Availability: it ensures that authorized entities can always have access to a given information (or application) whenever needed.
  - d) Non-repudiation: it makes sure that an entity cannot subsequently falsely deny a given action (e.g. sending a packet, triggering a given command, etc.).
  - e) Privacy: it prevents the disclosure of any sensitive or personal information such as habits and health status.
- 4) Secure device software management
  - a) Firmware update: it is a process to update the device firmware completely and securely. It also allows fixing a security vulnerability that pervades the platform firmware.
  - b) Firmware rollback: in case of firmware update failure, the system should be able to roll back to a previously functional firmware version.
  - c) Software update and maintenance: it is a process to update software application completely and securely. It also allows fixing application bugs or adding simple feature enhancements.
- 5) Secure device configuration and monitoring
  - a) Remote device configuration: most of the time, a personal device will need to be further configured by the end user with attributes implementing new configuration changes.
  - b) Monitoring and diagnostics: in a system of thousands of remote devices, can detect when something is amiss by monitoring compute, storage, networking, and I/O statistics at the task or process level, and comparing those statistics to characterized nominal values.

#### **3.1.10.4 DevOps foundational practices and the five stages of DevOps evolution**

The report 2020 State of the DevOps [IoTDSO-3], the DevOps evolution model shows that organizations do not progress to self-service and security integration until Stages 4 and 5, after individual people are given more autonomy to work without manual approval from outside the team in Stage 3.



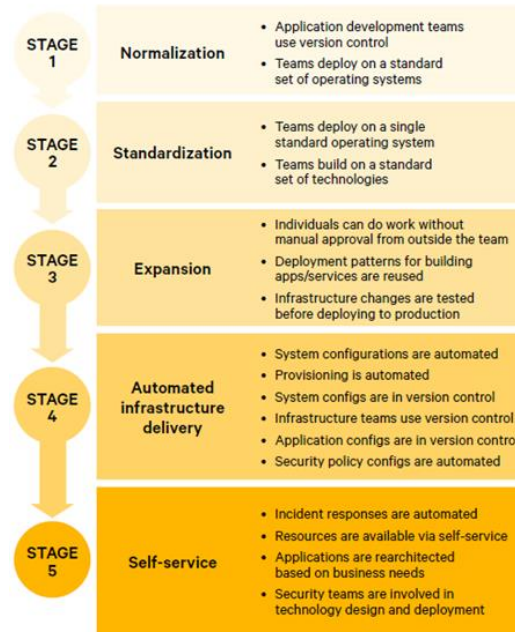


Figure 65: DevOps evolution model in 5 stages

### DevOps evolution and platform evolution

The graph below shows how platform offerings change as organizations progress through their DevOps evolution. The y-axis shows different types of self-service offerings. In each row representing a self service offering, the 2020 State of DevOps Report [IoTDSO-4] placed three coloured dots, with each colour representing a different level of DevOps evolution. The x-axis represents the percentage of a group that has adopted a given self-service offering.

It is showed the gaps in adoption between groups at low, mid, and high levels of DevOps evolution.

- At a low level of DevOps evolution, organizations offer self-service for CI/CD workflows, internal infrastructure, and public cloud infrastructure.
- Mid-evolution organizations expand their internal platforms, providing development environments, monitoring, and alerting.
- High-evolution organizations tend to offer a wide variety of internal platforms. This is where you can see more self-service for deployment patterns, database provisioning and audit logging.

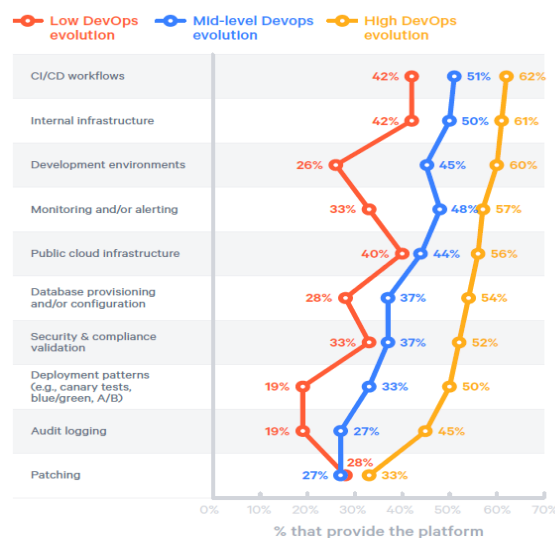


Figure 66: DevOps evolution and platform evolution

### 3.1.10.5 DevSecOps Definition

DevSecOps is defined in [IoTDSO-4] as DevOps embedded with security controls providing continuous security assurance. DevSecOps is natural extension of DevOps that advocates shift- security-left, security-by-design and continuous security testing by building automated security controls in DevOps workflow. Figure 67 depicts DevSecOps as DevOps with continuous security assurance wherein security controls can be embedded across DevOps workflow.

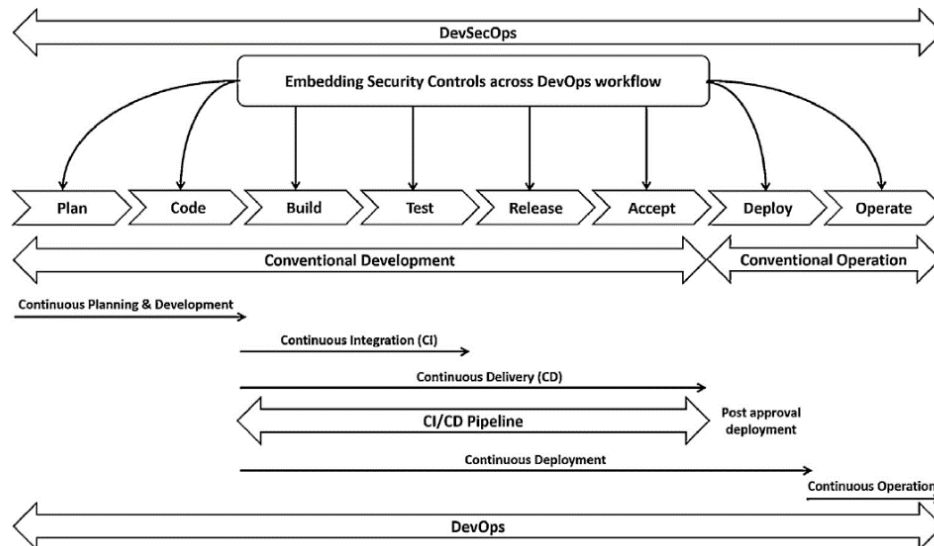


Figure 67: DevSecOps. DevSecOps with security [IoTDSO-4]

DevSecOps ambition is to include and if possible, to automate as much as possible security controls in the software development life cycle.

## 3.2 NG-IoT pilots / testbeds

### 3.2.1 State of the art in Port Automation

#### 3.2.1.1 Scientific review

Although container ports around the world are currently at different stages of an ongoing transformation process evolving towards digital, connected, and intelligent fully integrated Industry 4.0 entities, scientific literature about Industry 4.0 enablers in port environments is scarce and only simplistic and isolated practical experiences are reported by practitioners, vendors, terminal operators or port authorities on their respective websites, or newsletters. Nevertheless, an overview of the latest NG-IoT innovations in Ports, which are relevant to the ASSIST-IoT key enablers, is provided in the next subsections.

#### 3.2.1.2 Relevant initiatives

iTerminals 4.0 is one of many research projects co-funded by the EU. Its goal is to boost digitalisation of port operations and the adoption of Industry 4.0 technologies within the container-handling by upgrading port equipment's sensor networks, the design of advanced big data and predictive analytics, the application of artificial intelligence as well as the provision of business intelligence models and real-time dynamic KPIs reporting. The project is founded on four pillars: i) operational efficiency, enabling real time machine-to-machine communication to detect operational bottlenecks and facilitate decision making, ii) operational safety, enhance situational awareness based on reliable positioning/detection of machines and persons, iii) operational sustainability, allow real-time calculation of the carbon footprint generated in container terminals, assigning to each manipulated container a unique carbon footprint value generated during its handling, iv) operational maintenance, improve maintenance management by enabling digital transmission of failure codes to the maintenance areas, thus facilitating better predictive maintenance and increasing efficiency of operations. The

Horizon 2020 COREALIS project proposes a strategic, innovative framework, supported by disruptive technologies and emerging 5G networks, for cargo ports to handle future capacity, traffic, efficiency, and environmental challenges. The Horizon 2020 CYBER-MAR project aims to develop cyber preparedness for cyberattacks in the maritime environment and estimating the impact of a cyberattack from a financial perspective.

### ***Robots and Automation in Ports***

Container terminals that handle significant volumes of container traffic have automated to a large extent their operational-information management process. Ports automation started with automated decision making in the early 1990s pushed first with berth planning models and after with stowage and yard planning, making use Terminal Operating Systems (TOS). This was followed by automated terminal's inland gates during the 1990s and automated tracking and tracing in early 2010s [PA-1], [PA-2].

For a port terminal to become fully automatic, machinery must work without a driver in the cabin (although human-in-the-loop supervision or remote control is expected). However, the automation of the physical handling (unloading, storing, loading) of containers has only been partially achieved. After more than 25 years of developments, robotization has definitively taken off and more than 1100 driverless cranes are in operation worldwide and thousands of Automated Guided Vehicles (AGV's) carry out transport operations from quay to yard, becoming a standard product in modern terminals, but all these automated robots are only placed in 35 out of approximately 2000 container terminals globally (1.75%). The automation of quay (ship-to-shore) crane is less developed, as current practice requires that controlling their dynamic behaviour, such as undesirable swaying, is the responsibility of a skilled operator [PA-1]–[PA-5].

Some of the main limitations for this successful deployment of full automated CHE comes due to the requirements of deploying a high variety of sensing systems (inertial sensors, ultrasonic sensors, eddy current sensors, radar, lidar, imaging sensors, local radio-positioning networks, RFID readers and tags, transponders or magnets buried in the ground and antennas in the bottom of the vehicle, global navigation satellite systems) in order to support tasks such as container positioning, detection, and handling using computer vision methods or corner casting recognition [PA-6], AGV localization, navigation and control, and structural health monitoring of the quayside cranes [PA-2], [PA-7]. Connecting all these sensors over the internet is a challenge as container terminal environment are inherently hostile for wireless communication. Although wireless technologies have been widely used for many years in container terminals for not time-critical communication, remote or automated crane operation is extremely intolerant of latency and jitter, often requiring sub-50ms latency to operate at its full potential. For instance, the main disadvantages of WiFi deployments in container terminals are related to the limited available throughput and latency (roaming times are usually 100-700ms). In another vein, even though 4G LTE-only infrastructure provides a promising alternative the video-streaming bandwidth is still limited. The development of 5G technology promises to enable tactile internet; meanwhile a wireless Multiprotocol Label Switching (MPLS) technology has also been proposed as a solution and was implemented for automated Rubber Tyred Gantry (RTG) crane systems [PA-7], [PA-8].

### ***Edge computing***

Automated operations and remote controlling systems (particularly for cranes and other vehicles) have been among the topmost expected initiatives from several port authorities throughout the world, but with limited success. To support remote controlling operations from a control room elsewhere in the port, gantry cranes should be equipped with multiple high-definition cameras and PLCs. The number of cameras installed on each crane can vary from 6 to 27 cameras (depending on their size and payload capabilities), which could lead to a total uplink bandwidth of approximately 30 – 120 Mbps. Large coverage requirements are also imposed for enabling cranes movement within terminal ports (e.g., quayside cranes demand horizontal movements of 100m to 200m, smaller RMG cranes need to move on a 200m to 400m track, and other container handling machines, such as the RTG cranes and AGVs, have a greater range of mobility with speeds up to 40km/h).

The connectivity challenges for automation or remote controlling initiatives have been fulfilled to an extent by a mix of fixed and wireless networks, using fibre-optic cables together with Wi-Fi and 4G systems. However, on the one hand, fibre solutions require expensive and time-consuming deployments, as well as some areas of ports are unreachable via wired solutions. On the other hand, wireless Wi-Fi and 4G technologies are not sufficient to cope with ultra-reliable and low-latency communications requirements of automation (e.g., Wi-Fi

only delivers a coverage area of tens of meters with limited QoS or switching between multiple APs can take several seconds). 5G, unlike 4G, is expected to provide significantly higher bandwidths, both in the downlink, and more importantly in the uplink, and a rapid response rate to the controller. However, even though, 5G networks on their own will not guarantee such ultra-low latencies, as all mobile data is sent to the operators' core network before reaching an external data network, significantly adding the overall latency. The advent of edge computing deployed at local gateways will have a twofold advantage:

1. Through user plane and control plane separation, edge computing ensures the data is kept being processed locally within the port networks, thereby reducing the overall latency.
2. Edge computing can create a private local network, improving data security. Given that ports are independent enterprises, the port authorities will not want their data to interact with the MNOs external infrastructure.

The availability of local computing resources as part of edge computing can thus improve data processing and reduce the machine vision system cost in ASSIST-IoT port automation pilot. Next, different edge computing applications for port automation are briefly described.

- Machine vision systems used for container identification are expensive due to the dedicated monolithic architecture (tightly coupled HD cameras and image processing servers in the far cloud). A more cost-effective machine vision system would offload the image processing capability from cloud servers to local edge computing servers.
- As another example edge computing use can benefit port's networks, making future upgrades and daily maintenance easier, as well as facilitating the AI and big data algorithm training by breaking the data silos [PA-9].
- Fleet and asset management solutions could use Edge computing hardware and software to increase the visibility, integrity, and security of assets moving through ports' premises, helping operators to gain near real-time tracking and monitoring of asset location, temperature, humidity, shock, ambient light, pressure, and tilt. Comprehensive dashboards enable effortless monitoring and analysis; and may include programmable notifications and alerts for quick intervention.

Although several open edge computing alliances have been described in Section 3.1.3, it should also be noticed that they are still not successfully deployed in real commercial environments. Regarding edge computing solutions, Dell and Intel are leading the market race, helping to different stakeholders across the globe to develop, test, and deploy the edge computing technologies to make the vision of maritime automation a reality, enabling maritime organizations to build Edge to Cloud infrastructure that adapts and scales to help port operators to sustain, grow, and protect their data, cargo, workers, environment and ultimately their business. Together, Intel and Dell are bringing new capabilities to the Edge with performance optimized, cloud-ready solutions that excel even in space- and power-constrained environments. A brief portfolio of Intel-Dell solutions is depicted below.



Figure 68. Dell-Intel edge and IoT portfolio for port operations [PA-10].



## Artificial Intelligence

The amount of operational data from TOS, together with data from a variety of new data sources is growing fast. However, the most part remains under-analysed. Therefore, given this growing volume and complexity of data, discovering patterns or irregularities by developing ML algorithms to support decision making has become increasingly important for container terminals operators and port authorities. A high-level example about how an ML model can be inferred within ports is depicted in the next figure.

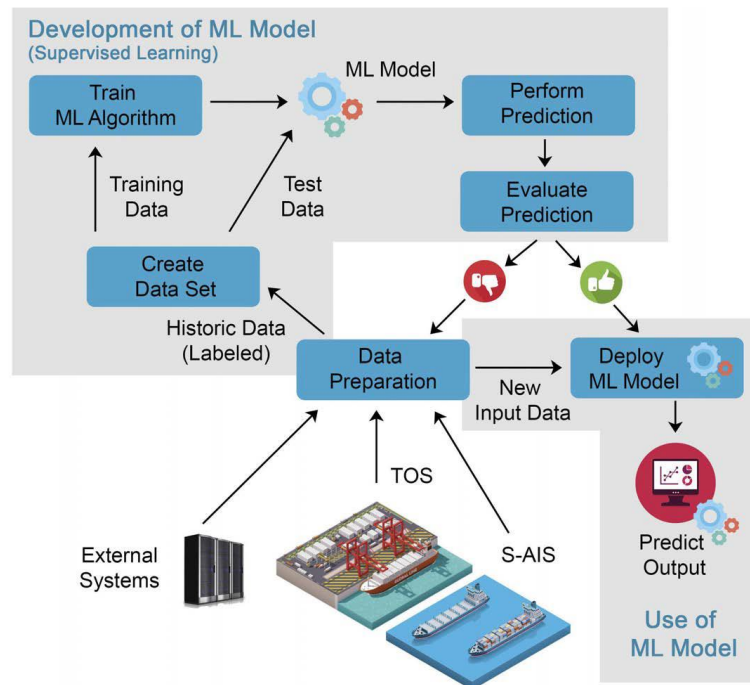


Figure 69. ML deployment over smart ports [PA-11].

In [PA-9], ML application over port's logistics is classified in three areas:

### Quayside ML

The performance of quayside planning depends on many factors, including vessel arrival times, vessel call patterns, peak demands, and the handling capabilities of the quayside equipment. Uncertainties may result from a lack of reliable information and forecasting, such as delays of vessel arrivals, weather and tidal conditions, traffic congestion, and equipment breakdowns. To limit some of these uncertainties, a strong research has been focused on the analysis of satellite Automatic Identification System (S-AIS) data. It will help for identifying patterns and anomalies of vessel operations, e.g., to avoid vessel accidents or to identify unauthorized activities like illegal bunkering. Applications of ML in the quayside include:

- **Prediction of vessel arrival times:** To reduce uncertainty of vessel arrivals, research has been conducted to evaluate different algorithms to enhance their predictions considering weather conditions like wind speeds.
- **Prediction of turnaround times:** To reduce uncertainty of vessel departure, research has been conducted to evaluate different algorithms to enhance their predictions considering type of vessels, type of goods, port of origin, performance of the local agents and number of assets available in the terminal.
- **Prediction of ETC time:** To reduce uncertainty of vessel end of cargo operations (i.e., Estimated Time of Completion).
- **Berth planning:** Existing approaches predict the performance of vessel loading operations thanks of previous gathered data. However, ML can also be used to improve the selection of optimisation methods used for berth allocation planning.



### Yard ML

Several complex planning and optimisation problems result from yard operations (e.g., yard allocation, post-stacking, crane scheduling, etc.) It is important therefore to reduce uncertainties by predicting future scenarios by making use of ML applications like:

- **Prediction container dwell times:** Different algorithms have been developed and evaluated. Models can be used to assess the impact of changing determinants on the container dwell times yard capacity and terminal demurrage revenues.
- **Container stacking:** algorithms have been developed to predict the quantity of incoming containers and weight groups of containers to optimise the container stacking policy.

### Landside ML

Improving landside operations by ML can lead to better hinterland accessibility and inland connectivity, which is crucial for the competitiveness of container terminals. Contextual data extracted from as sensors can be used to better understand and coordinate traffic flows, including:

- **Prediction of truck traffic:** they could predict inbound and outbound heavy-truck volumes using for instance geospatial sensor-based data from them.
- **Prediction of truck waiting and turnaround times:** by analysing truck arrival rates and waiting times gathered by embedded sensors and cameras.
- **Prediction of truck delays:** algorithms have been developed for identifying causes of abnormally high truck turn times in container terminals.

### *DLTs*

Blockchains are another enabling technology that is expected to contribute to the digital transformation of ports. In fact, blockchain has been recognized to play a pivotal role in Ports 4.0 revolution. Its benefits in ports are summarized in:

- building trust and simplifying transactions, without the need of 3<sup>rd</sup> parties arranging a deal between two parties.
- providing secure data and avoiding frauds by using encryption mechanisms.
- increasing the visibility of the transactions in real time, which means that e.g., containers can be easily tracked and traced, dispatched, and invoiced almost instantaneously.
- permitting integration of physical, financial and information supply flows.

However, the use of blockchain technologies is overcoming some difficulties like technical and functional adaptation concerns, resilience to share data becoming more vulnerable, governance (who owns the data shared in the platform and grants access to new participants), and legal and regulatory uncertainty.

Blockchain research within the context of container terminals is limited [PA-12] as it is relatively new and there is still misunderstanding on the potential applications and impact in the field [PA-13]. However, several initiatives are being developed for its application [PA-3]. For example, Maersk and IBM have founded a joint called TradeLens [PA-14] to develop a blockchain system to track containers and reduce bureaucratic procedures, seeking for a more efficient and secure methods for conducting global trade [PA-15]. While some Port Authorities and terminal operators have announced they will join TradeLens, several others are also launching their standalone experiments, several ports, such as those of Antwerp and Rotterdam, have introduced blockchain solutions to facilitate port operations and logistics processes. A practical implementation example is that of sharing cargo information on a ledger instead of exchanging documentation between logistics stakeholders; the chain can thus be extended to several other actors such as banks and insurance companies once security concerns have been addressed and trust has been established. Data from connected sensors and IoT devices can also be added as blockchain nodes in order to monitor the status of goods [PA-16], e.g., food temperature [PA-17].

### 3.2.1.3 Relevant initiatives

Many research projects in the port industry indicated a growing interest in NG-IoT technologies for the maritime industry. Some of them are briefly introduced next.

- **iTerminals4.0** [PA-18] is one of many research projects co-funded by the EC. Its goal is to boost digitalisation of port operations, and the adoption of Industry 4.0 technologies within the container-handling, by means of an upgrade of port equipment's sensor networks, the design of advanced big data and predictive analytics, the application of AI, as well as the provision of business intelligence models and real-time dynamic KPIs reporting. The project is founded on four pillars: i) operational efficiency, enabling real time M2M communication to detect operational bottlenecks and facilitate decision making; ii) operational safety, enhancing situational awareness based on reliable positioning/detection of machines and persons; iii) operational sustainability, allowing real-time calculation of the carbon footprint generated in container terminals by assigning to each manipulated container a unique carbon footprint value generated during its handling; and iv) operational maintenance, improving maintenance management by enabling digital transmission of failure codes to the maintenance areas, thus facilitating better predictive maintenance and increasing efficiency of operations .
- The **COREALIS** [PA-19] project proposes a strategic, innovative framework, supported by disruptive technologies and emerging 5G networks, for cargo ports to handle future capacity, traffic, efficiency, and environmental challenges.
- The **CYBER-MAR** [PA-20] project aims to develop cyber preparedness for cyberattacks in the maritime environment and to estimate the impact of a cyberattack from a financial perspective.
- **PIXEL** [PA-21] project is developing and implementing predictive models that apply to small and medium-sized ports by using the data that is captured internally by ports or is accessible as open data in order to provide cost-efficient solutions, that are at the same time scalable so that they can also be used in larger ports. One of the main drivers behind the definitions of the tasks and their scope was the data that can be obtained by ports as stakeholders and can be used in the project.

Beyond EC R&D projects, several private partnerships have been carried out in the latest years for speeding up port automation, which are detailed below.

- The use of autonomous surface vessels navigating without human control forms part of project developed by Mitsui OSK Lines testing Rolls-Royce's intelligent awareness system in its vessels. The system combines data from onboard sensors with information from bridge systems looking for a safer, simpler, and more efficient way to operate [PA-22].
- A system to predict the Estimated Time of Arrival (ETA) for containerships at the Port of Rotterdam using neural networks and support vector machines. This system combines position data from GPS signals with weather predictions [PA-23].
- The port of Hamburg has created a Decision Support System (DSS) using deep learning techniques and neural networks capable of predicting the behaviour of land transport. The system forecasts the times when lorries should reach terminals and the drivers have received a notice about the expected terminal entrance times. The model supplies a dynamic forecast of the workload considering changes in the surrounding conditions like road and access route saturation, real ship arrival time, or degree of terminal saturation.
- Fujitsu jointly with the Port Authority of Singapore have developed and tested an AI-based system to analyse marine traffic risks in the Singapore Strait. The goal was to predict potential collisions routes, encouraging vessels to put in place avoidance measures [PA-24].
- The port of Qingdao in China and Ericsson launched a partnership programme at MWC 2019, following a technical trial in late 2018, to develop a 5G smart port solution. One of the key goals was to demonstrate the advantages and labour cost savings that could be possible if 5G networks were used for automation compared to a traditional port with no automation.
- The port authority of Livorno, together with Telecom Italia (TIM) and Ericsson has defined an innovative model to assess the introduction of 5G technologies and explore how digital transformation can meet the UN SDG-2030 goals [PA-25].

- The engagement of Huawei with the port authority at Ningbo, one of the world's largest with over 550 gantry cranes, successfully demonstrated the use of 5G together with Edge computing, delivering high data throughput needed to serve many HD camera feeds, together with latency of less than 20 ms for vehicle remote control [PA-26].

In addition, to the above industrial initiatives, it is important to mention that there are three collective effort initiatives whose objective is to collaborate in the creation of global standards which contribute to the digitalization of the Port Industry. Specifically:

- **International Taskforce Port Call Optimization** [PA-27], is about optimizing speed, draught and port stay, leading to lower costs, cleaner environment, more reliability and safety for Shipping, Terminals, and Ports.
- **TIC 4.0** [PA-28], whose mission is to promote, define and adopt standards that will enable cargo handling industry to embrace the 4th industrial revolution
- **Digital Container Shipping Association** [PA-29], whose goal is to make shipping services easy to use, flexible, efficient, reliable, and environmentally friendly.

### 3.2.2 State of the art in Smart Safety of Workers

There are several areas that can be impacted and improved by the application of I4.0 in the construction industry such as increased productivity, quality, flexibility, and production speed but more importantly safer and better working conditions. BIM and a cloud-based Common Data Environment (CDE) are central to the Construction 4.0 as they provide the framework upon which integrated digital tools are built with the help of image and laser scanning technology, AI and cloud computing, big data and data analytics, reality capture, Blockchain, 4D simulation and AR [SSW-1].

#### 3.2.2.1 Scientific review

Construction sites exhibit unique safety challenges because of characteristics such as complicated engineering processes, complex and constantly changing work environments, temporary organizational structures, non-standardized worker behaviors, decentralized crews operating or working in the proximity of heavy machines, concurrent collocated activities, time pressure and tight schedules [SSW-2]. Many accidents are caused by unsafe behavior and involve striking against or being struck by moving objects or vehicles, slips, trips and falls from height [SSW-3].

The implementation of a behavior-based approach [SSW-4] to construction site safety [SSW-5] follows a few basic steps, namely identification of unsafe behaviors, observation, intervention, review, follow-up, monitoring and training [SSW-2]. One of the drawbacks of the behavior-based approach is the fact that it is based on the premise that workers are trained to identify hazards and are empowered to stop potentially unsafe behaviors and report dangerous activities if they happen to witness them. The integration of computer vision and deep learning can aid the implementation of behavior-based in construction through a process of observing, recording, understanding, learning, and predicting unsafe behavior. However, it comes with limitations such as the lack of training data and metrics for performance evaluation, poor generalization and inability to adapt to changing safety requirements, inability to detect small/hidden objects and multiple co-occurring safety-related features [SSW-3].

#### IoT systems for the construction sector

The development of the IoT technologies, in particular by making use of recent achievements in the areas of wearables as well as sensors and activators integrated with the various components of smart personal protective equipment (PPE) used in the workplace, makes it possible to exploit the potential of these technologies to better support systems for the detection of hazards and management of occupational risks, particularly in workplaces where environmental conditions are subject to dynamic changes that can have serious consequences for human health and life [SSW-6].

The use of IoT technologies in this domain leads to fundamental paradigm shifts in occupational health and safety management that consist in moving from traditional methods of carrying out collective risk assessment for specific groups of workers to assessment methods which allow to determine the level of risk individually

for each worker, and, moreover, in replacing existing periodical risk assessment approaches by continuous monitoring of hazards in the working environment in real or near real time. In addition, the use of extensive IoT networks for simultaneous monitoring of hazards and risk assessment of many employees working in a given workplace allows the collection and analysis of large data sets of sizes allowing for the use of advanced Artificial Intelligence techniques, such as machine learning or big data analytics, and thus can give a new “cognitive” dimension to occupational safety and health management [SSW-7].

Benefits of the application of IoT-based system for workers’ safety in construction sites were also studied by Kanan et al. [SSW-8] who proposed an autonomous system that is able to monitor, locate, and warn the workers entering the danger zones. The following techniques were applied for the purpose of detection and identification of workers: the 868 MHz radio frequency, directional antennas, and the 40 kHz ultrasound waves. Moreover, the workers were equipped with wearables that included a radio transceiver, a wake-up sensor, an alarm actuator, and a GPRS module. In this paper, an issue of battery consumption of IoT devices was also considered as the authors applied a power-saving scheme. They also implemented photovoltaic cells for powering wireless nodes, which can operate in both indoor and outdoor conditions.

A summary of the application of advanced machine learning algorithms in the construction sector for the purpose of supporting resource, risk and logistics management was presented by Akinosho et al. [SSW-9]. In the paper, authors indicate future innovations and prospective deep learning challenges and one of the areas of potential application of this technique is on-site safety and health monitoring, as well as risk mitigation and analysis. In this field a special focus was paid on early detection of tiredness or fatigue e.g., by means of video monitoring system. Besides potential benefits of the use of deep learning in construction industry, authors also draw attention to such challenges as black box, ethics and data privacy, cybersecurity, and cost of adoption of these techniques. A specific issue of safety of road repairing workers was undertaken by Ma Li [SSW-10] who proposed IoT-based system using a robotic arm aimed at accidents prevention due to thermal stress and vehicle accidents. Notifications indicating the need for drinking water, a possibility of slipping on the wet floor, as well as “no entry” instruction when too many workers are on site were suggested in the paper. Moreover, Ma Li suggests providing workers with important safety knowledge e.g., by posting such notifications at a webpage. In addition, workers can receive relevant information together with a voice message via QR code before entering the site.

High potential of integration of Building Information Modeling (BIM) with real-time data from the IoT devices in order to improve construction and operational efficiencies was indicated by Tang et al. [SSW-11]. On the basis of a comprehensive review, authors identified the following application domains: Construction Operation and Monitoring, Health and Safety (H&S) Management, Construction Logistics and Management, and Facility Management. Based on the conducted analysis, in the domain of health and safety management authors identified H&S trainings and on-site monitoring. Integration of BIM with IoT devices for the purpose of worker training was mainly aimed at tracking of trainers, trainees, materials and equipment and was used to analyse safety and productivity [SSW-12], [SSW-13]. For the purpose of on-site monitoring BIM and IoT integrated systems were mainly applied in order to achieve real-time data query, risk identification, visualization and notification over BIM model. In this domain, a need for a portable early warning device for workers was indicated. Moreover, authors [SSW-11] summarized several limitations of the already performed research works such as: leveraged RFID tags and BIM for monitoring location data and sending warnings, confirmation of scalability and reliability of data from health monitoring due to limited scenarios of performed testing, ease of implementation of the proposed solutions considering workers’ privacy, and sensor reliability and energy efficiency of battery.

### **Health and Safety monitoring and optimization using Augmented Reality**

The AR technology in construction is mainly used to visualize digital records relating to the functional properties of a building object. These records are presented in a parametric form and constitute a source of data about the facility that is available to stakeholders at the early stages of a construction project. Integrating AR technology into a IoT system consisting of other sensors capable of monitoring and improving health and safety in a construction site is quite a new approach. The use of AR goggles can allow the visualization of information obtained by different types of sensors (e.g., control of access, monitoring of use of required PPE, verification of requires trainings, etc.). The AR system integrated with Building Information Modelling (BIM) allows managers to check and control the work efficiency of employees, as well as employees to confirm their work



more easily [SSW-14] more effectively. Five trends of future development are anticipated: (1) the increasing rate of complex construction engineering could result in more intractable safety issues, the ICT tools with VR/AR support are the vital tools to be developed for achieving practical functions in improving safety performance; (2) the body of knowledge on safety science will contribute to more clear principles to support the VR/AR methods or tools for solving construction safety issues; (3) the approaches on ergonomics considering numerous human factors could become one of the critical assessment on VR/AR-CS systems; (4) the applicable theories in psychology will be adopted to make more situational experiments for evaluating the application effect of VR/AR-CS systems; and (5) the finer details of VR/AR environment are expected to attract significant attention on establishing more safety incidents' simulations to specifically examine and discuss the immediate reaction and response of workers. These development trends could make an optimal combination to improve the future safety management in construction industry [SSW-15].

The use of AR technology for evacuation has been known for many years. An example is the indoor augmented-reality evacuation system for the Smartphone using personalized Pedometry [SSW-16]. The authors describe how the system they developed leverages the sensors on a smartphone and utilizes Augmented Reality, cloud information, daily user walking patterns and an adaptive GPS connection method to deliver critical evacuation information to users' mobile phone in indoor emergency situations. AR technology is also used for practical training in the field of evacuation (building evacuation training system). Building evacuation training systems and training of employees in an organization have a vital role in emergency cases in which people need to know what to do exactly. In every building, procedures, rules, and actions are attractively shown on the walls, but most of the people living in that building are not aware of these procedures and do not have any experience what to do in these dangerous situations. In order to be able to apply these procedures properly in an emergency situation, community members should be trained with the state-of-the-art equipment and technologies, but to do so, up-front investment and development of such a system are necessary. In this study, augmented reality (AR) technology was applied to realize a game-based evacuation training system that implements gamification practices [SSW-17].

Virtual Reality (VR) has been additionally concluded as an efficient tool for providing understanding of the evacuation process to building designers and end users [SSW-18], [SSW-19] and make people accustomed to a building environment and prepare them for an evacuation [SSW-20]. Use of VR in evaluation of exit sign placement and escape route design, is nevertheless a novel approach in the building [SSW-21]–[SSW-24]. VR technologies can significantly enhance the performance of building navigation. VR provides a more realistic means for viewing the interior and exterior of buildings than a plain two-dimensional (2D) drawing can offer. VR-based 3D building navigation has been used for generating practical or aesthetically pleasing designs [SSW-25].

In addition to research related to a use of AR/VR technologies, it is worth noting that AR technology is already covered by the standardization area [SSW-26]. In terms of the project, the following standards are of a particular interest:

- P2048.4 - Standard for Virtual Reality and Augmented Reality: Person Identity. The standard specifies the requirements and methods for verifying a person's identity in virtual reality.
- P2048.5 - Standard for Virtual Reality and Augmented Reality: Environment Safety. This standard specifies recommendations for workstation and content consumption environment for Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR) and all related devices where a digital overlay might interact with the physical world, potentially impacting users' perception. This standard focuses on setting quality assurance and testing standards for qualifying products in said environments, achieving satisfactory safety levels for creation and consumption environment for all or majority of related products available for consumer and commercial purposes.

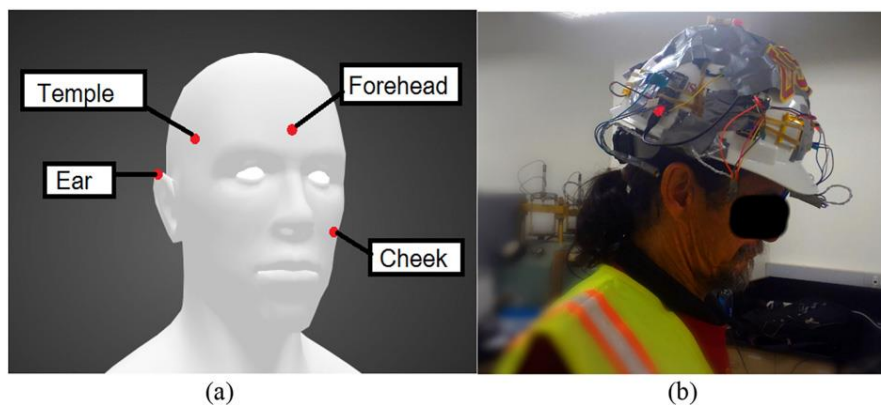
### **Smart actuation of intelligent IoT devices with an adjustment to individual needs**

Construction is one of the largest industries in the world. The International Labour Organization estimates that in industrialized countries as much as 35% to 40% of deaths occur in construction. Work in this sector requires physical effort, is often performed in difficult environmental conditions, which may contribute to poor assessment of the situation, fatigue, lower productivity and its poor quality, and an increased risk of accidents [SSW-27], which directly translates into employee safety. For this reason, it is very important to monitor



workers health status so that irregularities can be noticed in time. This can be done by assessing the physiological parameters of employees that reflect their actual condition.

The effect of thermoregulatory changes on the possibility of assessing the increase in employee fatigue in order to increase safety was investigated by Arayla et al. [SSW-27]. For this purpose, they designed a system consisting of four infrared sensors attached to a safety helmet, which collect skin temperature from selected places on the face. In addition, they extended their system to monitor the heart rate and brainwave signals measured by the EEG sensor. To monitor the heart rate, they used GARMIN Vivofit, a commercially available fitness monitor wristband that is connected to a heart rate sensor on the chest. The sensor sends data to the Vivofit device, which is a data logger, which is then synchronized with the GARMIN servers. This gives the option to get heart rate measurements as raw data. The sensor they used to record different frequencies of brain wave signals is the Neurosky Mindwave, which is available with the NeuroExperimenter software. The sensor has one dry electrode placed on the forehead. The sensors used to study temperature changes are non-contact infrared temperature sensors (MLX90614), connected to a data logger (Adalogger M0). They are non-contact sensors, moreover, this type of sensors ensures high reliability and shorter response time. They were placed at a distance of about 1 cm from the skin surface on selected places of the face shown in Figure 70a. The face was used for temperature monitoring because it does not contain the working muscle groups involved in the work, consists of several vascular areas, and is not obscured by clothing or protective equipment. For this reason, it is an area of the skin whose temperature is not influenced by additional factors [SSW-27].



*Figure 70. Helmet developed by Arayla et al. a) Facial skin temperature monitoring locations; b) Test person wearing a developed helmet [SSW-27].*

Edirisinghe and Blismas [SSW-28] have developed a prototype of a smart high visibility vest with temperature sensors to protect workers from overheating (next figure). The microcontroller (LilyPad Arduino USB) used in the vest, powered by a 3.7V LiPo battery, and temperature sensors were sewn to the fabric, and then attached to the protective vest that construction workers wear. It was decided that the electronics used in the solution would not be permanently sewn to the vest due to its aesthetics, ease of use and the possibility of easy maintenance. Thanks to the possibility of detaching the electronics, there is no problem to wash the vest. Applied the LilyPad Arduino is a small thermistor-type temperature sensor that has been sewn into a protective vest with conductive threads and measures the ambient temperature on an ongoing basis. The developed vest has a built-in visual (LilyPad RGB LED) and audible (LilyPad Buzzer) warning mechanism. Warnings appear when temperature values are not within the optimal range. They are in the form of a three-color LED light, the colour of which depends on the temperature value (blue - low temperature; green - normal temperature; red - high temperature), and a speaker. LEDs are sewn on the bottom side of the fabric, so they remain visible through the vest. Additionally, an acoustic signal sounds depending on the situation. It is active only when the temperature reaches unacceptable values. When the temperature is too low, the speaker emits a "beep" every 500 ms, while when the temperature is too high, it plays warning music.



Figure 71. (a) A vest with temperature sensors (b) and LED diode signalling incorrect temperature values [SSW-28].

Hashiguchi et al. [SSW-29] developed a method to assess the risk of the workload of individual construction workers in real time. For this purpose, they used the acceleration of employee movement, age, body mass index and wet bulb globe temperature (WBGT), which considers temperature, humidity, and thermal radiation. The physical activity of employees was measured on the basis of ECG signals recorded with smart clothing (next figure, on the left). For this purpose, stretchable ECG electrodes integrated with the pulse measuring equipment were used. The heart rate itself is done by detecting R-R intervals in the ECG signals. Using a low energy Bluetooth device, the heart rate and 3-axis acceleration data was transferred to the data collector (CS2650). Then the data was transferred and stored on a server installed in the network using an established wireless access point in the work area (next figure, on the right). Based on the height, weight and age of the employees, the body mass index (BMI) was calculated and the WBGT was calculated based on the working time. WBGT was measured at 5-minute intervals to determine the temperature and relative humidity of the working environment [SSW-29].

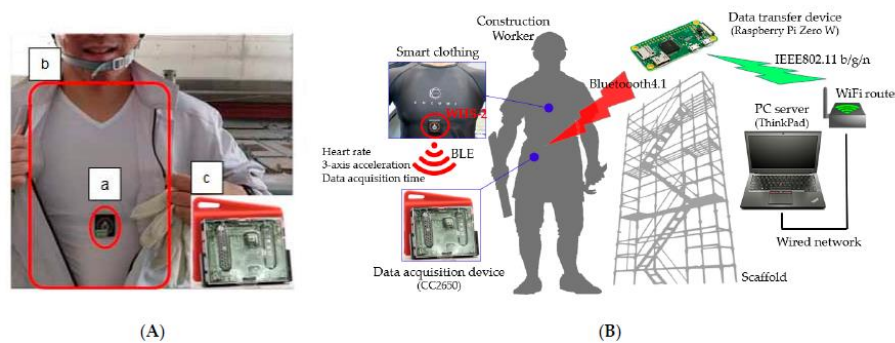


Figure 72. A view of the measuring system for construction workers (A), where: a) a heart rate and acceleration sensor WHS-2, b) smart clothing (COCOMI), c) data acquisition device (CC2650), and the system configuration (B) [SSW-29]

In fact, there are very few documented uses of intelligent systems in construction. In practice, it comes down to the proposed solutions for improving the safety of construction workers, which have not been implemented so far. [SSW-28] designed a vest system to monitor the ambient temperature of construction workers in real time to prevent workers from being exposed to excessive heat. [SSW-30] proposed the "Worker 4.0" system, which is designed to comprehensively collect information about the employee (such parameters as: heart rate, respiratory rate, body temperature, body movement, body orientation) and his environment to ensure the safety of employees and be able to better understand the factors influencing labour productivity. For the purpose of prevention against overheating of the personnel at the construction site, several cooling solutions have been designed so far. However, those individual devices were not a part of the IoT ecosystem, usually in the form of vests using phase change materials (PCM) and fans without the automatic control. Hoon Kim et al. [SSW-31] developed an IoT system measuring the physiological parameters of construction workers. These parameters are measured using a commercially available armband with three sensors: PPG, temperature, and acceleration. The PPG sensor measures the volume of blood flow by detecting a change in the intensity of the reflected light. The accelerometer that measures the acceleration shows the current position of the employee, and the thermometer provides information about the temperature of his skin. All system components, which include the microcontroller (MCU), GPS module, low-power wide area network (LoRa) module and power supply, are located on a single board. Data from the MCU determine the current physiological state of the employee, which

is sent directly to the network and to the smartphone application through the LoRa network. The system consists of two parts: the overall heat rating (OHS) and the individual management system (PMS). OHS aims to protect construction site workers from potential overheating diseases by adopting the Thermal Comfort Index (TCI) provided by the Korean Meteorological Administration (KMA). TCI is assessed based on wet-bulb global temperature (WBGT) but is modified to differentiate specific work environments and age groups. In the OHS system, thermal environmental data is retrieved from the KMA through the Internet and assessed against the TCI. The OHS system allows the manager supervising the work of employees to assess whether they should take a rest. The PMS system (PWB-300 wristband) provides monitoring of individual health, where local meteorological problems may not always be the main cause of irregularities. The data obtained from the employee, after filtration, constitute the basis for determining the individual level of risk. If the values of the individual physiological data of the employee and the local meteorological data from OHS are found to be incorrect, the developed platform warns about the irregularities in real time. The shift supervisor is notified of these results through the Internet or smartphone [SSW-31].

Stress also affects the health of employees, and thus their safety. Stress monitoring can be done by measuring EEG signals. EEG-based identification of worker stress on construction sites was made by Jebelli et al. [SSW-32]. The EEG signals were collected in 14 different channels using a wearable EEG device. Moreover, workers' salivary cortisol was also collected in order to identify stress level. The authors used several supervised learning algorithms to recognize employee stress. It turned out that the fixed windowing approach and the Gaussian Support Vector Machine (SVM) gave similar accuracy of 80.32% as in clinical domains. A procedure of applied stress recognition is presented in the scheme below (see Figure 73).

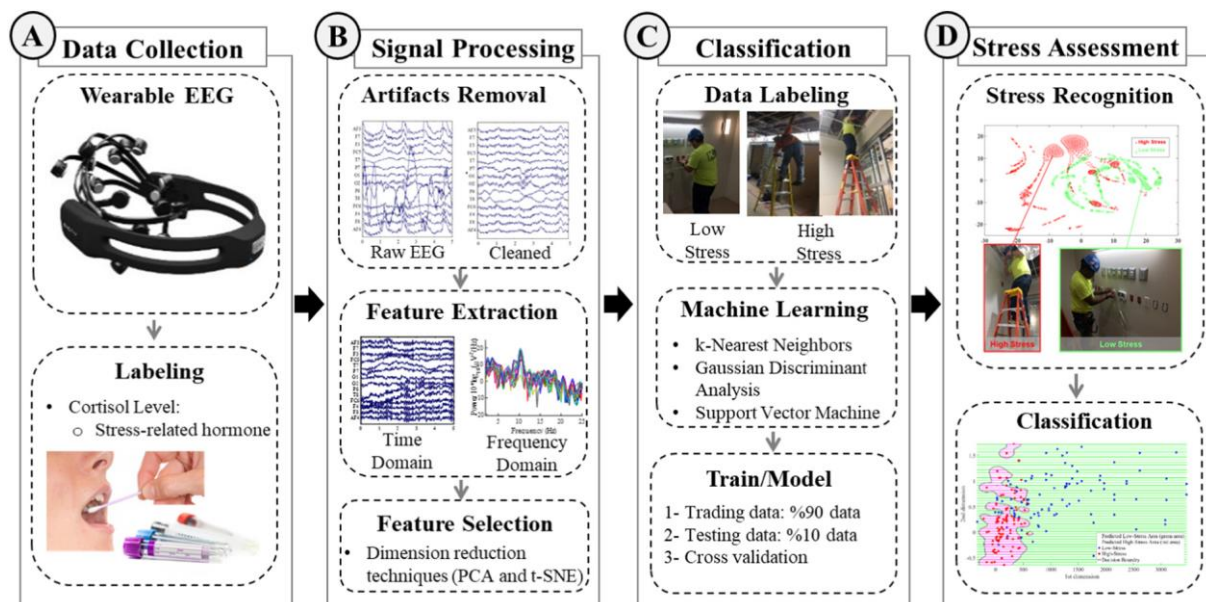


Figure 73. Procedure of stress recognition [SSW-32].

Runkle et al. [SSW-33] investigated the occupational, environmental and behavioural factors that contribute to individual variations in heat load in outdoor workers with wearable devices. For this purpose, they conducted tests on a group of employees for 4 weeks during their working days. The employee's exposure to ambient temperature was measured at 5-minute intervals throughout the working day using a Thermochron iButton temperature sensor that was worn on the outside of the shirt lapel. In addition, heart rate measurement was used to determine the heat load. For this purpose, the generally available Garmin Vivoactive HR wristband was used, which uses optical heart rate detection at 1-minute intervals. Moreover, it was used to collect GPS coordinates of employees. Additionally, a survey was conducted among the surveyed employees in order to get to know better their working conditions. The questions concerned issues such as time spent working outdoors, access to shade, access to a cooling area, access to regular breaks, removal of personal protective equipment, and the perception of the impact on productivity while working outdoors in heat. In addition, employees filled out an activity diary every day to capture changes in professional activity and location.

Gatti et al. [SSW-34] examined the usefulness of the so-called Physiological Status Monitoring (PMS) that measures heart rate and respiratory rate by comparing its measurements with laboratory instrument



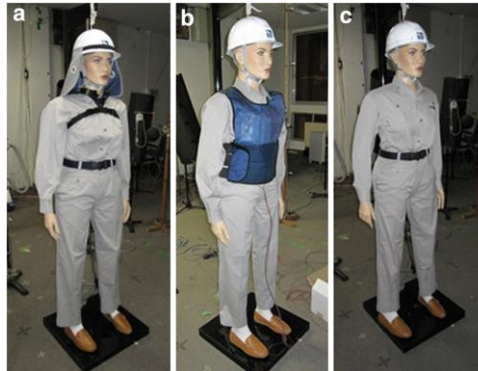
measurements taken during rest and during dynamic activities reminiscent of the routine activities of construction workers. For this purpose, they used two types of PMS: BioHarness BT 1 manufactured by Zephyr Technology Corporation (Annapolis, MD, USA) and Equivital EQ-01 manufactured by Hidalgo Ltd (Swavesey, UK). The PMSs used measure the pulse and respiratory rate by appropriately collecting the electrical signal from the heart with electrodes built into the PSM chest strap and measuring the elongation and contractions of it. Random displacement of this belt during movements and the electrical activity of the skeletal muscles can affect the measurements taken. This EMG activity may overlap with the heart's electrical signal. The PMS chest straps are placed under the breastbone using moistened skin electrodes. In order to avoid irregularities related to the described straps, additionally for comparison purposes, an ECG device at 500 Hz with five connections was used (CASE Exercise Testing Electrocardiogram, GE Healthcare, Waukesha, WI, USA) and a nose clip and mouthpiece connected to a metabolic cart developed by New Mexico University Scientific Laboratory to determine the respiratory rate by collecting inhaled and exhaled air. After the tests, the results obtained from both PMS and laboratory equipment were subjected to statistical analysis and comparisons. The developed results allowed to determine that BioHarness BT 1 turned out to be the correct PMS for heart rate assessment both in the resting state and during dynamic activities, but it is not able to reliably determine the respiratory rate during dynamic movements. Equivital EQ-01, on the other hand, cannot be taken into account in measuring the physiology of construction workers, because the collected heart rate data during exercise turned out to be incorrect.

Lee et al. [SSW-35] carried out a study on the usefulness of wearable sensors for monitoring the physiological condition of construction workers during work and off-work. During their work time, employees wore a Zephyr Bioharness™ 3 sensor (Medtronic, Dublin, Ireland), which is used to record ECG signals using chest sensors with a frequency of 250 Hz and three-axis acceleration. The data from the ECG was used to determine the heart rate value, and the acceleration allowed the assessment of employees' safety-related behaviour by analyzing ergonomic positions of employees. Additionally, during the research, workers also wore an ActiGraph GT9X (ActiGraph, LLC., Pensacola, Florida) wristband on their wrist for 5 days 24 hours a day. The device collected data such as: acceleration, level of physical activity and sleep quality. In addition, a survey among the respondents was conducted on personal information and feelings related to the devices used. The survey showed that employees rated the ActiGraph GT9X wristband much better than the Zephyr Bioharness™ 3 sensor due to the comfort of wearing it and its low weight. The conducted research shows that in order to explain how the physiological responses of an employee can change his work requirements and how they affect the safety and efficiency of work, not only the sensors themselves should be used, but also the individual information mentioned above should be obtained regularly from employees.

Mehata et al. [SSW-36] proposed intelligent devices to ensure the safety and health of construction workers. The system presented by them consists of two elements, which are wearables and a smartphone. The wearables include a smart band and helmet. Communication between the mentioned elements is possible thanks to the GSM module. The smart band monitors the pulse and temperature (LM35 sensor), and the acquired data is collected in the cloud controlled by the superior. The designed helmet detects a fall or skid of an employee thanks to the use of an accelerometer. When the described system detects a physiological abnormality or a worker fall, the supervisor is alerted of the threat. The system is protected against false warnings thanks to a button that employee can use within 1 minute from the occurrence of an irregularity to stop sending an alert. The concept of the system has been tested on a system prototype, which consists of Arduino Uno microcontroller, Wi-Fi-serial IoT, GSM/GPRS modem, heart rate sensor, temperature sensor and accelerometer.

Working in the construction industry also involves exposure to different temperatures. Working at high temperatures may turn out to be dangerous, as it results in an increase in body temperature considered comfortable and safe. Therefore, there is a real need to use a system that allows the employee's body to cool and thus maintain a comfortable body temperature. The cooling effect can be obtained by various methods. Cooling with fans and phase change materials (PCM) was tested using a thermal manikin by Miura et al. [SSW-37]. The first of the proposed cooling solutions uses fans to achieve a cooling effect (Figure 74a), and the total weight of the device is 700 g. There are two fans with leads in the form of channels made of plastic pipes on the belt. There are three 1.5 cm<sup>2</sup> air outlets on each duct. The fans are powered by batteries, and the amount of supplied air is estimated at about 10 m<sup>3</sup>/h for one fan. In this case, mainly the face and neck are cooled, and the cooling effect itself is caused by the high velocity of air around the body. The second presented device is a PCM vest (Figure 74b). On the inside of the vest there are 11 pockets where it is possible to place one or two PCM

elements per pocket. Two types of phase change materials were used in the study. One of them is water gels that change from solid to gel at 0 °C. The second is sodium sulphate which turns from solid to gel at 28 °C. The weight of the vest with 22 PCM elements is about 2.5 kg. The tests that were carried out for the described devices lead to the observation that the device with fans has an almost constant cooling effect for about 3 hours, while the effect of using the vest varies in individual measurement cases and may last about 30 minutes. The fans mainly cooled the face and skull and contributed to an increase in total body heat loss by about 9%. The obtained results show that the vest has a lower cooling effect than fans.



*Figure 74. Thermal manikin wearing cooling devices for construction workers a) fans; b) PCM; c) reference clothing [SSW-37]*

Yi et al. [SSW-38] designed a personal cooling system which main part is a ventilation element consisting of a battery pack and a pair of fans. The cooling capacity of the designed system was tested on a thermal manikin. A generally available fan was selected and tested for comparison. The aim of the study was to find a ventilation element that would provide longer operation time and greater cooling power than the reference unit. The element proposed by them showed much better performance in terms of air flow rate and working time than the unit available on the market. Moreover, its cooling power was higher and amounted to 68 W, while the cooling power of a commercially available element was 51 W.

### Identification of suspicious and undesirable behaviours within the construction site

Loss of balance, overturning or falling down are one of the most serious causes of human body injuries. The most serious consequences are falls from heights, e.g., in the work environment, and falls at home by elderly people. In such cases, it is very important to quickly detect the accident and inform people who can help the victim. This allows to shorten the time between the occurrence of a fall and the assistance of the appropriate technical and medical services. As a result of this, the hospitalization time is shortened, and the potential risk of serious post-traumatic complications is minimized. The identification of an uncontrolled fall and reporting it to the relevant services requires the use of advanced technical devices. Nowadays there are not many applications of IoT solutions related to this aspect of safety at the construction site. Yang et al [SSW-39] developed a method that automatically detects, and documents potentially accidental falls based on employee kinematic data captured from wearable inertial measurement units (WIMU).

### 3.2.2.2 Relevant initiatives

Constructing a fall detection device is a relatively difficult task. In most cases, fall detection is based on data from an accelerometer [SSW-40] placed on the head, near the centre of gravity, hips or on the human wrist. In this type of solution, it is necessary to define a reference level that characterizes normal activity, e.g., walking, sitting, squatting, etc. These data are obtained during typical human activities, and significant deviations from this pattern activate the alarm procedure. Practically in all such solutions, their operation may involve the risk of triggering false alarms, e.g., when jumping or running. In the paper [SSW-41], the authors proposed a fall detection concept based on the analysis of data from a biaxial gyro sensor placed on the torso and measuring angular velocities and angles. A special algorithm identifies the results and compares them with the threshold values. There are also solutions that use an accelerometer, a gyroscope or a magnetometer to detect falls [SSW-42], [SSW-43]. Thanks to this, the number of false alarms can be significantly reduced. In the solution presented in [SSW-44], apart from the sensors mentioned above, a barometric sensor was also used. This allows to



accurately determine the direction of fall. There are also solutions based on the analysis of the monitored person's movement and position, e.g., with the use of video cameras [SSW-45].

A different group of fall detection systems are systems based on the use of mobile phones [SSW-46]. These are devices that can be equipped with an accelerometer, gyroscope, or barometer. Appropriate software allows to identify the occurrence of a fall and other effects, e.g., immobility, etc. Using a mobile phone for such a function creates an additional possibility of determining the position in which its user is. This is especially important when it requires both medical and technical assistance, e.g., evacuation from the suspended state after the fall arrest by personal protective equipment. Such solutions use GPS and send information outside via BT, Wi-Fi, or GSM. Systems of this type are currently used in industrial practice [SSW-47].

Determining the employee's position, e.g., on a construction site, is very important from the point of view of his safety. The knowledge of this position can be used, for example, in the event of falling from a height, fainting, getting hit by a falling object, etc. Another use of determining the position is supervision over the presence of employees in safe zones and informing them when entering hazardous zones [SSW-48]–[SSW-51]. Technical solutions of such systems are most often based on GPS technology or other telemetric techniques. In relation to access restrictions and localization, it should be stated that, GPS tracking at the construction site is often impossible. However, there are also other methods enabling locating of people in building environments. An example is a method that uses AprilTags that are linked to previously known coordinates in the 3D Building Information Model (BIM). Using the UAV on-board cameras and extracting the transformation from the tag to the cameras frame, the UAV can be localized on the site. It can then use the previously computed information for navigation between critical locations on construction sites. Park et al [SSW-52] developed a mobile distance sensing and warning system that uses BLE technology as the main communication element used to detect the distance between workers and equipment. Luo et al [SSW-13] have developed an intelligent real-time video surveillance system for construction that detects people and machines in a hazardous area. The indoor GPS system was developed by Redpoint Positioning Corporation (RPC) and commercialized as a wearable device [SSW-53]. It is implemented in the form of a protective vest, thanks to which the employee can wear a vest with a built-in GPS system instead of a traditional vest. The system allows the person responsible for employees to define dangerous zones on the workplace map. The vest allows you to track the location of an employee in the workplace in real time and send this information to the manager. Thanks to this, when an employee enters a zone marked as dangerous, he will be automatically notified via a wireless warning system built into the smart vest, which significantly increases his safety.

The human head is a very sensitive part of the body exposed to various dangerous factors occurring at workplaces in the construction industry. This mainly applies to mechanical factors, i.e., hitting dangerous stationary objects and falling objects. Examples of other factors are high or low temperature, infrared, and UV radiation. For this reason, a number of protective helmet solutions have been developed that are integrated with sensors for acceleration, temperature, UV radiation, etc. Such a device also includes a module for data transmission and user location identification [SSW-54]–[SSW-57]. The fall arrest of the user of personal fall protection equipment can also be identified by suitable detectors. These detectors can be installed in series with the components of the protective equipment (e.g. lanyards, shock absorbers, etc.). The principle of operation is to generate a signal at the moment of exceeding the limit value of the fall arresting force. This signal is remotely transmitted to people supervising work or appropriate emergency services. Currently, there are no publications indicating the practical use of such devices in construction industry.

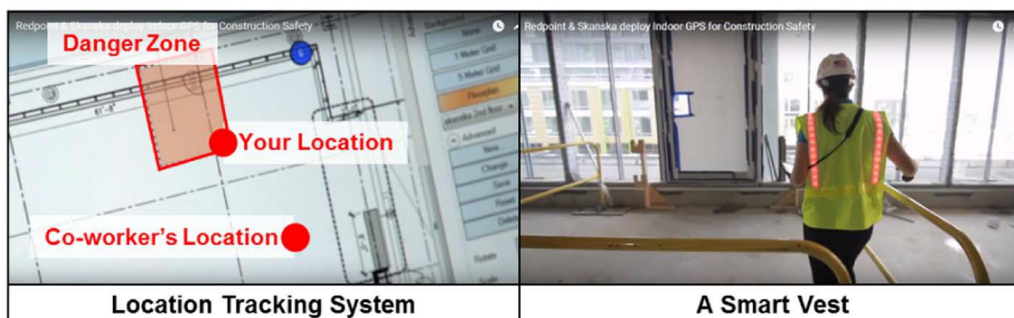
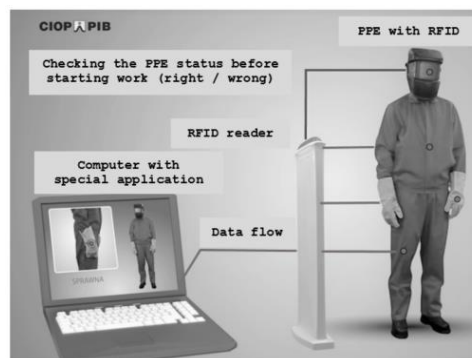


Figure 75. A vest with location tracking system developed by RPC.

Another issue that relates to undesirable behaviours at the construction site considers a use of personal protective equipment (PPE). To monitoring of a use of PPE, the RFID systems can be used. Such systems usually use the 865 MHz (UHF) and 2.4 GHz (MW) frequency bands. The reading range is several meters. Passive RFID tags have been used for many years in systems designed to control the use of personal protective equipment [SSW-58]. Various forms of access control systems using automated-identification (ID) technologies combined with time and attendance recording capabilities are available on the market. Barcode and (passive) RFID-based systems are already partly used on construction sites.

An example of a system operating on the basis of the concept of the Internet of Things (IoT), in which RFID tags were attached to PPE, is the automatic identification and management system for PPE in the workplace developed by CIOP-PIB [SSW-59]. The operational principle of the developed system is shown in the Figure 76. The reader communicates with the electronic tag attached to the personal protective equipment (e.g., protective clothing, helmet shoes, etc.). The tag consists of an integrated circuit with a flash memory with a capacity of several kilobytes. Data about monitored PPE and data from the antenna are saved in the memory. The antenna embedded in the tag transmits the data stored in the tag to the reader, and then the data is transferred to the database on the server. The application installed on the server processes this data, which is then visualized on the screen of user terminals. The described system uses RFID Motorola FX7400 readers and an AN489 antenna.



*Figure 76. The principle of operation of the system of automatic identification and management of personal protective equipment in the workplace [SSW-59].*

Monitoring of personal protective equipment using the system described above takes place on two levels: 1) always before starting work, 2) periodically (as specified in the PPE manufacturer's instructions). Such a procedure enables the control of the use of PPE, as well as the detection of exceeding the allowed time of use.

The operation of RFID systems integrated with personal protective equipment requires that the PPE user passes through the gate with the RFID reader. Gates can be placed in many zones in the workplace. This means that any workers may pass through the gate several times during one working day. The time of an employee's exposure to radiation depends on two main factors, including: 1) number of gates, 2) employee mobility. The amount of energy reaching the worker also depends on the personal protective equipment used, which can be a barrier to radiation exposure.

### 3.2.3 State of the art in Cohesive Vehicle Monitoring and Diagnostics

The ASSIST-IoT pilot on cohesive vehicle monitoring and diagnostics will focus on vehicle-condition diagnostics, aimed to OEMs, fleet managers and automobile repair professionals. Data streams coming from different sources will be integrated to provide insight into the vehicle condition, properly schedule predictive and corrective maintenance tasks, over-the-air update diagnostics firmware, verify in-service conformity, evaluate the need of vehicle recalls, etc. To this end, data will be collected from the remote monitoring of powertrain parameters as well as for the evaluation of external vehicle damage.

#### 3.2.3.1 Scientific review

To date, monitoring and diagnostic functions largely reside within the vehicle, or more specifically, within the electronic control modules (ECM) or powertrain control module (PCM) of the vehicle. On Board Diagnostics mechanism are enforced by regulation, and the software must be able to diagnose any system potentially able

to vary the emission levels, presumable almost any subsystem of the engine. This forces a long software development phase, followed by extensive calibration efforts, since software code must be finished before the vehicle is marketed. This software development and calibration phase is sometimes identified as a bottleneck of the development time [CVMD-1]. That is exactly where NGIoT comes into play. Using information from connected cloud/edge resources, observing the behaviour of systems/subsystems in the fleet and applying statistical methods to complex mathematical problems within the real time domain will gradually become possible. The ASSIST-IoT reference architecture will be key enabler to such use cases. Another key could be the 5G standard, as it will include a dedicated band for Automotive, along with low latency connections. In that sense, the automotive pilot will be a unique value proposition: Innovative enabling technologies will become available just in time to correspond to new regulatory challenges in the mobility sector.

The OBD-II (On Board Diagnostic II) port has been used for automatic fail detection based on measured parameters of the vehicle, such as speed, engine and water temperature, battery charge level and error codes [CVMD-2]. These measurements can also be combined with additional sensors measuring, for example, vibrations (for crack prediction), gas leakage or liquid levels [CVMD-3], or vision systems [CVMD-4]. To that end, OBD-II dongles are connected with the in-vehicle Control Area Network (CAN) bus to fetch diagnostic data through the OBD-II port [CVMD-5]–[CVMD-11]; they also interact with external companion apps via wireless network to transfer data and commands. A recent study revealed that all the 77 dongles that have been assessed exposes at least two types of vulnerabilities related to privacy leakage, property theft and even safety threats [CVMD-12].

Eventually, the method of accessing the in-vehicle data will transform from traditional wired access via the OBD-II connector towards remote, over-the-air access [CVMD-13]. Technical enablers do exist to allow vehicles to communicate with nearby vehicles and roadway infrastructure through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I/V2x) communications [CVMD-14]. The V2V and V2I communications use wireless technology, such as Dedicated Short-Range Communications (DSRC), cellular network (e.g., 4G/LTE) or WiFi. However, there is a limited number of existing connected propulsion control system monitoring and diagnostic use cases deployed within the fleet.

There is an on-going debate about the access to vehicle data for several years now which has been dominated by the trade-off between cybersecurity and data access [CVMD-15]. This scope of the debate is no longer limited only to repair and maintenance information and is ever more relevant when it comes to connected autonomous vehicles [CVMD-16], [CVMD-17] or over-the-air (OTA) software update [CVMD-18], [CVMD-19]. On the one hand, OEMs want to have exclusive control over vehicle data access. To this end, the extended vehicle concept has been recently introduced to encapsulate the entity within the physical boundaries of a road vehicle and extend it by including off-board systems, external interfaces, and the data communication between them [CVMD-20]. On the other hand, several other stakeholders would benefit from open access to these datasets, such as drivers and aftersales service providers [CVMD-21], [CVMD-22].

Either way, the concept of the electronic horizon can only be enhanced by the availability of more in-vehicle data; data that is shared between vehicles in real time. The fact that modern cars are becoming IoT-devices means that they will not only consume static data provided through Advanced Driver-Assistance Systems (ADAS), but they will also acquire self-learning attributes (self-learning electronic horizon). In addition, they will be able to learn from other vehicles information about weather, traffic, or road conditions in the vicinity (connected electronic horizon) [CVMD-23]. AutoMat is an example of a Horizon2020 project that treats vehicles as rolling sensors that perceive various environmental and mobility parameters producing over 4000 signals per second per vehicle [CVMD-24].

Concerning powertrain sensors, production-ready sensors exist for most relevant intermediate and final variables for the control and diagnostics of the power plant. The last years have seen a significant advancement in automotive sensor development, in addition to classical lambda sensors, air mass flowmeters and various temperature and pressure sensors, some of the recent developments are:

- **Gas concentration sensors:** In addition to binary and linear lambda sensors, NOx sensors have been used for a while in automotive diesel engines [CVMD-25], resistive sensors for particulate matter [CVMD-26] are already in the market. Other sensors include ammonia (for urea slip detection and SCR diagnostics) [CVMD-27]

- ***In-cylinder pressure*** has been used in research from the very beginning of the IC engine for diagnosis, and many applications have been proposed for conventional SI and CI engines (e.g., for misfire detection [CVMD-28], for in-cylinder trapped air mass estimation [CVMD-29], charge composition [CVMD-30], etc.); however, it has not been implemented until recently to series production.
- Efforts are being made for developing ***fuel composition sensors*** able to operate with a wide range of fuels (including gasoline, diesel and other alternative fuels). For example, light transmission in the infrared spectrum [CVMD-31] or electrical capacitance [CVMD-32] measurement may be used for quantifying several relevant fuel quantities and inferring fuel composition. As far as fuel reactivity may be determined, such sensors may play a major role for the implantation of new combustion technologies.

It still is an open question which sensor set is more suitable for an accurate estimation of vehicle emission footprint [CVMD-33], [CVMD-34]. Although gas pressure, air mass flow and concentration sensors are widespread, observers and system models are widely used, and sometimes used as feedback quantities, e.g., in [CVMD-35]. Many of these models are run in modern ECMs, and the results of the models are available in internal ECM variables. To some extent, model-based control has been implemented in several powertrain subsystems.

Different approaches have been presented for harnessing the information connectivity offers for maintenance and diagnostics, including manufacturer modification of software and calibration along service life [CVMD-36], third parties service providers [CVMD-37] to user centred services [CVMD-38], [CVMD-39]. Data processing and analysis of automotive fleets data stands a major difficulty, because of the variability of use cases, differences in installed parts, and differences in ECM calibrations [CVMD-40]. Stored data may be used for the diagnostics itself [CVMD-41], [CVMD-42] or for developing new products and services [CVMD-43]. While most published results present exclusive cloud diagnostics approach as opposed to conventional onboard diagnostics, cloud-edge diagnostics is also under research [CVMD-44].

Predictive maintenance is commonplace for commercial fleets to reduce downtime and to increase operational efficiencies. Tracking and analysing driver habits to take appropriate service actions requires statistical modelling and application of AI/ML techniques. These have already been developed within, and successfully applied to, other application domains. Recommendations for future research in this context include developing sensing techniques for vehicle equipment to improve the quantity and quality of data, compare the results of the application of different ML algorithms, or ensembles, to predictive maintenance tasks and create benchmark data sets [CVMD-45].

A basic car maintenance step is the visual inspection of the physical boundaries of a vehicle including body, underbody, and tyres. This task has been traditionally performed manually by experience personnel, but several systems have been developed to automate the process. Ford Motor Company factories use a moving structure made up of several light bars (high-frequency fluorescent tubes) and a set of cameras in fixed positions around the stationary car body, that can detect millimetric defects of 0.3 mm diameter or greater with different shapes using Photometric stereo [CVMD-46]. Vision-based methods often utilise cameras and light sources. For example, Kieselbach et al. used an array of 8MP CMOS cameras and LED elements [CVMD-47] and Zhou et al. used four LED elements and five plane-array Charge Coupled Device (CCD) cameras [CVMD-48]. A vision algorithm based on deflectometry techniques for detecting small defects on specular surfaces in general, and car body surfaces in particular, was developed by Molina et al. [CVMD-49]. Chang et al. detected tiny defects in a large image with uneven illumination using a deep ensemble learning algorithm based on YOLOv3. The experimental results show that their inspection system's performance is as good as that of senior inspectors but is 20 times faster [CVMD-50]. The challenge is to be able to manage and communicate all the generated information to the users. To improve both ergonomics and productivity of workers involved in the quality control inspection process of car body surfaces, Muñoz et al. introduced a new interface based on mixed reality (MR) tools that substitutes current 2D hand-held devices, i.e., screens, printers, PADs, etc. [CVMD-51].

The automatic defect detection can be implemented on vehicle body paint to enhance the efficiency and accuracy compared to the manual process. On this note, Zhang et al. [CVMD-52] proposed the adoption of MobileNet-SSD network. Both individual models, the traditional Single Shot Detectors (SSD) and the MobileNet algorithm may perform sub-optimally in real-time data detection. The combination of the two models seeks to improve model accuracy. Additionally, merging the BN and convolution layer improves the model speed. The results are encouraging as they are compared to models as VGG16-SSD, MobileNet and



MobileNet-SSD. Another work on painting defects was done by Xu et al. [CVMD-53] who proposes an automatic detection method with computer vision based on the Ant Colony Algorithm (ACO). The proposed method is based on three parts which are the APF-ACO edge detection, the reflective area elimination and defect area identification algorithms. In more details, the APF-ACO edge detection algorithm is aimed in indicating the position with the edges of the deflection. The reflective area elimination algorithm is to reduce the reflection in the images. The defect detection method is based on five types.

Exterior inspection to vehicles is studied in aircrafts vessels as it is essential for the safety of flights. The paradigms could be extended to other vessels such as cars. Jovančević et al. [CVMD-54] have proposed the completion of an exterior inspection with a pan-tilt camera on a mobile robot. The exterior inspection goals are to search for mechanical defects on the engine and cracks or damage caused by impacts. The work is deploying several image-processing approaches in addressing each inspection problem. For instance, shape edge detectors as though transform, and edge-drawing circles are deployed.

Engine inspections are another topic that is researched in literature as manufacturers are dedicating hours to pinpoint defections. Priya et al. [CVMD-55] suggest an automated disparity check system that leverages matching technique to pinpoint damaged components. The system relies on processing techniques and is developed in MATLAB. The Scale-Invariant Feature Transform (SIFT) algorithm is applied for the feature extraction that finds similarities between images. The comparison is between a perfect engine image against a sample that needs to be inspected.

Additional to engine inspects, manufacturers are performing dent inspections in their attempts in delivering a quality product. A vehicle body inspection with the use of a Region-based Convolutional Neural Network (R-CNN) is suggested by Park et al. [CVMD-56] for that purpose. The dents were highlighted by special lighting devices with LED and stripe cover that resulted in the creation of Mach bands. The Mach bands were essential in indicating the dents as a distortion was noted around dents. The structure of R-CNN was constructed upon four layers which were the input layer, two hidden layers, and the output layer. The ReLU activation function was deployed in the hidden layers. It should be added that the R-CNN objective apart from classifying the result of an image, was to localise the estimation of a dent based on a heat-map implementation.

Finally, the assurance sector has a place for the damage detection of vehicles as it is a research topic in literature. Harshani et al. [CVMD-57] are predicting the cost of the damages by implementing image processing techniques. The application demands the user to upload the image of the damaged vehicle to provide the severity of the damage and a cost estimation. The SIFT methodology is deployed for the application to be independent of the angle of the image that would be fed as a sample. The Bag of Visual words algorithm is implemented for the feature description. The classification of the severity of the damaged is the output of the SVM model.



## 4 NG-IoT H2020 Ecosystem

There are two main things that organizations want from the Internet of Things: operational efficiencies and new revenue streams. The connection of new devices, new networking paradigms, IoT platforms or innovative application with human in the middle, although it is easily depicted in presentations and architectures, is not so easily achieved and at the same time introduces several problems and concerns, mainly associated with interoperability, integration, and inclusion of evolutive new components to achieve the paradigm of Next Generation Internet of Things. Instant digital transformation, with an increase in revenues, efficiencies and an ocean of data is not so easy. Most organizations today are looking at undergoing a digital transformation and a big part of that will involve IoT new mechanisms and interfaces to interact with it and the definition of innovative business models to exploit it. But bridging the physical world with the digital world, or digitization, is just the beginning, as the next step will be related with Artificial Intelligence and the deployment of intelligence closer to the edge, even in more intelligent and less constrained devices.

The next step after creating a link between the physical and the digital worlds is digitalization. It is where a stakeholder uses these digital technologies to change a business model and provide new revenue and value-producing opportunities. This is where a regular business transforms into a digital business. And, although there are many technology solutions and many companies claiming to have the answer to IoT and the future evolution, no one vendor can offer a complete end-to-end digitalization solution that offers both operational efficiencies and new revenue streams, including the new features claimed by NGIoT, like low latency, security and privacy by design or the Tactile Internet approach. Digitalization involves nurturing of a vast ecosystem comprising devices, technology infrastructures, markets, end-users and industries worldwide. There are different ways to create, cultivate and maintain such an ecosystem. During the last years in the framework of H2020 different initiatives related to IoT projects have been maintained and additionally in the framework of 5G-PPP projects and other areas. Given the potential breadth and depth of an IoT ecosystem, this means cultivating partnerships and collaborating with the entire community. In such a continuously evolving landscape with new protocols, new ontologies, new platforms, there is a need for openness and flexibility and the only way to guarantee this is by partnering with the latest cutting-edge technology vendors and developers; so, as interaction with other research communities like Big Data, Artificial Intelligence, Robotics, electronics and 5G.

Different initiatives supported in some cases by funded CSAs or industrial alliances have evolved from IERC to AIOTI with different support from temporal initiatives like IoT-EPI (H2020 ICT30), IoT-LSP (H2020 IoT1), IoT security (H2020 IoT3 projects) and leading to the current H2020-ICT56 call for projects. Different corollaries can be added to this list, related with digital transformation, FOF, BDVa or 5G-PPP projects but we consider enablers of the different actions and developments. While EU-based initiatives and policies are doing significant amount of work to tackle such issues, often with very positive results, solutions suitable to tackle challenges arising for futuristic IoT usage scenarios are still missing. Future critical issues may have not been detected yet and be ready to appear in the close future, putting at stake user acceptance and the credibility of the whole eco-system hindering wider adoption of IoT solutions in potentially valuable markets.

### 4.1 European IoT calls

IoT ecosystem and community has been supported by different research and innovation action during the last 12 years. Following an approach Plan-Do-Continue-Act, next figure represents how the ecosystem has been evolving, with different research actions related with key enablers and components that have led to the NGIoT paradigm.



*Figure 77. Evolution of IoT ecosystem based on different research action.*

The ecosystem has consolidated and has evolved by means of different joint activities like:

- IERC (IoT European Research Cluster), which has kept active the activities of the IoT community by means of different research projects and several training and dissemination actions.

- IoT-EPI, cluster of seven H2020 ICT30 funded projects, coordinated and supported by two CSA (Unify-IoT and Be-IoT).
- IoT-LSP, cluster of the five Large Scale Pilots funded under H2020 IoT1 call for proposals and supported by two CSA (CREATE-IoT and U4IoT). After the execution of the projects and the closure of the CSA a cluster of SME and startups around the IoTNext concept has been created.
- IoT-ESP (European IoT Security and Privacy Projects initiative) in which security and privacy aspects, so as enhancements of different aspects associated with IoT enablers have been developed.
- AIOTI (Alliance of Internet of Things Initiative) that has appeared as a European catalyst of IoT results and support for pre-normative activities and entrance to some standardization efforts.

IoT research has evolved in different lines and has added new enablers and components to the different proposed architectures, that started with IoT-A, went through AIOTI HLA and its different versions arriving to the AIOTI 3D architecture. The support for the different results and finding depends on having the right partners, which is key in order to be able to develop new components and enlarge the ecosystem with the adequate promotion and support. As underlined by the “Digitising European Industry” communication, if European companies can achieve leadership in IoT platforms, this will stimulate the development of open ecosystems where SMEs, researchers, entrepreneurs, and innovators can develop multiple IoT-based services and applications, improving the competitiveness of the European industry. Open platforms have proved to achieve more easily a critical mass, allowing platform owners to encourage third party developers, suppliers, and users, as well as competitors.

### **IoT-EPI and associated projects**

An IoT Platform is an integrated software that packages together key pieces of functionality to collect, manage, and analyze various forms of IoT data, while monitoring IoT network connectivity and connected devices. IoT platforms offer an efficient way to scale up IoT deployments, by providing a secure way to quickly access, analyze, and act on data. Decoupling data producers and data consumers in a single entity allowing better efficiency in the access, storage, processing, security and privacy.

Open platforms ensure interoperability among IoT systems, which is required to capture 40 percent of the potential economic benefits – in the factory and production environment up to 60 percent of the potential value requires the ability to integrate and analyse data from various IoT systems. Standardization and pre-normative activities are key for the success of an IoT ecosystem and an open environment. Few, consolidated and shared standards remove uncertainty, but too many standards can be worse than none, creating complexity, uncertainty about relevance and access rights for potential innovators, time-consuming interactions between multiple technical communities, and a risk of irrelevance in global markets. The liaisons between communities, conferences, workshops and support from policy makers and regulators is paving the way to reduce number of standards, identify gaps and provide reference architectures.

IoT architectures require interoperability in multiple layers, which means finding the characteristic functionalities of each layer and defining protocols that can be mapped on the ones used in the platforms. A layered approach is the most adequate in order to select the right partners to develop an adequate ecosystem. IoT connectivity is the first step in making the IoT work for your organization. It involves linking to sensors, actuators, Bluetooth, Wi-Fi, near field communication (NFC), 4G, 5G, and other low power short range communications, and sending the data to the organization systems. Networking and mobility are the second layer in order to connect the different gateways and support for access networks. The support for the IoT platform middleware’s will allow to have on board all the IoT alliances and foundations (e.g., FIWARE, UniversAAL IoT, or AIOTI) that are providing and supporting digital platforms. The access to these middleware APIs, will allow the possibility of sharing data and having all of them in the same access point in order to create new applications and services. Another layer in which interoperability and ecosystem growth is needed, is service composition as all the IoT platforms are providing native services. Additionally, API development and aligned ontologies may require collaboration from different parties. The alignment of this layered approach with the needs of cybersecurity has led to different approaches in terms of security architectures specially in devices, access and core networks (physical or virtually defined by software), middleware, semantics and data management. With a clear focus in addressing the requirements of next generation Internet (NGI) and the requirements of 5G/6G, Artificial Intelligence, Data Spaces, Digital Transformation, Cybersecurity and Tactile Internet as a new concept. Placing Human in the middle as a Human Centric approach, may provide a new

ecosystem that will bring the results of long-time research in IoT but will incorporate results from other communities and ecosystems making the results broad and encompassing the adoption of IoT in more verticals and with new capabilities and possibilities.

### **IoT-EPI**

The IoT European Platforms Initiative (IoT-EPI) projects addressed the topic of Internet of Things and Platforms for Connected Smart Objects and delivered an IoT extended into a web of platforms for connected devices and objects that supports smart environments, businesses, services, and persons with dynamic and adaptive configuration capabilities. The specific areas of focus of the research activities were architectures and semantic interoperability, which reliably cover multiple use cases. The successful goal was to deliver dynamically configured infrastructure and integration platforms for connected smart objects covering multiple technologies and multiple intelligent artefacts. The IoT-EPI ecosystem was created with the objective to increase the impact of the IoT-related European research and innovation, including seven European promising projects on IoT platforms: AGILE, BIG IoT, INTER-IoT, VICINITY, SymbIoTe, bIoTope, and TagItSmart. The seven RIA projects were supported by two CSAs UNIFY-IoT and Be-IoT that coordinated different joint actions related to ecosystem building and mainly dissemination and business modelling.

The IoT platforms adoption was driven by factors such as economics that add cloud services and the development of partner ecosystems. In this context, device manufacturers provide built in solutions and models with the IoT SDKs to provide ease of use that allows the use of multiple portals and applications to get the IoT platforms and devices fully configured. The relationship with the service providers is increasingly important with the integration within the IoT suite and the various offerings from service providers. The development of standardisation is accelerating in the area of device discovery to support ability for heterogeneous devices to communicate and interoperate. Standards are key to enable interoperability, driving down costs and stimulating growth. However, standards processes are complex, take a long time to evolve and be adopted, and will still take some time to have mature, stable standards dominating, so suppliers and buyers are having to over-invest in multiple standards.

In this complex environment, the IoT-EPI projects developed interoperability solutions that were addressing different layers in the IoT architecture and offer mechanisms for providing interoperability between different IoT platforms addressing various use cases and applications. The seven projects (i.e., INTER-IoT, AGILE, symbIoTe, BIG-IoT, TAGIT-Smart, VICINITY and bIoTope) provided different approaches and focused on different verticals, enlarging the ecosystem in different directions, and providing the seed for further developments, e.g., IoT-LSP and IoT-ESP.

### **INTER-IoT - Interoperability of Heterogeneous IoT Platforms <sup>68</sup>**

INTER-IoT project aimed at the design, implementation, and experimentation of an open cross-layer framework and associated methodology and tools to enable voluntary interoperability among heterogeneous IoT platforms. The proposal allowed effective and efficient development of adaptive, smart IoT applications and services atop different heterogeneous IoT platforms, spanning single and/or multiple application domains. The project was tested in two application domains: port transportation and logistics and mobile health; additionally, it was validated in a cross-domain use case by means of the creation of an IoT ecosystem.

The project idea was supported because most existing sensor networks and IoT device deployments work and independent entities of homogenous elements that serve a specific purpose and are isolated from “the rest of the world”. In a few cases where heterogeneous elements are integrated, this is done either at device or network level, and focused mostly on unidirectional gathering of information. A multi-layered approach to integrate heterogeneous IoT devices, networks, platforms, services, and data allows heterogeneous elements to cooperate seamlessly to share information, infrastructures, and services as in a homogenous scenario.

Lack of interoperability causes major technological and business issues such as impossibility to plug non-interoperable IoT devices into heterogeneous IoT platforms, impossibility to develop IoT applications exploiting multiple platforms in homogeneous and/or cross domains, slowness of IoT technology introduction at a large-scale, discouragement in adopting IoT technology, increase of costs, scarce reusability of technical solutions, and user dissatisfaction. The main goal of the INTER-IoT project was to comprehensively address

---

<sup>68</sup> <https://inter-iot.eu>

the lack of interoperability in the IoT realm by proposing a full-fledged approach facilitating “voluntary interoperability” at any level of IoT platforms and across any IoT application domain, thus guaranteeing a seamless integration of heterogeneous IoT technology. INTER-IoT aims to provide open interoperability, which delivers on the promise of enabling vendors and developers to interact and interoperate, without interfering with anyone’s ability to compete by delivering a superior product and experience.

In the absence of global IoT standards, the INTER-IoT project supported and made it easy for any company to design IoT devices, smart objects, and/or services and get them to the market quickly, thus creating new IoT interoperable ecosystems. The solution adopted by INTER-IoT included three main products or outcomes: INTER-LAYER, INTER-FW, and INTER-METH. The INTER-IoT approach was use case-driven, implemented, and tested in three realistic large-scale pilots: transportation and logistics in a port environment, mobile health and a cross-domain pilot.

### **AGILE - Adaptive Gateways for dIverse muLtiPle Environments<sup>69</sup>**

AGILE built a modular and adaptive gateway for IoT devices. Modularity at the hardware level can provide support for various wireless and wired IoT networking technologies (e.g., KNX, Z-Wave, ZigBee, Bluetooth Low Energy etc.). AGILE allowed fast prototyping of IoT solutions for various domains (e.g., home automation, environment monitoring, wearables, etc.). At the software level, different components enabled new features: data collection and management on the gateway, intuitive interface for device management, visual workflow editor for creating IoT apps with less coding, and an IoT marketplace for installing IoT apps locally.

The AGILE software environment could autoconfigure and adapt, based on the hardware configuration so that driver installation and configuration could be performed automatically. IoT apps were recommended based on hardware setup, reducing the gateway setup and development time significantly. All AGILE software modules were delivered as 100% Open Source, with the majority of them becoming part of a new Eclipse Foundation IoT Project. The objective was to provide IoT developers and communities with free software components for effective and agile IoT prototyping, and at the same time to establish a community of users and developers, maximizing the adoption of the AGILE Project.

AGILE run five pilots from wearables for self-tracking, and open-air crop and livestock monitoring using drones, to smart retail solutions for enhanced shopping experiences. These pilots demonstrated the applicability of the hardware and software in managing IoT devices and creating applications and sharing data and set the foundations for further commercial exploitation of the Project and innovations. SMEs and Start-ups active in the IoT domain had the opportunity to build products and services on top of AGILE hardware and software.

AGILE open, flexible, and widely usable IoT solution put it at the disposal of industries (start-ups, SMEs, tech companies) and individuals (researchers, makers, entrepreneurs) as a framework that consists of:

- A modular IoT gateway enabling various types of devices (wearables, home appliances, sensors, actuators, etc.) to relate to each other and to the Internet
- Data management and device control maximizing security and privacy, at local- and cloud-level as well as technologies and methodologies to better manage data privacy and ownership in the IoT
- Support of various open and private clouds
- Recommender and visual developer’s interfaces enabling easy creation of applications to manage connected devices and data
- Support of mainstream IoT/M2M protocols, and SDKs from different standardization bodies for device discovery and communication
- Two separate gateway hardware versions: a) the “makers” version, based on the popular RaspberryPi for easy prototyping and b) the “industrial” version for more industrial and production ready environments.

AGILE has become a flagship open-source initiative supported by the Eclipse Foundation and several developers coming from the created ecosystem.

---

<sup>69</sup> <http://www.agile-project-iot.eu>



### **symbIoTe - Symbiosis of Smart Objects Across IoT Environments <sup>70</sup>**

symbIoTe aimed at introducing IoT platform federations, provisioning of domain-specific enablers, sharing of IoT resources and new business models in the IoT landscape. Vertical IoT solutions focus on specific activities of everyday life but are restricted to the ecosystem that can be created around a single platform. Through federations, multiple IoT solutions can collaborate so as to provide cross-domain solutions, and share IoT resources and the respective measurements in locations originally out of their reach.

symbIoTe focused on ecosystem building and for the co-creation of cross-domain solutions it is important that expertise in a certain domain by existing solutions is exploited. For example, if IoT solution providers should wrap and offer their domain-specific platforms in a “Sensing as a Service” manner. This way, important and useful information with respect to a single domain can be provided to third parties, in the form of a domain-specific enabler, typically after some pre-processing and aggregation.

symbIoTe dealt with the increasing complexity of IoT systems and tried to reduce the deployment costs, collocated platforms can choose to be cooperative by opening up the access to their resources to third parties and by implementing generic high-level APIs. In addition, they may choose to collaborate by sharing the common physical resources in a coordinated way. Putting the technical details aside, the federations among IoT solution providers need to be supported by the appropriate business models in order to be viable. symbIoTe builds around a hierarchical IoT stack connecting smart objects and IoT gateways within smart spaces with the Cloud. Smart spaces share the available local resources, while platform services running in the Cloud should enable federations and open up northbound interfaces to third parties. The architecture comprises four layered domains: application domain, cloud domain, smart space domain and device domain. symbIoTe was tested in five use cases: Smart residence, Smart campus, Smart stadium, Smart Mobility and Ecological Routing and Smart yachting.

### **BIG-IoT - Bridging the Interoperability Gap of the IoT <sup>71</sup>**

BIG-IoT aimed to create a broadly accepted professional IoT ecosystems. Several barriers existed and BIG-IoT focused on the data. The reason for these barriers were: (i) that are high market entry barriers for developers and service providers due to a fragmentation of IoT platforms; (ii) developers who want to make use of smart objects hosted by various providers need to negotiate access to their platforms individually and implement specific adapters; and (iii) the efforts to negotiate individual contracts often outweigh the possible gains, platform providers do not see strong incentives to open their platforms to third parties.

The goal of BIG-IoT was to overcome these hurdles by creating marketplaces for service and application providers as well as platform operators. BIG-IoT addressed the interoperability gap by defining a generic, unified Web API for smart object platforms, called the BIG IoT API. The establishment of a marketplace where platform, application, and service providers can monetize their assets will introduce an incentive to grant access to formerly closed systems and lower market entry barriers for developers. With this approach based on the generic BIG IoT API, an IoT ecosystem came to life, as it offered a functionally rich but at the same time easy way to discover, access, control, manage, and secure smart objects. The API was designed in an open community process and the project consortium engaged with current standardization initiatives to receive input and deliver contributions to specifications. The BIG IoT API was implemented by overall eight smart object platforms.

Following an evolutionary and agile approach, the developed technologies were concurrently demonstrated in three regional pilots involving partners with strong relation to public authorities. Under a common theme of “smart mobility and smart road infrastructure”, various use cases within the pilots validated the developed technologies.

### **TAGIT-Smart! - A Smart Tags driven service platform for enabling ecosystems of connected objects <sup>72</sup>**

Leveraging the features of functional codes (such as QR codes printed using functional inks) to change according to the context changes of each tagged product together with wide availability of smart phones that could capture/record/transmit these codes the consortium aims to create context sensors for mass market

<sup>70</sup> <https://www.symbiote-h2020.eu>

<sup>71</sup> <http://big-iot.eu>

<sup>72</sup> <https://www.tagitsmart.eu>



products and convert mass market products into connected mass market products with unique identity that can report on their environment. This opens up possibilities for a whole new range of services to be created and consumed by the user, and for the user. The outcome was the creation of an almost infrastructure-less IoT framework applicable in multiple industry sectors. The overall objective of TagItSmart was to create a set of tools and enabling technologies integrated into a platform with open interfaces enabling users across the value chain to fully exploit the power of condition-dependent functional codes to connect mass market products with the digital world across multiple application sectors.

TagItSmart defined a framework, enabling technologies and the tools required to design and exploit functional codes across multiple application sectors in a secure and reliable manner. The project leveraged clearly identified and well-established catalysts (i.e., functional inks, printed circuit NFC, smartphones pervasiveness and cloud computing) to enable inclusion of any mass market product into the world of connected objects. Functional inks and printed NFCs were used to create functional codes which provided sensing capabilities to the objects they were attached to. Product manufacturers, shopping centres, supply chain providers and other stakeholders from different sectors were able to leverage the framework to produce and deploy these codes according to their needs and the properties they need to observe and track easily and automatically. Functional codes scanners (fixed and provided by existing infrastructure or supported by participatory engagement of consumers) were used to obtain data from functional codes throughout the product lifecycle. The five use cases in which the technology was tested were: Digital Beer, Lifecycle and Consumer Engagement, Brand protection, Supply Chain and Dynamic Pricing, Home Service

### **VICINITY- Open virtual neighbourhood network to connect IoT infrastructures and smart objects**<sup>73</sup>

The VICINITY project built and demonstrated a platform and ecosystem for IoT infrastructures offering “Interoperability as a Service”. The platform was device- and standard-agnostic and relied on a decentralized and user-centric approach. VICINITY retained full control of the ownership and distribution of data across the different IoT domains. VICINITY introduced the concept of virtual neighborhood, where users could share the access to their smart objects without losing the control over them. A virtual neighbourhood was defined as a part of an IoT infrastructure that offers decentralised interoperability and releases the vendor locks that are present in IoT ecosystems. New independent value-added services across IoT domains benefited from the availability of the vast amount of data in semantic formats that are generated by IoT assets.

VICINITY presented a virtual neighbourhood concept. The users were allowed to configure installations and integrate standards according to the preferred services, as well as being able to fully control their desired level of privacy. Data exchange between different devices was handled through the VICINITY open interoperability gateway, which reduced the need for having a technical background in order to exploit to the VICINITY ecosystem. An API allowed for easy development of an adapter to the platform. Once an IoT infrastructure was integrated, its owner could simply manage the access to his/her IoT data and controls using the VICINITY neighbourhood manager (VNM).

Connecting to detected IoT infrastructures was handled by the open VICINITY auto discovery device. The device automatically discovered the smart objects. These devices appeared in a device catalogue and allowed the users to manage access rules for the discovered smart objects. VICINITY was tested in four different use cases: smart energy micro-grid that is enabled by municipal buildings; a Smart Grid ecosystem was combined with an Assisted Living use case; eHealth; and large number of data sources from different domains can be combined in an intelligent parking application

### **bioTope - Building an IoT Open Innovation Ecosystem for Connected Smart Objects**<sup>74</sup>

New IoT applications that leverage ubiquitous connectivity, system interoperability and analytics, are enabling Smart City initiatives all over the world. Although the smart city paradigm paves the way for societal and economic opportunities (e.g., to reduce costs for societies or foster a sustainable economic growth), they also pose architectural and structural issues that must be addressed for businesses to benefit. One of the most critical obstacles has been the vertical silos’ model, which has hampered developers – due to the lack of interoperability and openness – to produce new added value across multiple platforms (data is “siloes” in a unique systems,

<sup>73</sup> <https://vicinity2020.eu/vicinity/>

<sup>74</sup> <https://biotope-project.eu>

clouds, domains, and stays there). Several organizations and standardization fora have understood this critical challenge and started to build up consortia and IoT initiatives to address it.

The Open Group was among the first ones with the IoT Work Group established in 2010. Other initiatives are, for example, the Web of Things initiative at W3C that aims to create open ecosystems based upon open standards, including identification, discovery and interoperation of services across platforms; the Alliance for IoT Innovation (AIOTI) launched by the EU with the aim of strengthening links and building new relationships between the different IoT players (industries, SMEs, start-ups); the Open Platform 3.0™ at The Open Group that focused more on organization applications and practices; the OneM2M global standards initiative that involved eight standards bodies for M2M communications; or still the IEEE IoT initiative. Although most of those initiatives have promoted various types of standards and specific technology enablers, they all shared the same vision about relying as much as possible on open and interoperable standards to foster open ecosystems and unlock the commercial potential of the IoT.

Primary goal of bIoTopen was to enable companies to easily create new IoT systems and rapidly harness available information using advanced Systems-of-Systems (SoS) capabilities for Connected Smart Objects. To this end, bIoTopen took full advantage of messaging standards developed and officially published by The Open Group, notably the Open Messaging Interface (O-MI) and Open Data Format (O-DF) standards. Those standards emerged out of past EU FP6-FP7 projects, where real-life industrial applications required the collection and management of product instance-level information for many domains involving heavy and personal vehicles, household equipment, etc. Based on the needs of those real-life applications, and as no existing standards could be identified that would fulfil those requirements without extensive modification or extensions, the partner consortia specified new IoT interoperability standards.

### IoT-LSP

IoT solutions allow industries to address their specific business needs and implement digital innovation in a sustainable and cost-effective way, for example allowing to develop new services based on IoT – generated data flows and to manage the interaction with customers in real time. The size of investments, security and privacy concerns are the main reasons why users struggle to scale IoT to their mainstream processes. This is why the IoT Programme priorities include proving the business case, demonstrating scalability, and developing secure and trustworthy multi-user platforms. Collaboration between stakeholders across the ecosystem is also a way to respond to the digital capacity and skills gaps suffered by potential users.

Knowledgeable users understand that moving to automation oriented IoT solutions, helping to monitor assets and manage safety can actually improve cost efficiency and security. In addition, quality and productivity improvements are positive drivers of adoption. The IoT LSP Programme has helped the IoT research community to navigate the technology environment, identify priorities and gaps, and define increasingly important reference architectures. Main contributions include for example:

- The collaborative development by LSPs of a 3D Reference Architecture model expanded the reach of architecture specification and aimed at contributing to standardization
- The development of requirements for a new standard for time-critical data links for IoT sensors (partner Ring Advocacy has made a submission for a new wireless interface)
- The LSPs contributions to SAREF (Smart Appliances REference ontology) a modular network of standardized semantic models led by ETSI, which is being extended to IoT application environments such as Smart Cities and Smart Agri-food, contributing to the development of a strong EU standards ecosystem
- The contributions to the ITU Study Group 20 on IoT and Smart Cities, where two standards promoted by the project are under work since 2017: Draft recommendation on Open API for IoT in Smart Cities and the Technical Report on Artificial Intelligence in the IoT and Smart City ecosystem.

The IoT European Large-Scale Pilots Programme has included the innovation consortia that are collaborating to foster the deployment of IoT solutions in Europe through integration of advanced IoT technologies across the value chain, demonstration of multiple IoT applications at scale and in a usage context, and as close as possible to operational conditions. The consortia have been five Innovation Actions (i.e., ACTIVAGE, AUTOPILOT, IoF2020, MONICA and SYNCHRONICITY) and two CSA to support them CREATE-IoT and U4IoT. Regarding the two CSAs that have coordinated different activities between the LSPs by means of IoT-

LSP initiative. CREATE-IoT's aim has been to stimulate collaboration between IoT initiatives, foster the take up of IoT in Europe and support the development and growth of IoT ecosystems based on open technologies and platforms aligning the activities with AIOTI and with contractual PPPs (e.g. Big Data, Factories of the Future, 5G-infrastructure), Joint Technology Initiatives (e.g. ECSEL – Electronic Components and Systems for European Leadership Joint Technology Initiative), European Innovation Partnerships (e.g. on Smart Cities) as well as with other FAs (e.g. on Autonomous transport). While U4IoT that has addressed the Responsible Research and Innovation – Social Sciences and Humanities (RRISSH).

#### **ACTIVAGE - ACTivating InnoVative IoT smart living environments for AGEing well<sup>75</sup>**

ACTIVAGE built the first European interoperable and open IoT ecosystem enabling the deployment, at large scale, of a wide range of Active & Healthy Ageing IoT based solutions and services. To achieve this, ACTIVAGE integrated thousands of devices to collect and analyse older adults' environmental and lifestyle information, identified their needs, and provided customized solutions, ensuring users' data privacy and security.

Europe has been undergoing major socio-economic changes that made the welfare state's foundations teeter; namely, an increased life expectancy and a drop-in birth rate. And the numbers seem to have an upward trend. Projections indicate that the older population (> 65 years) in the European Union will grow from the current 18% up to 28% by 2060. In addition to the above demographic change, the increasing growth of social and health costs jeopardizes the sustainability of the current social and health system models. The ACTIVAGE project took base on these arguments, with the primary objective of developing evidence and bringing to life the positive impact of the technologies and solutions that are based on the IoT in order to improve the quality of life, the health, and the autonomy of older adults. And all this, with the aim to ensure the sustainability of social and health systems in Europe. ACTIVAGE through the AIOTES component and the different measurement and evaluation components achieved the proposed goal, creating an ecosystem of entities that used and will use the developed technologies.

This large-scale pilot actively involved nearly 10,000 older persons across nine deployment sites in seven different European Union countries. It is important to highlight that ACTIVAGE ambition was that end users from the different sites were involved in the piloting of several use cases, in such a way that it was considered a single pilot and not the sum of different pilots with diverged ambitions. This has been thought intentionally to simulate real conditions that will emerge in an IoT-enabled European society sharing a homogenized offering of interoperable services, in order to maximize the adoption and minimize the effects of market fragmentation.

#### **AUTOPILOT - AUTomated driving Progressed by Internet Of Things<sup>76</sup>**

AUTOPILOT developed an IoT connected vehicle platform and IoT architecture based on the existing and forthcoming standards, as well as open source and vendor solutions. The IoT ecosystem has accommodated vehicles, road infrastructure and connected IoT objects, with particular attention to safety critical aspects of automated driving. Automated driving is expected to increase safety, provide more comfort, and create several new business opportunities for mobility services. The market size is expected to grow steadily reaching 50% market penetration by 2035.

There is little doubt that automated vehicles will be part of the IoT revolution. Indeed, connectivity and IoT have the capacity for disruptive impacts on highly and fully automated driving along all value chains towards a global vision of Smart Anything Everywhere. In order to stay competitive, the European automotive industry is investing in connected and automated driving, with cars becoming moving "objects" in an IoT ecosystem and eventually participating in Big Data for Mobility. AUTOPILOT brought IoT into the automotive world to transform connected vehicles into highly and fully automated vehicles. AUTOPILOT developed a range of services combining autonomous driving and IoT, such as car sharing, autonomous valet parking, and better digital maps for autonomous vehicles.

AUTOPILOT IoT-enabled autonomous driving services were tested in real conditions at large-scale pilot sites in the Netherlands, Italy, France, Finland, Spain, and South Korea. The test results allowed multi-criteria evaluations (technical, user, business, legal) of the IoT impact on advancing the level of autonomous driving.

<sup>75</sup> <https://www.activageproject.eu>

<sup>76</sup> <https://autopilot-project.eu>

**IoF2020 - Internet of Food and Farm 2020<sup>77</sup>**

IoF2020 was dedicated to accelerating the uptake of IoT technologies in the European farming and food chains and ultimately strengthening their competitiveness and sustainability, by demonstrating, together with end-users, the use of IoT in 19 use-cases spread throughout Europe, and focusing on 5 areas: dairy, meat, arable crops, fruits, and vegetables. The project built on and leverages the ecosystem of previous key projects (e.g., FIWARE, IoT-A) to foster the end-user acceptance and adoption of IoT Solutions in agriculture. At the heart of the project, 19 use-cases distributed in 5 trials: Arable, Dairy, Fruit, Vegetables and Meat. Under each trial, IoT integrators made the business case for innovative IoT solutions applied to many areas.

A lean multi-actor approach focusing on user acceptance, stakeholder engagement and the development of sustainable business models improved technology and market readiness levels and encouraged end-user adoption. This development was enhanced by an open IoT architecture and infrastructure of reusable components based on existing standards and a security and privacy framework. Anticipating technological developments and emerging challenges for the farming and food industry.

IoF2020 was designed to generate maximum impact right from the outset and in the long run, bringing closer together and integrating the supply and demand sides of IoT technologies in the agrifood sector. IoF2020 has paved the way for data-driven farming, autonomous operations, virtual food chains and personalized nutrition for European citizens.

**MONICA - Management of Networked IoT Wearables – Very Large-Scale Demonstration of Cultural and Societal Applications<sup>78</sup>**

MONICA was a large-scale demonstration of how cities can use existing and new IoT solutions to meet sound, noise, and security challenges at big open-air cultural and sports events, which attract and affect many people. Innovations included the establishment of sound zones at outdoor concerts for noise mitigation as well as security measures improving crowd information and management. Several sound, security and user experience applications were deployed at large events in six European cities, involving more than 100,000 application users in total. The applications were based on the use of IoT-enabled devices such as smart wristbands, video cameras, loudspeakers, smart glasses, airships, and smartphones. The applications offered enhanced monitoring and management of sound levels and crowds as well as value-added functionality for customers, crowds, and citizens. To support the applications, MONICA deployed a cloud based IoT platform, wirelessly connecting and handling the devices, whether fixed, worn or moved around.

MONICA demonstrated how it is possible to securely operate a very dense cloud of different IoT-enabled devices and networks with a low probability of interference. Six pilot sites demonstrated the technology solutions at concerts, festivals, sports events, and city happenings, which attract millions of people. Each of the sites chose several relevant applications that they wish to deploy. Whereas some cities emphasise optimal concert sound and enhanced noise control, and others security and service, all pilots actively involved their end users, engaging more than 10,000 people in the evaluation process. Central to the project was the involvement of multiple stakeholders in the design, deployment, and evaluation of the applications. Additionally, several innovation tools were made available in terms of open data, development kits, entrepreneurship packages and business models.

**SynchroniCity - Delivering an IoT-enabled Digital Single Market for Europe and Beyond<sup>79</sup>**

The SynchroniCity project represented the first attempt to deliver a digital single market for IoT-enabled urban services in Europe and beyond - in 8 European cities and more worldwide - connecting 39 partners from 13 countries over 3 continents. Building upon a mature European knowledge base, derived from initiatives such as OASC, FIWARE, EIP-SCC, FIRE, and including partners with leading roles in standardization bodies, e.g., IETSI, SF-SSCC, ITU, OMA, IETF, SynchroniCity delivered a harmonized ecosystem for IoT-enabled smart city solutions where IoT device manufacturers, system integrators and solution providers innovated. With an already emerging foundation, based on OASC Minimal Interoperability Mechanism (MIMs), SynchroniCity established a reference architecture model for the envisioned IoT-enabled city marketplace with identified

<sup>77</sup> <https://www.iof2020.eu>

<sup>78</sup> <https://www.monica-project.eu>

<sup>79</sup> <https://synchronicity-iot.eu>



interoperability points and interfaces and data models for different verticals. This included tools for co-creation and integration of legacy platforms and IoT devices for urban services and enablers for data discovery, access and licensing lowering the barriers for participation on the market.

SynchroniCity piloted these foundations in the cities together with a set of citizen-centred services in three high-impact areas, showing the value to cities, businesses and citizens involved, linked directly to the global market. With a running start, SynchroniCity served as frontrunner initiative to inspire others to join the established ecosystem and contribute to the emerging marketplace and globally, to establish a momentum and critical mass for a strong European presence in a global digital single market of IoT-enabled urban services.

### IoT-ESP

The IoT technology and market landscape will become increasingly complex in the longer term i.e., 10+ years from now, especially after IoT technologies will have proven their full potential in business-critical and privacy-sensitive scenarios. An important shift is expected to happen as technology evolutions will allow to safely employ IoT systems in scenarios involving actuation and characterized by stricter requirements in terms of dependability, security, privacy and safety constraints. Attracted by the trend, several organizations have started studying how to employ IoT systems also to support tasks involving actuation and control in business-critical conditions, resulting in a demand for more dependable and "smart" IoT systems. In order to turn such vision in reality, many issues must still be faced. The European IoT Security and Privacy Projects initiative (IoT-ESP) has advanced concepts for end-to-end security in highly distributed, heterogeneous, and dynamic IoT environments. The approaches presented by the eight related projects have been holistic and include identification and authentication, data protection and prevention against cyber-attacks at the device and system levels. The projects present architectures, concepts, methods, and tools for open IoT platforms integrating evolving sensing, actuating, energy harvesting, networking, and interface technologies. Platforms should provide connectivity and intelligence, actuation and control features, linkage to modular and ad-hoc cloud services. The IoT platforms used are compatible with existing international developments addressing object identity management, discovery services, virtualisation of objects, devices, and infrastructures and trusted IoT approaches.

Adequate security and privacy are key to ensure trust and wide uptake of IoT solutions. The IoT-ESP projects cluster has researched and proposed new solutions for security and privacy by design and by default in Internet of Things. The IoT-ESP projects have been: (i) Smart End-to-end Massive IoT Interoperability, Connectivity and Security (SEMioTICS); (ii) Trustworthy and Smart Actuation in IoT systems (ENACT); (iii) Secure and Safe Internet of Things (SerIoT); (iv) Secure Open Federation for Internet Everywhere (SOFIE); (v) Predictive Security for IoT Platforms and Networks of Smart Objects (SecureIoT); (vi) IoT-Crawler; and (vii) Cognitive Heterogeneous Architecture for Industrial IoT (CHARIOT). The projects have explored how to enhance overall security and deploy new approaches for data privacy such as Distributed Ledger Technology/Blockchains. Concepts that are directly linked with NGI and NGIoT initiatives and enlarges the IoT ecosystem in a new direction covering some new features of the architectures and association with other research communities:

- Heterogeneity and (lack of) interoperability
- Difficulty of implementing "Smart Behaviors" in open collaboration context.
- Security and safety
- Enforcement of Privacy and Data Ownership policies
- Business models colliding with long-term resilience and survivability of IoT services
- Market Fragmentation and incumbency of large players

### Smart End-to-end Massive IoT Interoperability, Connectivity and Security (SEMioTICS)<sup>80</sup>

SEMioTICS aims to develop a pattern-driven framework, built upon existing IoT platforms, to enable and guarantee secure and dependable actuation and semi-autonomic behaviour in IoT/IIoT applications. Patterns will encode proven dependencies between security, privacy, dependability, and interoperability (SPDI) properties of individual smart objects and corresponding properties of orchestrations involving them. The SEMioTICS framework will support cross-layer intelligent dynamic adaptation, including heterogeneous smart

<sup>80</sup> <https://www.semiotics-project.eu>



objects, networks, and clouds, addressing effective adaptation and autonomic behaviour at field (edge) and infrastructure (backend) layers based on intelligent analysis and learning. To address the complexity and scalability needs within horizontal and vertical domains, SEMioTICS will develop and integrate smart programmable networking and semantic interoperability mechanisms. The practicality of the above approach will be validated using three diverse usage scenarios in the areas of renewable energy (addressing IIoT), healthcare (focusing on human centric IoT), and smart sensing (covering both IIoT and IoT); and will be offered through an open Application Programming Interface (API).

The main goal of the SEMioTICS project is to develop a pattern-driven framework, built upon existing IoT platforms. The proposed framework will enable and guarantee the secure and dependable actuation and semiautomatic behaviour in IoT/IIoT applications. Specifically, the SEMioTICS vision in delivering smart, secure, scalable, heterogeneous network and data driven IoT is based on two key features:

- **Pattern-driven approach:** Patterns are re-usable solutions to common problems and building blocks to architectures. In SEMioTICS, patterns encode proven dependencies between security, privacy, dependability and interoperability (SPDI) properties of individual smart objects and corresponding properties of orchestrations (composition) involving them. The encoding of such dependencies enables: (i) the verification that a smart object orchestration satisfies certain SPDI properties, and (ii) the generation (and adaptation) of orchestrations in ways that are guaranteed to satisfy required SPDI properties. The SEMioTICS approach to patterns is inspired from similar pattern-based approaches used in service-oriented systems, cyber physical systems, and networks.
- **Multi-layered Embedded Intelligence:** Effective adaptation and auto-nomic behaviour at field (edge) and infrastructure (backend) layers depends critically on intelligent analysis and learning the circumstances where adaptation actions did not work as expected. Intelligent analysis is needed locally for semi-autonomous, prompt reaction, but considering IoT smart objects limited resources (thus requiring specialized lightweight algorithms). It should also be possible to fuse local intelligence to enable and enhance analysis and intelligent behaviour at higher levels (e.g., using results of local analysis of "thing events" to globally predict and anticipate failure rates).

SEMioTICS will target three IoT application scenarios: two verticals in the areas of energy and health care and one horizontal in the areas of intelligent sensing. These scenarios have been selected since they involve: (a) different and heterogeneous types of smart objects (i.e., sensors, smart devices, actuators) and software components; (b) different vertical and horizontal IoT platforms; and (c) different types of SPDI requirements. Due to these dimensions of variability, our scenarios provide comprehensive coverage of technical issues, which should be accounted for in developing the SEMioTICS approach and infrastructure.

### **ENACT - Trustworthy and Smart Actuation in IoT systems<sup>81</sup>**

Until now, IoT system innovations have been mainly concerned with sensors, device management and connectivity, with the mission to gather data for processing and analysis in the cloud in order to aggregate information and knowledge. This approach has conveyed significant added value in many application domains; however, it does not unleash the full potential of the IoT. The next generation IoT systems need to perform distributed processing and coordinated behaviour across IoT, edge and cloud infra-structures, manage the closed loop from sensing to actuation, and cope with vast heterogeneity, scalability, and dynamicity of IoT systems and their environments. Moreover, the function and correctness of such systems has a range of criticality from business critical to safety critical. Thus, aspects related to trustworthiness such as security, privacy, resilience, and robustness, are challenging aspects of paramount importance. Therefore, the next generation of IoT systems must be trustworthy above all else. In ENACT, they are called trustworthy smart IoT systems, or for short, trustworthy SIS.

Developing and managing the next generation trustworthy SIS to operate in the midst of the unpredictable physical world represents daunting challenges. Challenges, for example, that include that such systems always work within safe operational boundaries by controlling the impact that actuators have on the physical world and managing conflicting actuation requests. Moreover, the ability of these systems to continuously evolve and

---

<sup>81</sup> <https://enact-project.eu>

adapt to their changing environments are essential to ensure and increase their trustworthiness, quality, and user experience. DevOps is a philosophy and practices that covers all the steps from concept to delivery of a software product. In ENACT, DevOps advocates for a set of software engineering best practices and tools, to ensure Quality of Service while continuously evolving complex systems, foster agility, rapid innovation cycles, and ease of use. DevOps has been widely adopted in the software industry. However, there is no systematic DevOps support for trustworthy smart IoT systems today. The aim of ENACT is to enable DevOps in the domain of trustworthy smart IoT systems.

DevOps seeks to decrease the gap between a product design and its operation by introducing software design and development practices and approaches to the operation domain and vice versa. In the core of DevOps there are continuous processes and automation supported by different tools at various stages of the product life cycle. In particular, the ENACT DevOps Framework will meet the challenges below and support the DevOps practices during the development and operation of trustworthy smart IoT systems. ENACT will provide innovations and enablers that will feature trustworthy IoT systems built by implementing the seven stages of the process. Three use cases from the Intelligent Transport Systems (Rail), eHealth and Smart Building application domains will guide, validate, and demonstrate the ENACT research.

### **SerIoT - Secure and Safe Internet of Things<sup>82</sup>**

SerIoT aims to conduct research for the delivery of a secure, open, scalable, and trusted IoT architecture. The solution will be implemented and tested as a complete, generic solution to create and manage large scale IoT environment operating across IoT platforms and paying attention on security problems.

A decentralized approach, based on peer to peer, overlay communication is proposed. SerIoT will optimize the security of IoT platforms in a cross-layered manner. The concept of Software Defined Networks (SDN) is used and SDN controllers are organized in hierarchical structure. The objectives of SerIoT include to provide the prototype implementation of a self-cognitive, SDN based core network, easily configurable to adapt to any IoT platform, including advanced analytics modules, self-cognitive honeypots, and secure routers. The solution will be supported by appropriate technologies such as Decision Support System (DSS) supplementing controller's functionality. The DSS will be able to detect the potential threats and abnormalities. The system will be supplemented with comprehensive and intuitive visual analytics and mitigation strategies that will be used according to the detected threats. It will be validated in the final phase of the project through representative use cases scenarios, involving heterogeneous EU wide SerIoT network system. The innovatory approach used in SerIoT network will be using Cognitive Packets for gathering network data on QoS, security state and energy usage, and Cognitive Packet Network routing engine, based on Random Neural Networks (RNN). The concept is a combination of neural networks-based routing and source routing. It was successfully applied in SDN network, and in the SerIoT project will be extended both in terms of data used as input for routing engine and of scale of the networks. Security data will be used as input for learning of RNN, along with QoS and energy usage data, to allow finding secure and efficient routes for every SDN flow.

SerIoT aims to design and to deploy four innovative use cases arising from three significant for the global economy domains where the use of IoT is rapidly increasing: (i) Smart Cities domain will be covered by two ambitious use cases where Surveillance and Intelligent Transportation IoT networks will be evaluated, (ii) Flexible Manufacturing domain with the detection of physical attacks on wireless sensor networks, and finally (iii) a novel Food Chain Scenario will be exploited demonstrating mobility security issues. Each of the use cases considers one or several scenarios. A scenario is intended to describe and specify the system behaviour according to a specific situation, or in other words to describe the situation in which a specific system should work and how the system works and interacts with the different users.

### **SOFIE - Secure Open Federation for Internet Everywhere<sup>83</sup>**

The main goal of the SOFIE project is to enable diversified applications from various application areas to utilise heterogeneous IoT platforms and autonomous things across technological, organisational, and administrative borders in an open and secure manner, making reuse of existing infrastructure and data easy. SOFIE is guided by the: needs of three pilot use cases with diverse business requirements: food supply-chain, mixed reality

---

<sup>82</sup> <https://seriot-project.eu>

<sup>83</sup> <https://www.sofie-iot.eu>

mobile gaming, and energy markets. Furthermore, we will explore the synergies among these areas, building a foundation for cross-application-area use of existing IoT platforms and data.

SOFIE will design, implement, and pilot a systematic, open, and secure way to establish new business platforms that utilise existing IoT platforms and distributed ledgers. With "openness", we mean flexible and administratively open business platforms, as well as technically decentralised federation to enable the interoperability of different IoT platforms, ledgers, and autonomous devices. SOFIE combines several IoT platforms and distributed ledgers into a federated IoT platform supporting the reuse of existing IoT infrastructure and data by various applications and businesses. SOFIE achieves decentralization of business platforms through the use of DLTs. Since the properties of various DLTs, such as scalability, throughput, resilience, and openness, are significantly different, SOFIE relies on using multiple different DLTs in parallel. To allow transactions to be recorded into multiple blockchains or other ledgers, SOFIE will design and implement the inter-ledger transaction layer. We will build upon existing leading-edge work, including the W3C-associated Inter-ledger Protocol (ILP), applying the results to the IoT domain, and developing them further. The transactions will be implemented as multi-stage smart contracts whose resolution depends on the transactions being correctly recorded in all the participating ledgers, but without requiring that all the ledgers support smart contracts.

The SOFIE federation approach is designed to be technology-agnostic, allowing systems with different APIs and data formats to interoperate to the extent allowed by the applicable security policies. Some of the existing IoT platforms already support interoperability across different protocols and standards. Examples of this include FIWARE through its IoT adapters, such as the already existing LWM2M and oneM2M adapters, and W3C WoT, where the IoT servient concept supports both proprietary APIs and various protocol adapters. While most of the data will reside within existing IoT systems, a key aspect of SOFIE is the so-called smart contract, available in some blockchains, such as Ethereum. From the SOFIE point of view, a smart contract is simply a computer program and its associated computational state that "lives" in a blockchain.

The SOFIE security architecture provides end-to-end security (confidentiality and integrity), identification, authentication, and authorization, and supports users' privacy and control over their data. Most existing solutions already provide decent end-to-end security within the system and system-specific authentication. Therefore, SOFIE concentrates on innovating in the areas of data sovereignty, privacy and federated key management, authentication, and authorization.

The SOFIE federation approach will help make the existing siloed IoT platforms interoperable, enabling cross-platform applications and reuse of data in a secure and scalable manner. SOFIE will offer data sovereignty in GDPR compliant way, giving users more control of their data. Through the usage of distributed ledgers, SOFIE will promote open business platforms, allowing creation of new kinds of decentralised open marketplaces, which no single entity - public or private - can technically control and thus exercise sole pricing power over them. This in turn will lower the barrier of entry for small businesses and individuals. The SOFIE federation framework will be released as open-source and SOFIE partners have: the capacity to deliver and boost the penetration of SOFIE offerings in the market and relevant standardization bodies.

### **SecureIoT - Predictive Security for IoT Platforms and Networks of Smart Objects**<sup>84</sup>

SecureIoT is motivated by the need to support cyber-security in scenarios involving cross-platform interactions and interactions across networks of smart objects (i.e., objects with semi-autonomous behaviour and embedded intelligence), which require more dynamic, scalable, decentralized and intelligent IoT security mechanisms. To this end, it introduces a multi-layer, data-driven security architecture, which collects and processes information from the field, edge, and cloud layers of an IoT system, in order to identify security threats at all these layers and accordingly to drive notifications and early preparedness to confront them. Furthermore, SecureIoT foresees cross-layer coordination mechanisms and will employ advanced analytics towards a holistic and intelligent approach that will predict and anticipate secure incident in order to timely confront them. Also, SecureIoT introduces a range of security interoperability mechanisms in order to support cross-vertical and cross-platform cyber-security scenarios. The SecureIoT architecture serves as basis for the provision of security services to IoT developers, deployers and platform providers, including a risk assessment, a compliance auditing, and a secure programming support service.

---

<sup>84</sup> <https://secureiot.eu>

The architecture provides placeholders for predictive IoT security mechanisms, which can be contributed by different security experts in order to protect IoT infrastructures and services. In the scope of SecureIoT the partners will specify and implement such mechanisms in the areas of security monitoring and predictive analysis, which will serve as a basis for supporting the project's use cases. Nevertheless, the project's architecture is more general and therefore able to accommodate additional algorithms and building blocks. The architecture complies with the reference architectures specified by the Industrial Internet Consortium (TIC) and the OpenFog consortium, as it specifies: (i) The field level, where IoT devices (including smart objects) reside; (ii) The fog/edge level, which controls multiple devices close to the edge of the network. Note that the fog/edge level might be the first security layer in an IoT application, especially when resource constrained devices are deployed; (iii) The enterprise and platform levels, which reside at the core and where application and platform level security measures are applicable. SecureIoT is destined to support cybersecurity scenarios in both consumer and industrial settings. In order to strengthen the industrial relevance of the project's architecture, the project will provide a mapping of the main building blocks of the SecureIoT architecture to the Reference Architecture Model Industry4.0 (RAMI 4.0).

SecureIoT is a first of a kind attempt to introduce a standards-based architecture for end-to-end IoT security. The project's architecture is aligned to recent standards for industrial IoT security, including standards of the Industrial Internet Consortium and the OpenFog consortium. It makes provisions for collecting and analysing data from all layers of an IoT platform, while at the same time catering from cross platform and cross layer security analysis. Moreover, the SecureIoT architecture provides the means for defining and executing security actions at specific PEPs, as a means of enforcing policies and instigating mitigation actions. Based on this architecture, the project will implement risk assessment, compliance and the programming support services. The project's architecture and services will be validated in three use cases: Industrial plants' security, socially assistive robots and connected cars.

### **IoTCrawler - Search Engines for Browsing the Internet of Things<sup>85</sup>**

Efficient and secure access to Big IoT Data will be a pivotal factor for the prosperity of European industry and society. However, today data and service discovery, search, and access methods and solutions for the IoT are in their infancy, like Web search in its early days. IoT search is different from Web search because of dynamicity and pervasiveness of the resources in the net-work. Current methods are more suited for fewer (hundreds to millions), static or stored data and services resources. There is yet no adaptable and dynamic solution for effective integration of distributed and heterogeneous IoT contents and support of data reuse in compliance with security and privacy needs, thereby enabling a true digital single market. Previous reports show that a large part of the developers' time is spent on integration. In general, the following issues limit the adoption of dynamic IoT-based applications:

- The heterogeneity of various data sources hinders the uptake of innovative cross-domain applications
- The large amount of raw data without intrinsic explanation remains meaningless in the context of other application domains
- Missing security and neglected privacy present the major concern in most domains and are a challenge for constrained IoT resources
- The large-scale, distributed, and dynamic nature of IoT resources requires new methods for crawling, discovery, indexing, physical location identification and ranking
- IoT applications require new search engines, such as bots that automatically initiate search based on user's context. This requires machine intelligence
- The complexity involved in discovery, search, and access methods makes the development of new IoT enabled applications a complex task

The project aims to create scalable and flexible IoT resource discovery by using meta-data and resource descriptions in a dynamic data model. This means, for example, that if a user is interested in measuring temperature in a certain location, the result (e.g., list of sensors) should only contain sensors that can measure temperature, but the user may accept sensors that closely fulfil her/his application requirements even though all

---

<sup>85</sup> <https://iotcrawler.eu>



other characteristics may not be favourable (e.g., cost of acquisition may be high and sensor response time may be slow). For this reason, the system should understand the user priorities, which are often machine-initiated queries and search requests and provide the results accordingly by using adaptive and dynamic techniques. IoTcrawler provides novel approaches to support an IoT framework of interoperable systems including security and privacy-aware mechanisms, and offers new methods for discovery, crawling, indexing and search of dynamic IoT resources. It supports and enable machine-initiated knowledge-based search in the IoT world. IoTcrawler is currently evaluating its technologies in four real world use-cases: Smart Cities, Social IoT, Smart Energy, and Industry 4.0.

### **CHARIOT - Cognitive Heterogeneous Architecture for Industrial IoT<sup>86</sup>**

Recently, cloud computing as well as Internet of Things (IoT) technologies are rapidly advancing under the concept of future internet. Numerous IoT systems and devices are designed and implemented following industrial domain requirements but most of the times not considering recent risk relating to openness, scalability, interoperability as well as application independence, leading to a series of new risks relating to information security and privacy, data protection and safety. As a result, securing data, objects, networks, infrastructure, systems, and people under IoT is expected to have a prominent role in the research and standardization activities over the next several years. CHARIOT EC co-funded, research project, clearly recognises and replies to this challenge, identifying needs and risks and implementing a next generation cognitive IoT platform that can enable the creation of intelligent IoT applications with intelligent shielding and supervision of privacy, cyber-security and safety threats, as well as complement existing IoT systems in non-intrusive ways and yet help guarantee robust security by placing devices and hardware as the root of trust. CHARIOT provides a design method and cognitive computing platform supporting a unified approach towards Privacy, Security and Safety (PSS) of IoT Systems including the following innovations summarised below:

- A Privacy and security protection method building on state-of-the-art Public Key Infrastructure (PKI) technologies to enable the coupling of a pre-programmed private key deployed to IoT devices with a corresponding private key on a Blockchain system. This includes the implementation of security services utilising a cryptography-based approach and IoT security profiles all integrated to the CHARIOT platform
- A Blockchain ledger in which categories of IoT physical, operational, and functional changes are both recorded and affirmed/approved by the various run-time engines of the CHARIOT ecosystem while leveraging existing blockchain solutions in innovative ways
- Fog-based decentralised infrastructures for Firmware Security integrity checking leveraging Blockchain ledgers to enhance physical, operational, and functional security of IoT systems, including actuation and deactivation
- An accompanying IoT Safety Supervision Engine providing a novel solution to the challenges of securing IoT data, devices, and functionality in new and existing industry-specific safety critical systems
- A Cognitive System and Method with accompanying supervision, analytics and prediction models enabling high security and integrity of Industrials IoT
- New methods and tools for static code analysis of IoT devices, resulting in more efficient secure and safer IoT software development

CHARIOT is closely following a business and industrially driven approach to align the developed technologies and outcomes to actual industrial needs in the fields of transport, logistics etc and in general domains of IoT applications. With this vision, CHARIOT, will apply its outputs and recent developments to three living labs in order to demonstrate its realistic and compelling heterogeneous solutions through industry reference implementations at representative scale, with the underlying goal of demonstrating that Secure, Privacy Mediated and Safety IoT imperatives are collectively met, in turn delivering a key stepping-stone to the EU's roadmap for the next generation IoT platforms and services. The actual living labs will be implemented in the industrial framework of TRENITALIA (rail), Athens International Airport (transport) and IBM Ireland (smart buildings).

---

<sup>86</sup> <https://www.chariotproject.eu>



### **BRAIN-IoT - model-Based fRamework for dependable sensing and Actuation in INtelligent decentralized IoT systems<sup>87</sup>**

The BRAIN-IoT project has focused on complex scenarios, where actuation and control are cooperatively supported by populations of heterogeneous IoT systems. In such a complex context, many initiatives fall into the temptation of developing new IoT platforms, protocols, models, or tools aiming to deliver the ultimate solution that will solve all the IoT challenges and become "the" reference IoT platform or standard. Instead, usually they result in the creation of "yet-another" IoT solution or standard. BRAIN-IoT will establish the principle that future IoT applications should never be supported by a single, unique, irreplaceable IoT platform. Rather future IoT services should exist within a federated/evolving environment that not only leverages current Industry Standards but is also capable of adapting to embrace future unforeseen industry developments. BRAIN-IoT aims at demonstrating that the lack of a single IoT standard and platform, which is generally recognized as the most notable weakness of IoT, can be turned into a strength and a guarantee for market competitiveness and user protection - if the proper framework for IoT security and privacy is in place.

The breakthrough targeted by BRAIN-IoT is to establish a practical framework and methodology suitable to enable small cooperative behaviour in fully decentralized, composable and dynamic federations of heterogeneous IoT platforms. BRAIN-IoT builds on mode l-based approaches and open industry standards and aims at supporting rapid development and deployment of applications and services in professional usage scenarios characterized by strict constraints in terms of dependability, safety, security, and privacy. The overall BRAIN-IoT concept follows the reference model proposed by Recommendation ITU-T Y.2060. BRAIN-IoT looks at heterogeneous IoT scenarios where instances of IoT architectures can be built dynamically combining and federating a distributed set of IoT services, IoT platforms and other enabling functionalities made available in marketplaces and accessible by means of open and standard IoT APIs and protocols.

At the bottom of the conceptual architecture, the IoT Devices and Gate-ways layer represents all physical world IoT devices with sensing or actuating capabilities, computing devices and includes complex subsystems such as autonomous robots and critical control devices. It is worth observing that BRAIN-IoT specifically aims to support the integration into an IoT environment of devices and subsystems with actuation features that could possibly give rise to mixed-criticality situations and require the implementation of distributed processing approaches. The BRAIN-IoT Management capabilities includes all the features needed to support the envisioned fully decentralized scenario dynamically integrating heterogeneous IoT Devices and Gateways as well as IoT Services. The overall depicted concept addresses use cases from IoT applications in two usage scenarios namely Service Robotics and Critical Infrastructure Management, which provide the suitable setting to reflect future challenges in terms of dependability, smart behaviour, security, and privacy/data ownership management.

### **NGIoT projects**

Internet of Things (IoT) technologies and applications are bringing fundamental changes to all sectors of society and economy and constitute an essential element of the Next Generation Internet (NGI). The challenge is to leverage EU technological strength to develop the next generation of IoT devices and systems which leverage progress in enabling technologies such as 5G, cyber-security, distributed computing, artificial intelligence (AI), Augmented Reality and tactile internet. In addition, it is important to build and sustain a competitive ecosystem of European technology and system providers in IoT as well as ensuring end-user trust, adequate security, and privacy by design. These projects aim at providing reference implementations in terms of a dynamically configured infrastructure and integration schemes for smart devices into self-adaptive, robust, safe, intuitive, secure, and interconnected smart network and service platforms. Reference implementations should include proof-of-concept, demonstrations, and validation, driven by realistic use cases with advanced needs in areas such as wearables, transportation, agriculture homes, health, energy, and manufacturing. The project will be coordinated by the EU-IoT CSA in certain common aspects of the activity.

### **ASSIST-IoT - Architecture for Scalable, Self-\*, human-centric, Intelligent, Secure, and Tactile next generation IoT<sup>88</sup>**

Growth of volume of unstructured data, sent by IoT devices, exceeds that of structured data, and as data grows in size and heterogeneity, issues of scalability and interoperability become a rising concern. ASSIST-IoT will

<sup>87</sup> <http://www.brain-iot.eu>

<sup>88</sup> <https://assist-iot.eu/>

provide an innovative reference architecture, envisioned as a decentralized ecosystem, where intelligence is distributed among nodes by implementing AI/ML close to data generation and actuation, and hyper connecting nodes over software-based smart network. Smart network will be realized by means of virtualized functions, with clear separation of control and data planes, facilitating efficient infrastructure programmability. The proposed approach is focused on the edge-fog-cloud continuum model, so data processing takes place in the appropriate location within the IoT ecosystem, as close as possible to sensing/actuating.

The multiplane reference architecture based on decentralized P2P topology of ASSIST-IoT is enabled by horizontal and vertical components. The horizontal technological components support NGI paradigm, Tactile Internet, and human-centric applications. Cross-plane enablers provide different capabilities to improve modularity and adaptability in environments with heterogeneous data sources. The architecture will support continuous integration and long-term sustainability of domain-agnostic, interoperable, self-\* capable, intelligent, distributed, scalable, secure, and trustworthy IoT ecosystems. ASSIST-IoT will be supported by several pillars: (i) innovative IoT architecture, to adapt to the NGI paradigm, with three dimensional approach, including intelligence, security and privacy by design, supporting decentralized collaborative decision-making; (ii) moving from semantic interoperability to semantically-enabled cross-platform, cross-domain data transactions, within decentralized governance, DLT-anchoring transaction security, privacy and trust; (iii) development and integration of innovative devices, supporting context-aware computing, to enable effective decision making close to events; (iv) introduction of self-\* mechanisms, supporting self-awareness and (semi-)autonomous behaviors across IoT deployments, and (v) Tactile Internet support for latency applications, like AR/VR/MR, and human-centric interaction with IoT components. Results of the action will provide foundation for a comprehensive practice-based methodology, for future designers and implementers of smart IoT ecosystems.

Moreover, the action will follow a DevSecOps methodology with short iterative cycles of work, with highly parallel streams of activities. Rapid and frequent development cycles to ensure the integration of security, privacy, and trust, by design, in all aspects of the envisioned ecosystems.

ASSIST-IoT aims at achieving measured impacts, with contribution to:

- Human-centric IoT evolution
- Emerging or future standards and pre-normative activities
- Evolution of NGIoT infrastructures and novel, future semi-autonomous IoT applications
- Disruptive business models
- Security and privacy mobilization
- Maintain an active community of all relevant IoT stakeholders

Finally, to validate research results, and developed solutions, and to ensure their wide applicability, extended pilot deployments with strong end-user participation will take place in:

- Port automation. Evolve from the traditional centralized platform based IoT deployment to a decentralized Edge approach.
- Smart safety of workers. Increase OSH at the Dynamic environment of a busy construction site.
- Cohesive vehicle monitoring and diagnostics. Accelerate the development process and increase monitoring capabilities.

Each pilot will include different scenarios, in which different technological pillars and enablers will be executed and validated, some preliminary KPIs are provided from the perspective of the stakeholders involved. Moreover, experiences from pilots will be used to improve action outcomes (feedback-loop), guaranteeing quality and broad range applicability of results.

### **ingenIOUS - Next-GENERation IoT sOolutions for the Universal Supply chain<sup>89</sup>**

The appearance of IoT is transforming every sector subject to be digitalized. After a period of evaluation of the use of IoT, companies are now moving to complete digitalization of their supply chains. During the last decades, supply chains have become huge networks of heterogeneous organizations involved in the manufacture and

---

<sup>89</sup> <https://ingenious-iot.eu/web/>

delivery of products to end users. Supply chains of the future are in for a big change, thanks to the many new technologies such as 5G, big data, blockchains, virtual reality and artificial intelligence. The EU-funded iNGENIOUS (Next-GENeration IoT sOlutions for the Universal Supply chain) project will design the next generation of internet of things (IoT) technology to add digital value to future supply chains. It will also propose technical and business enablers to build a complete platform for supply chain management. Formed by 21 partners from 8 countries, including telecommunications vendors and manufacturers, logistic partners, universities, research institutes and high-tech small and medium-sized enterprises, the project will address interoperability between IoT and blockchain platforms for transport.

iNGENIOUS will exploit some of the most innovative and emerging technologies in line with the standardised trend, contributing to the Next-Generation IoT (NG-IoT) and proposing technical and business enablers to build a complete platform for supply chain management. In order to improve data handling and to support highly differentiated demands from several stakeholders in the same physical infrastructure, three key technology enablers such as Edge Computing, Big Data with Artificial Intelligence, and Distributed Ledger Technologies, also known as blockchains, will need to complement the native 5G-IoT solution. Innovative 5G systems at both New Radio (NR) and 5G Core (5GC) enable the enhanced Mobile Broadband (eMBB) and Ultra-reliable and Low-latency Communications (URLLC) capabilities, with special focus on supply chain use cases. A native 5G-IoT solution is proposed to provide service operations beyond terrestrial deployments with minimum battery usage, guarantee the ultra-reliable and low-latency communication requirements needed at industrial environments, or enable the use of high-quality video delivery with surveillance cameras.

iNGENIOUS embraces the 5G Infrastructure Association (5G IA) and Alliance for Internet of Things Innovation (AIoTI) vision for empowering smart manufacturing and smart mobility verticals. The iNGENIOUS network layer brings new smart 5G-based IoT functionalities, federated Multi-Access Edge Computing (MEC) nodes and smart orchestration, needed for enabling the projected real-time capable use cases of the supply chain. Security and data management are fully recognized as important features in the project. iNGENIOUS will create a holistic security architecture for next-generation IoT built on neuromorphic sensors with security governed by Artificial Intelligence (AI) algorithms and tile-based hardware architectures based on security by design and isolation by default. In the application layer, iNGENIOUS new AI mechanisms will allow more precise predictions than conventional systems. Project outcomes will be validated into 4 large-scale Proof of Concept demonstration, covering 1 factory, 2 ports, and 1 ship, encompassing 6 use cases.

### **IntellIoT - Intelligent, distributed, human-centered and trustworthy IoT environments<sup>90</sup>**

The traditional cloud centric IoT has clear limitations, e.g., unreliable connectivity, privacy concerns, or high round-trip times. IntellIoT overcomes these challenges in order to enable NG IoT applications. The initiative aims to facilitate a competitive ecosystem and to strengthen the European market in finding deep-tech solutions. Enabling technologies such as 5G, cybersecurity, distributed technology, Augmented Reality and tactile internet, the project champions end-user trust, adequate security and privacy by design.

IntellIoT's objectives aim at developing a framework for intelligent IoT environments that execute semi-autonomous IoT applications, which evolve by keeping the human-in-the-loop as an integral part of the system. Such intelligent IoT environments enable a suite of novel use cases. IntellIoT focuses on: Agriculture, where a tractor is semi-autonomously operated in conjunction with drones. Healthcare, where patients are monitored by sensors to receive advice and interventions from virtual advisors. Manufacturing, where highly automated plants are shared by multiple tenants who utilize machinery from third-party vendors. In all cases a human expert plays a key role in controlling and teaching the AI-enabled systems.

The following 3 key features of IntellIoT's approach are highly relevant for the work programme as they address the call's challenges:

- Human-defined autonomy is established through distributed AI running on intelligent IoT devices under resource constraints, while users teach and refine the AI via tactile interaction (with AR/VR).
- De-centralised, semi-autonomous IoT applications are enabled by self-aware agents of a hypermedia-based multi-agent system, defining a novel architecture for the NG IoT. It copes with interoperability by relying on W3C WoT standards and enabling automatic resolution of incompatibility constraints.

---

<sup>90</sup> <http://intelliott.eu>

- An efficient, reliable computation & communication infrastructure is powered by 5G and dynamically manages and optimizes the usage of network and compute resources in a closed loop. Integrated security assurance mechanisms provide trust and DLTs are made accessible under resource constraints to enable smart contracts and show transparency of performed actions.

In the upcoming 3 years, IntellIoT will also support SMEs and start-ups in Europe with funding and access to technology per pilot projects executed in collaboration with the IntellIoT consortia partners.

### **IoT-NGIN - Next Generation IoT as part of Next Generation Internet<sup>91</sup>**

Internet of Things (IoT) is one of the next big concepts to support societal changes and economic growth, being one of the fastest growing ICT segments. A specific challenge is to leverage existing technology strengths to develop solutions that sustain the European industry and values. To address this, IoT-NGIN introduces novel research and innovation concepts, to establish itself as the “IoT Engine” that will fuel the Next Generation of IoT as a part of the European Next Generation Internet. First, IoT-NGIN uncovers a pattern based meta-architecture that encompasses evolving, legacy, and future IoT architectures. Second, it optimizes IoT/M2M and 5G/MCM communications, including using secure-by-design micro-services to extend the edge cloud paradigm. Thirdly, it enables user and self-aware, autonomous IoT systems through privacy-preserving federated ML and ambient intelligence, with AR support for humans. Finally, IoT-NGIN research towards distributed IoT cybersecurity and privacy, for example, using Self-Sovereign Identities and interconnected DLTs to implement Meta-Level Digital Twins.

IoT-NGIN will be validated via more than 30 types of heterogeneous IoT devices, ranging from tiny resource constrained IoT sensors to intelligent, autonomous buses, drones, and robots. Beyond partners exploitation plans, to maximize impact and sustainability, IoT-NGIN will push all results via alliances, clusters, SDOs and DIHs, including FIWARE, BDVA, and AIOTI, offer developed software as open source, and organize open Open Calls to engage FGPA/ASIC/fabless and IoT application developers. The areas of validation address cross-cutting issues, including:

- 5G New Radio & Edge Cloud connectivity
- Resource Self-Awareness & Dynamic Connectivity
- Cross Blockchains/DLT data sovereignty
- Federated ML/ Edge Cloud ML Aggregation
- Trained ML model sharing (e.g., AGV/AGLV)
- Human Centric/AR applications Design
- Cybersecurity attacks on Privacy preserving ML
- Privacy preserving Cross-Trial/ borders Federation
- 3rd Party Application Support

The IoT-NGIN outcomes will be validated across a multitude of real-life use cases through 7 trials, involving 5 living labs and 1 IoT/5G lab:

- IoT-NGIN Integration Infrastructure Technology Lab. Comprehensive integration and evaluation throughout the development of the IoT-NGIN technologies. The task will ensure that the IoT-NGIN components achieve the expected Technology Readiness Level (TRL).
- Human-Centered Twin Smart Cities Living Lab. Adopt an innovative cross-border-by-default twin city context with the city of Helsinki in Finland and the city of Tallinn in Estonia.
- Smart Agriculture IoT Living Lab. Demonstrate significant benefits arising from IoT exploitation in optimizing various aspects of smart agriculture.
- Industry 4.0 Use Cases & Living Lab #1. Ensure human workers safety and driven Forklifts (from AGVs and the surrounding factory equipment), and to avoid collisions, a user-aware and semi-autonomous IoT system is required, which acts in real-time and solves performance challenges prioritizing human-centered safety.

<sup>91</sup> <https://iot-ngin.eu/>



- Industry 4.0 Living Lab #2. Enable advanced proactive diagnostics and optimisation of energy efficiency and productivity and for customer use case demonstrations.
- Smart Energy Grid Active Monitoring/Control Living Lab. This use case is expected to implement a smart energy pilot to demonstrate the capability of smart grid asset performance management and creating human-centred smart micro-contracts and micro-payments in a fully distributed energy marketplace.
- IoT-NGIN pilots will be federated to enable cross-IoT-NGIN services deployment. This federation will be further extended via new partners joining IoT-NGIN via Open Calls. A number of technologies developed by IoT-NGIN will be the enablers for the federation.

### **TERMINET - nexT gEneRation sMart INTERconnectEd IoT<sup>92</sup>**

Information is being constantly sent and received from one smart device to another, and the number of connections is growing every second. To reduce the complexity of the connecting vast number of heterogeneous devices TERMINET's vision is to provide a novel next generation reference architecture based on cutting-edge technologies such as SDN, multiple-access edge computing, and virtualization for next generation IoT, while introducing new, intelligent IoT devices for low-latency, market-oriented use cases.

TERMINET's primary intention is to bring (more efficient and accurate) decisions to the point of interest to better serve the final user targeting at applying distributed AI at the edge by using accelerated hardware and sophisticated software to support local AI model training using federated learning. The solution proposes flexible SDN-enabled middleware layer. It also aims to design, develop, and integrate novel, intelligent IoT devices such as smart glasses, haptic devices, energy harvesting modules, smart animal monitoring collars, AR/VR environments, and autonomous drones, to support new market-oriented use cases. Great expectation of the proposal is to foster AR/VR contextual computing by demonstrating applicable results in realistic use cases by using cutting-edge IoT-enabled AR/VR applications.

By designing and implementing an IoT-driven decentralized and distributed blockchain framework within manufacturing, TERMINET aims to support maintenance and supply chain optimization. The solution intends to apply a vertical security by design methodology by meeting the privacy-preserving and trust requirements of the NG-IoT architecture. To foster standardization activities for the IoT ecosystem, TERMINET will provide novel disruptive business models. For the evaluation of its wide applicability, TERMINET will validate and demonstrate six proof-of-concept, realistic use cases in compelling IoT domains such as the energy, smart buildings, smart farming, healthcare, and manufacturing, in order to achieve the proposed objectives:

- Provide a flexible, open, and decentralized next generation IoT reference architecture for new real-time capable solutions by enabling secure and privacy-preserving IoT services, user-aware solutions, semi-autonomous devices, and self-aware mechanisms, frameworks, and schemes, supported by distributed AI and new intelligent IoT devices within a virtualized edge-platform-cloud environment.
- Provide a set of innovative mechanisms and tools for moving AI to the edge by using cutting-edge ML technologies, avoiding data collection, and offering decentralized analytics, privacy by design and data protection.
- Enable emerging IoT security, privacy-preserving, and trust mechanisms and schemes by offering security by design and end-to-end security solutions based on leading technologies such as attestation modelling, distributed and decentralized blockchain, and enterprise-level privacy.
- Deliver an SDN-enabled MEC environment as a key enabler for IoT and mission-critical, vertical solutions, able to enable industrial 5G use cases without a full 5G roll-out, while offering a set of innovative middleware tools and mechanisms for IoT orchestration, data collection and decentralized analytics that guarantees network security, data protection, identity management and resource integrity.
- Design, implement, and integrate intelligent IoT devices supporting new generation IoT use cases, by fostering digital business development, while creating business opportunities of digitization across multi-discipline ecosystems.

<sup>92</sup> <https://terminet-h2020.eu/>



- Provide a tactile IoT model as a collaborative paradigm, by adding human-centric perspective and sensing/actuating capabilities, while enabling humans and machines to interact with their environment in real-time using haptic interaction and AR/VR capabilities.

### **VEDLIoT - Very Efficient Deep Learning in IoT<sup>93</sup>**

As the Internet of Things (IoT) continues to take shape, promising widespread automation and data exchange, one of the biggest challenges is to act on the data generated. The amount of data collected is huge, the computational power required for processing is high, and the algorithms are complex. The EU-funded VEDLIoT project develops an IoT platform that uses deep learning algorithms distributed throughout the IoT continuum. The proposed new platform with innovative IoT architecture is expected to bring significant benefits to a large number of applications, including industrial robots, self-driving cars, and smart homes.

The ever-increasing performance of computer systems in general and IoT systems, in particular, delivers the capability to solve increasingly challenging problems, pushing automation to improve the quality of our life. This triggers the need for a nextgeneration IoT architecture, satisfying the demand for key sectors like transportation (e.g., self-driving cars), industry (e.g., robotization or predictive maintenance), and our homes (e.g., Assisted living). Such applications require building systems of enormous complexity, so that traditional approaches start to fail. The amount of data collected and processed is huge, the computational power required is very high, and the algorithms are too complex allowing for the computation of solutions within the tight time constraints. In addition, security, privacy, or robustness for such systems becomes a critical challenge. An enabler that aims at delivering the required keystone is VEDLIoT, a Very Efficient Deep Learning IoT platform. Instead of traditional algorithms, artificial intelligence (AI) and deep learning (DL) are used to handle the large complexity. Due to the distributed approach, VEDLIoT allows dividing the application into smaller and more efficient components and work together in large collaborative systems on the Internet of Things (IoT), enabling AI-based algorithms that are distributed over IoT devices from edge to cloud.

In terms of hardware, VEDLIoT offers a platform, the Cognitive IoT platform, leveraging European technology, which can be easily configured to be placed at any level of the compute continuum starting from the sensor nodes and then edge to cloud. Driven by use cases in the key sectors of automotive, industrial, and smart homes, the platform is supported by cross-cutting aspects satisfying security and robustness. Overall, VEDLIoT offers a framework for the Next Generation Internet based on IoT devices required for collaboratively solving complex DL applications across a distributed system. VEDLIoT brings together 12 partners, including universities, research institutions, SMEs and large companies. The project offers an Open Call at project midterm, incorporating additional VEDLIoT-related industrial use-cases in the project, increasing the market readiness of the VEDLIoT solutions.

### **EU-IoT - The European IoT Hub - Growing a sustainable and comprehensive ecosystem for Next Generation Internet of Things**

As in any other cluster of projects, EU-IoT is the CSA that will act as glue between the different projects, aligning the efforts in different areas like dissemination, education, and standardization. EU-IoT will act as an accelerator for the whole European IoT ecosystem towards transforming the current IoT community of researchers and innovators in Europe into an increasingly cohesive, dynamic, participatory, and sustainable ecosystem, as an essential part of the Next Generation Internet initiative. It will intervene to assist stakeholders to engage and create value, as well as set up a self-sustaining European IoT community.

This requires tackling a number of challenges related to the complex interplay among stakeholders and the many relevant initiatives. The overarching need is the consolidation of fragmented IoT verticals and the still disconnected research and technology domains. To this purpose, EU-IoT set up a strong consortium and plan of action for the establishment of an open and inclusive ecosystem facilitating interactions of all players, know-how exchange, creation of strategic partnerships and durable liaisons. Agility of planning and action is paramount to meet the demand and needs of an ecosystem that is in continuous transformation.

EU-IoT will a) help to create a common strategy aligned with the NGI vision to achieve the H2020 goals, while supporting the transition to Horizon Europe; b) foster synergies, liaisons and exchange among all key players in the European landscape; c) support and coordinate outreach and impact creation activities of upcoming ICT-

---

<sup>93</sup> <https://vedliot.eu/>

56 projects and Large Scale Pilots; d) pave the way for the development of business models, innovation activities and skills building that lower adoption and deployment barriers for IoT solutions; e) provide a collaborative framework, including content, tools and processes, to engage all EU researchers, developers, integrators and users, thus overcoming fragmentation and assisting further development of a strong European IoT-empowered economy as core building block of the Digital Single Market and Digital Europe altogether.

#### **AIOTI – Alliance of Internet of Things Innovation<sup>94</sup>**

Many organizations start to see the potential opportunities of the Internet-of-things and its impacts on providing solutions that could offer operational advantages. In line with this, there are several research initiatives on IoT, such as IERC - European Research Cluster on the Internet of Things, Industrial Internet Consortium, Industry 4.0, and the creation of the Alliance for Internet of Things Innovation (AIOTI) by the European Commission, which initiates the development and future deployment of the IoT technology in Europe.

Among them, the Internet of Things Alliance for Innovation (AIOTI) represents the most relevant European initiative for this aim. This Internet of Things Alliance for Innovation (AIOTI - Alliance for IoT Innovation) has recently been created at the European level (2015), born within the Internet of Things European Research Cluster (IERC). It must be noted that nowadays, AIOTI is today the largest European IoT ecosystem. The AIOTI members include key European IoT players – large companies, successful SMEs and dynamic start-ups – as well as research centres, universities, associations, and end-user representatives. As AIOTI is an inclusive body, any interested stakeholders can freely join to this organization, enlarging this IoT ecosystem and augmenting the members' perspectives and point of view which will lead to a broader view and analysis of the current IoT landscape.

AIOTI drives on behalf of its members business, policy, research and innovation development in the IoT & Edge Computing and other converging technologies across the Digital Value Chain to support digitization in Europe, and competitiveness of Europe. The Alliance for Internet of Things Innovation (AIOTI) was initiated by the European Commission in 2015, with the aim to strengthen the dialogue and interaction among Internet of Things (IoT) players in Europe, and to contribute to the creation of a dynamic European IoT ecosystem to speed up the take up of IoT.

Other objectives of the Alliance include fostering experimentation, replication, and deployment of IoT and supporting convergence and interoperability of IoT standards; gathering evidence on market obstacles for IoT deployment; and mapping and bridging global, EU, and member states' IoT innovation activities. The AIOTI, among other activities, will support the European Commission in relation to the future of R&D on the Internet of Things and topics such as standardization and development of policy recommendations on IoT, including the definition and design of pilots to be financed in H2020 and support for the constitution of inter-sectoral consortia.

AIOTI activities are carried out through Working Groups, which focus on well-defined areas of development, to provide a very tight focus on each of these key areas. These groups include horizontal areas: research, innovation ecosystems, policy, proposed standards and distributed ledger technologies, as well as vertical, cross-disciplinary activities focused on key IoT issues and horizontal, cross-disciplinary activities focused on hot topics in the field. In this regard, 11 working groups have been created, which were initially composed mainly of large companies, and are open to the inclusion of entities that cover the entire value chain, especially SMEs and start-ups. The areas covered by these 11 working groups are:

- WG 1: IoT European research cluster
- WG 2: Innovation Ecosystems
- WG 3: IoT Standardisation
- WG 4: Policy issues (trust, security, liability, privacy)
- WG 5: Smart living environments for ageing well (e.g., smart house)
- WG 6: Smart farming and food security
- WG 7: Wearables

---

<sup>94</sup> <https://aioti.eu>

- WG 8: Smart cities
- WG 9: Smart mobility (smart transport/smart vehicles/connected cars)
- WG 10: Smart environment (smart water management)
- WG 11: Smart manufacturing

Regarding the tangible outcomes of AIOTI activity, several recommendations on different areas in IoT have been provided by this organization since its foundation. In October 2015, the Alliance published 12 reports covering IoT policy and standards issues. With these reports, AIOTI provided detailed recommendations for future collaborations on the Internet of Things Focus Area of the 2016-2017 Horizon 2020 Programme. Later, in August 2018, AIOTI published recommendations for the future IoT research priorities under Horizon Europe and Digital Europe programmes 2021-2027. This work continued with AIOTI priorities for the new political cycle in the EU (2019-2024) and Strategic Foresight Through Digital Leadership: IoT and Edge Computing Convergence.

Main benefits for the IoT community from the AIOTI initiative are the following. First, the support provided regarding the IoT, that goes from nurturing raw experimentation to enabling market deployment at scale. Second, the connection and alignment performed between key players and ideas. AIOTI brings key players together, both online and offline, in dedicated events, workshops and informed dialogue in order to discuss key topics and important aspects in IoT and obtain fruitful results of this pooling and discussion among experts and relevant stakeholders of the IoT ecosystem. Third, in the context of sense of the IoT for the European community, AIOTI performs the mapping and evaluation of the global IoT innovation. In this regard, AIOTI makes actionable business insight and market data available to all its members. And fourth, AIOTI performs a key role in Europe as it has the active lead on the convergence and interoperability of IoT standards. From an overall perspective, AIOTI helps to realize the socioeconomic benefits of an interconnected world in the IoT to gain invaluable insight into how society can benefit from the power of interconnected devices and industry improve efficiency whilst every domain remains safe, secure, and resilient. Some AIOTI activity is focused on the digital education of European citizens and on the close support to those citizens dealing with new IoT technologies, which in most cases represent European non-technical IoT end-users, to who the underlying IoT technologies and infrastructure are transparent. Taking into account that every Wi-Fi network, has a router that makes Internet connection possible, AIOTI encourages citizens to accessing to routers' administration in order to ensure the best security options and fully exploit its functionalities, while providing guidance and advice for these operations.

## 4.2 Non-IoT but related calls

Several project calls have addressed aspects that will influence the advance of ASSIST-IoT developments and ecosystem building. Finding references in this areas and liaisons with clusters, individual projects and asset results may support the project findings and contributions. The identified areas are:

- 5G calls, as Tactile Internet may be supported in some cases by results in this area.
- Artificial Intelligence as ASSIST-IoT aims to bring intelligence and decision close to the events and reduce the time between acquisition and decision making.
- Edge computing which will be one of the value propositions of ASSIST-IoT.

The research on Artificial Intelligence has been scattered in different projects and programs and analyzed as an enabler to different verticals. The research on AI has been condensate in the global initiative name AI4EU<sup>95</sup>, which was established to build the first European Artificial Intelligence On-Demand Platform and Ecosystem. With several research activities in five key interconnected AI scientific areas (Explainable AI, Physical AI, Verifiable AI, Collaborative AI, Integrative AI), which arise from the application of AI in real-world scenarios.

On the other hand, the research activities in the area of edge computing have been embedded in three main clusters: IoT, 5G and HPC. The IoT community has dealt with edge computing as an enabler for more powerful IoT gateways and new business models that will be studied and analyzed in the NG-IoT projects. All the projects associated with IoT of the previous initiative deal with the aspects of edge computing that will be useful for

<sup>95</sup> <https://www.ai4eu.eu>

ASSIST-IoT. Additionally, HPC has introduced edge computing as a corollary of cloud computing and several projects from the cloud related calls introduce edge computing as scenario or related use case to achieve the cloud continuum.

Regarding 5G, we analyze it in detail in the next section, as through 5G-PPP a structured set of calls have been launched, and moreover several aspects of 5G are cornerstones for the advancement of ASSIST-IoT, namely edge components, reduced latency or softwarization. Which are basic elements to conform the tactile approach of the project.

### 4.2.1 5G Research Projects Ecosystem and 5G-PPP

5G technological and architectural features that will shape the new access, networking, and management domains in mobile communications are currently being developed and tested across Europe. These features promise countless opportunities for service innovation and business efficiencies, creating an unprecedented impact on multiple vertical sectors<sup>96</sup>. The first wave of 5G standards (3GPP Release 15) has been released recently, while, many cutting-edge technologies, resulting from huge private and public research investment within the industry and a series of 5G-PPP projects<sup>97</sup>, are pushing their way towards higher technology readiness levels (TRL) and eventual commercialization. The next 5G release is focused on industrial applications and involves multiple trials across 28 member states, conducting both conforming and field trials for concurrent support of heterogeneous 5G use cases set by multiple vertical sectors, including the five major vertical sectors defined by 5G-PPP, namely Media & Entertainment, Public Protection and Disaster Relief (PPDR), e-Health, Automotive, and Industry 4.0.

5G vertical trials in Europe have been performed through 5G Public Private Partnership projects (5G-PPP) funded by 700M€ of the European Union research funding grants and matched by 3,5B€ of private funding in the 2014-2020 timeframe. The 5G Infrastructure Public Private Partnership (5G-PPP) is a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications operators, service providers, SMEs and researcher Institutions). The 5G-PPP is now in its third phase where many new projects were launched in Brussels initially in June 2018 and more followed in 2019 and 2020. The 5G-PPP will deliver solutions, architectures, technologies, and standards for the ubiquitous next generation communication infrastructures of the coming decade. The challenge for the 5G Public Private Partnership (5G-PPP) is to secure Europe's leadership in the particular areas where Europe is strong or where there is potential for creating new markets such as smart cities, e-health, intelligent transport, education, or entertainment and media<sup>98</sup>.

The underlying technology developed in the context of the 5G-PPP Initiative was a key enabler for many success stories. The 5G-PPP Initiative has provided a number of scientific solutions that have been contributed to standardization activities and also the global academic and research community through publications. In addition, the 5G-PPP projects have been driving test and validation activities in Europe, collecting significant experience for all stakeholders, and raising public awareness on the capabilities of 5G networks. The whole 5G-PPP trial project portfolio is now worth more than EUR 300 million of EU funding and is expected to leverage more than EUR 1 billion of private investment in 5G vertical trials, reinforcing Europe's leading position in this field<sup>99</sup>.

As the last project calls for H2020/5G-PPP took place, it is worth pointing out that the development of mobile communication technology will not stop with the end of this Programme. The last 5G-PPP project calls will be the first set of projects to consider what comes after 5G. These Beyond 5G (B5G) projects should provide the bridge to the future activities foreseen in the next Smart Networks and Services (SN&S) partnership Programme which is proposed to be part of Horizon Europe.

---

<sup>96</sup> Vertical sectors: <https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf>

<sup>97</sup> 5G-PPP projects <https://5g-ppp.eu/5g-ppp-phase-3-projects/>

<sup>98</sup> <https://5g-ppp.eu/>

<sup>99</sup> Full-5G-Annual-Journal-2020



## 5G-PPP Phases and ICT calls

More than half a decade after the launch of the 5G-PPP, first commercial 5G services are now available in a number of European cities and many 5G-PPP research projects are still ongoing. The 5G-PPP Initiative is organized in 3 different main Phases.

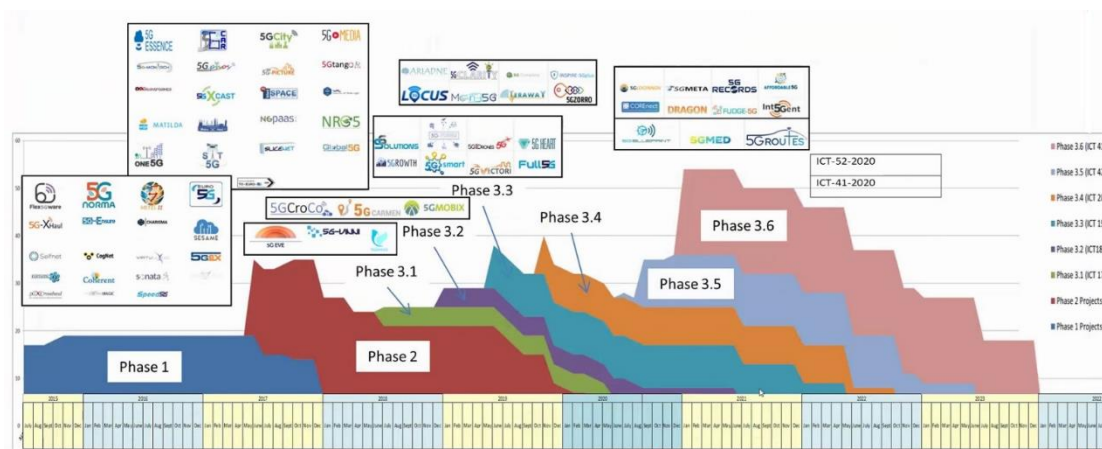


Figure 78. Overview of the 5G-PPP Programme<sup>100</sup>

The first phase (Phase 1) focused on basic research to provide the key concepts and solutions for 5G networks. The second phase (Phase 2) concentrated on bringing this new 5G technology to the vertical industries and finally Phase 3 where large-scale trials and innovation infrastructures are being created. The third phase (Phase 3) also contains basic research activities to consider evolution beyond 5G.

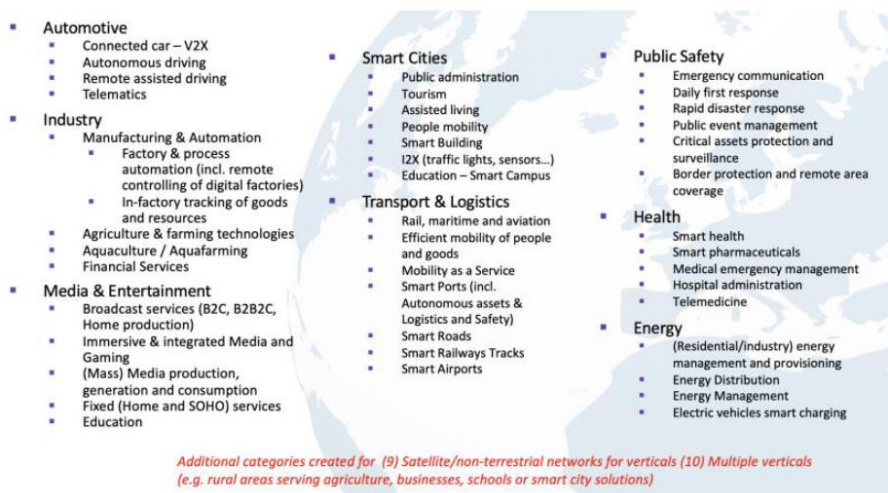


Figure 79 Mapping of use cases to vertical categories<sup>101</sup>

The last two Phases of 5G-PPP have managed to cover a significant number of vertical industries as shown in Figure 79. This is an important achievement because one of the main aims of 5G is the support of the so call verticals. Phase 2 started in June 2017, with 21 new 5G-PPP projects, including 2 complementary CSA projects. These projects relied on the technologies, produced during Phase 1, for the digitization and integration of vertical industries in Europe. Most Phase 2 projects successfully completed in 2019, while some were continuing in 2020. This phase was more focused on demonstrating and validating the developed technology and explicitly trying to integrate use cases from vertical industries beyond classical tele-communications.

During 2018, the Phase 3 of the 5G-PPP framework was initiated with the first three Phase 3 projects. This involved essentially the roll out of 5G platforms across Europe. The target was to enable large scale trials to help the stakeholders testing, in realistic environments, the key findings from the previous phases and draw

<sup>100</sup> 5G-PPP Progress Monitoring Report <https://5g-ppp.eu/wp-content/uploads/2020/10/5G-PPP-PMR2019v1-6.pdf>

<sup>101</sup> <https://global5g.org/>



significant conclusions. In 2018, three infrastructure projects (ICT-17) were selected to create a pan-European large-scale 5G test platform to be used by a number of vertical use cases. During 2019, these projects have setup a significant part of their platforms and provided a clear and detailed roadmap of their features that will be offered in multiple sites all over Europe<sup>102</sup> (refer to Figure 80, which presents the 5G Infrastructure PPP Phase 3 Platforms Projects – Geographic Cartography). Also, these projects have clearly identified how their platforms can be used for advanced testing by other 5G-PPP and not only research projects<sup>103</sup>.

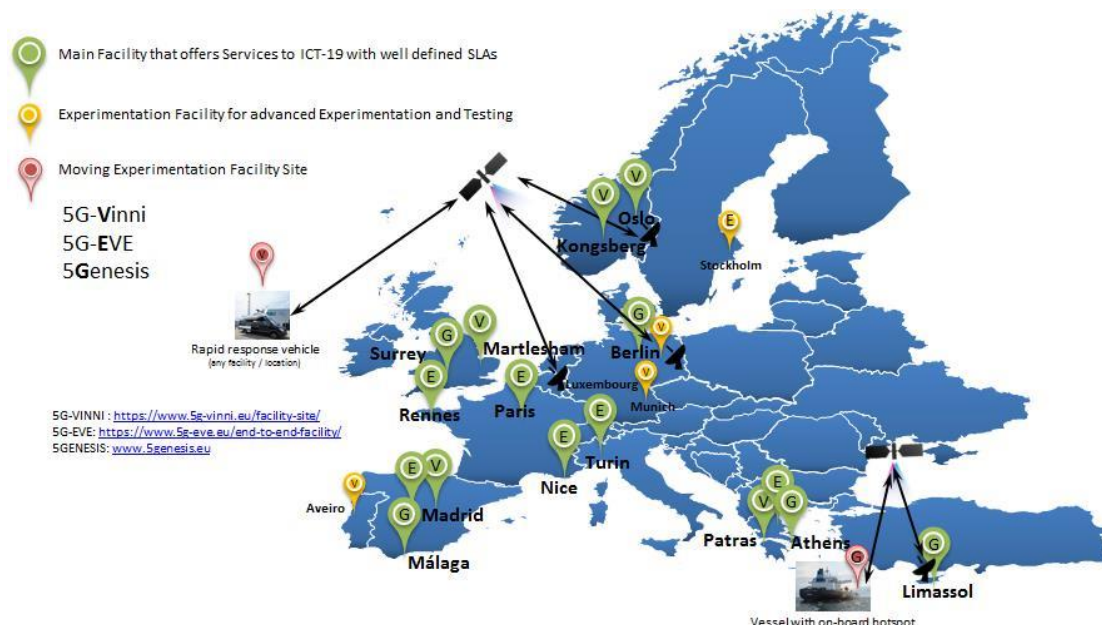


Figure 80. 5G Infrastructure PPP Phase 3 Platforms Projects – Geographic Cartography<sup>104</sup>

Also, in November 2018, three ICT-18 automotive/corridors projects started their activities implementing and testing advanced scenarios and one additional automotive project is also active in the context of EU-China Collaboration. During 2019 these projects have completed the identification of the use case to be validated in cross border/Mobile Network Operators/Vendor/Generation trials. They have identified network requirements, potential changes in the network architecture and provided recommendations for regulation and spectrum.

In relation to the ICT-19 projects (commenced June 2019), eight projects (seven R&I and one CSA projects) have been selected out from the 32 proposals that were evaluated by the EC, in response to the 5G-PPP ICT-19-2019 call. The projects mainly rely for their trials on the three ICT-17 platform projects, although some of them are also developing their own platforms to perform further testing.

The ICT-17 and ICT-19 projects are covering a significant number of vertical industries as shown in Figure 81. The first three rows illustrate the vertical industries being covered by the 3 ICT-17 projects while the remaining seven, present those covered by the ICT-19 projects.

<sup>102</sup> Technology Board white paper, 5G network support of vertical industries in the 5G-PPP ecosystem, February 2020, [https://5g-ppp.eu/wp-content/uploads/2020/03/5PPP\\_VTF\\_brochure\\_v2.1.pdf](https://5g-ppp.eu/wp-content/uploads/2020/03/5PPP_VTF_brochure_v2.1.pdf)

<sup>103</sup> Technology Board white paper, On board procedure to 5G-PPP Infrastructure Projects, April 2020, <https://5g-ppp.eu/wp-content/uploads/2020/04/On-Board-Procedure-to-5G-PPP-Infrastructure-Projects-1.pdf>

<sup>104</sup> <https://5g-ppp.eu/5g-ppp-platforms-cartography/>

	Industry 4.0	Agriculture & agri-food	Automotive	Transport & logistics	Smart Cities & utilities	Public Safety	Smart (air)ports	Energy	eHealth & wellness	Media & entertain.
5G EVE	✓		✓		✓	✓		✓	✓	✓
5GENESIS				✓	✓	✓				✓
5G VINNI	✓			✓		✓		✓		
5GIDRONES				✓		✓				✓
5G HEART		✓	✓	✓					✓	
5G GROWTH	✓			✓				✓		
5G SMART	✓									
5G SOLUTIONS	✓				✓		✓	✓		✓
5G TOURS				✓	✓		✓		✓	✓
5G VICTORI	✓			✓				✓		✓

Figure 81. Vertical industries under validation by ICT-17 and ICT-19 projects<sup>105</sup>

In November 2019, and under the ICT-20 call, eight new projects have started working on the longer-term vision for telecommunication networks. These projects target providing innovative solutions to transform the network into a low energy distributed computer. In such a system, processes and applications will be dynamically created, moved, and suppressed, depending on the information flows and customer needs. In the evolved networks, new terminal types based on gestures, facial expressions, sound, and haptics may also form the basis of the interaction between humans and infosystems. Figure 82 is the main Phase 3 reference figure of 5G-PPP.

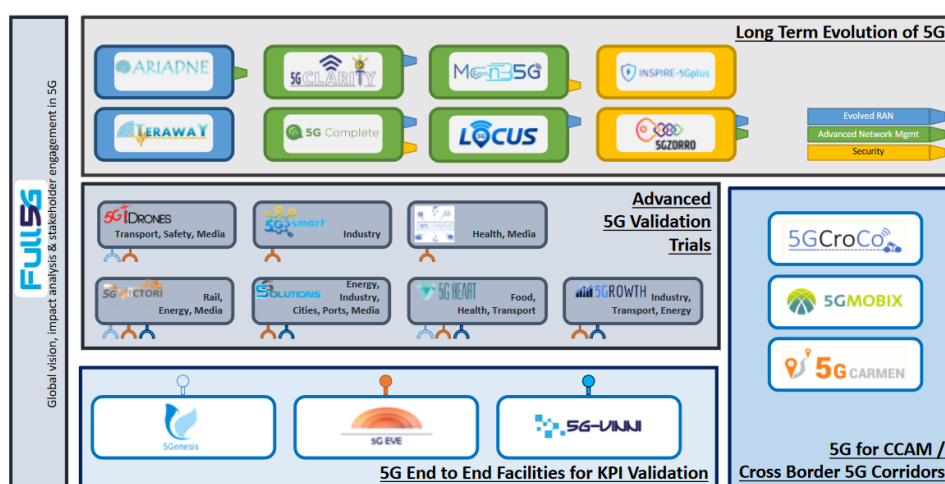


Figure 82. 5G-PPP Phase 3 Reference Figure<sup>106</sup>

5G-PPP Phase 2 and Phase 3 projects follow the overall Programme's goal to move from initial research results to large scale test-beds, getting closer to market applications. Since Phase 1, 62 projects in total have been so far contractually active in the 5G-PPP Programme, ensuring an outstanding momentum and dynamism. Also,

<sup>105</sup> 5G-PPP Progress Monitoring Report <https://5g-ppp.eu/wp-content/uploads/2020/10/5G-PPP-PMR2019v1-6.pdf>

<sup>106</sup> 5G-PPP Progress Monitoring Report <https://5g-ppp.eu/wp-content/uploads/2020/10/5G-PPP-PMR2019v1-6.pdf>

note that Phase 2 Key Achievements from 5G-PPP projects include 60 highlighted results categorised under 14 program level achievements whereas a latest counting of Key Achievements v3.0 (Figure 83), including an updated list of key achievements from Phase 2 projects and key achievements from Phase 3 projects, amount to 80 innovations under 11 categories<sup>107</sup>.



Figure 83. 5G-PPP Key Achievements v3.0

## 5G-PPP projects<sup>108</sup>

The currently active (within 2020) 5G-PPP projects are briefly presented in this section.

### Phase 2 Projects

21 5G-PPP Projects were retained from the 101 proposals received by the EC in response to the second call of the 5G-PPP. The phase 2 projects still active in 2020 are presented below:

- **5G Picture:** 5G-PICTURE designed and developed an integrated, scalable, and open 5G transport infrastructure that relies on a converged fronthaul (FH) and backhaul (BH) solution, integrating advanced wireless access and novel optical and packet network domains. 5G-PICTURE adopts the novel concept of Disaggregated-Radio Access Networks (DA-RANs), allowing any service to flexibly mix-and-match and use compute, storage and network resources through hardware (HW) programmability. This disaggregated network approach is key for the creation of a 5G infrastructure able to support a large variety of 5G ICT and “Vertical” services
- **5G-PHOS:** The main goal of the 5G-PHOS project is to create an ultra-broadband converged Fibre-Wireless (FiWi) Point-to-Multipoint (PtMP) fronthaul network, capable of supporting the required 5G New Radio fronthaul bandwidth, while at the same time alleviating the need to install Fibre terminations at every Mobile Network Operator (MNO) Base Station site.
- **5GTANGO:** It enables the flexible programmability of 5G networks by delivering an integrated NFV Service Platform, which includes a) A Service Development Kit (SDK) to facilitate developers the creation of innovative Network Services (NS) and applications; b) A Validation and Verification (V&V) Platform that facilitates the automatic testing of these NSs in “quasi-production” environments before being deployed in a real network. It targets Network Operators and/or Third-party Organizations that may provide services for the certification of these new Services. c) A Service Platform with an innovative Management and Orchestration (MANO) solution that allows the efficient orchestration of the available infrastructure resources and the control of the whole life cycle and expected performance of the NSs. It is oriented to support Network Operators.

<sup>107</sup> Annex 3 - 5G-PPP Progress Monitoring Report <https://5g-ppp.eu/wp-content/uploads/2020/10/5G-PPP-PMR2019v1-6.pdf>

<sup>108</sup> <https://5g-ppp.eu/>

- **BlueSpace:** The core concept of BlueSPACE is to exploit the added value of optical space division multiplexing (SDM) in the radio access network (RAN) and to introduce analogue radio-over-fibre (ARoF) fronthaul with an efficient optical beamforming interface for wireless transmission in the millimetre wave bands of 5G new radio (5G NR). Combining SDM with ARoF transport, BlueSPACE envisions a fronthaul network ideally suited to support large RF bandwidths and mm-wave carriers.
- **IoRL:** The Internet of Radio-Light (IoRL) project strives to develop a safer, more secure, customizable and intelligent in building network using millimetre Wave (mm-wave) and Visible Light Communications (VLC). The conceived solution reliably delivers increased through-put (greater than 10Gbps) from access points pervasively located within buildings. It does so, whilst minimizing interference and electromagnetic exposure and providing location accuracy of less than 10 cm at the same time. Thereby IoRL's ambition is to show how to solve the problem of broadband wireless access in buildings and promote 5G global standard.
- **MATILDA:** The goal of the MATILDA Project is to deliver a holistic and innovative 5G framework to under-take the design, development and orchestration of 5G-ready vertical applications (vApps) and 5G network services over programmable infrastructures. To this goal, a telecom layer platform has been designed to realise the autonomic management of the lifecycle of 5G network slices and edge computing resources. In accordance with 3GPP, the main stakeholders actively involved in this environment are three: the vertical industry owning the vApp, the telecom service provider delivering 5G services, and the telecom infrastructure provider offering computing and communication facilities.
- **MetroHaul:** The main goals were to develop an intelligent, dynamic and most importantly, 5G-aware optical transport layer that can support and deliver 5G services, far faster and far more efficiently compared to existing technologies.
- **SliceNet:** SliceNet's main objective is the design and prototyping of an innovative framework for management and control of Network Slices (NSs), leveraging Software-Defined Networking (SDN) and Network Function Virtualisation (NFV) technologies, with cognitive techniques and artificial intelligence for 5G networks.

### Phase 3 Projects - Part 1: Infrastructure projects

3 Projects have been selected from the 16 proposals received by the EC in response to the 5G-PPP ICT-17-2018 call. These three projects started in July 2018 and are running for 3 years implementing and testing advanced 5G infra-structures in Europe

- **5G-EVE:** The 5G EVE concept is based on further developing and interconnecting existing European sites to form a unique 5G end-to-end (E2E) facility. The four interworking sites are located in France, Greece, Italy and Spain (see figure) and provide both indoor and outdoor facilities. They are complemented by the Ericsson lab in Kista, Sweden. The French site is composed of a cluster of sites located in Paris, Nice, and Rennes. Each site is operated by a telecoms network operator, i.e., Orange in France, OTE in Greece, TIM in Italy, and Telefonica in Spain. The four sites are interconnected to provide a seamless single platform experience for experimenters from vertical industries. The 5G EVE end-to-end facility enables experimentation and validation with full sets of 5G capabilities – initially 3GPP Release 15 compliant and by the end of the project Release 16 compliant.  
Specifically, the technical objectives include: (i) Implementing Release 16 compatible technologies in the four sites, starting from the evolutions of current Release 15. Specific pilots validate that 5G KPIs can be achieved; (ii) Creating intent-based interfaces to simplify access to the 5G end-to-end facility; (iii) Designing and implementing site interworking and multi-x slicing/ orchestration mechanisms; (iv) Implementing a vertical-oriented open framework; (v) Creating advanced 5G testing and measurement mechanisms to validate advanced 5G features and KPIs; (vi) Advanced data analytics on the output of monitoring processes for anticipating network operations.
- **5G-VINNI:** 5G-VINNI's main objective is to provide and enable the longer term evolution of an end-to-end (E2E) 5G facility demonstrating that the key 5G-PPP network KPIs can be met, accessed and used by vertical industries to set up research trials, to further validate core 5G KPIs in the context of concurrent usages by multiple users, by serving end users with flexible and reliable services ranging from low bit rate high latency services to high bitrate low latency services and everything in between.



5G-VINNI adopts Network Slice as a Service (NSaaS) delivery model to offer customized service experience to verticals, basing its architecture on guidelines from telecom industry organizations and the normative specifications from standards bodies to ensure interoperability and reproducibility. For validating the NSaaS model, 5G-VINNI has assembled an end-to-end facility with the latest 5G technologies for radio access, backhaul, core networks, leveraging the most advanced virtualization technologies and optimization algorithms to test the model with demanding vertical sector driven applications and services. The 5G-VINNI facility sites ecosystem is modular. This modularity guarantees the highest degrees of freedom of both 5G-VINNI facility site configurations and facility interworking.

- **5GENESIS:** The main goal of 5GENESIS will be to validate 5G KPIs for various 5G use cases, in both controlled set-ups and large-scale events. This will be achieved by bringing together results from a considerable number of EU projects as well as the partners' internal R&D activities in order to realize an integrated End-to-end 5G Facility.

The 5GENESIS Facility, as a whole, will:

- Implement and verify all evolutions of the 5G standard, via an iterative integration and testing procedure;
- Engage a wide diversity of technologies and chain innovations that span over all domains, achieving full-stack coverage of the 5G landscape;
- Unify heterogeneous physical and virtual network elements under a common coordination and openness framework exposed to experimenters from the vertical industries and enabling end-to-end slicing and experiment automation; and
- Support further experimentation projects, in particular those focused on vertical markets.

The five platforms of the 5GENESIS Facility, and their main features/orientation, are:

- The Athens Platform. An edge-computing-enabled shared radio infrastructure (gNBs and small cells), with different ranges and overlapping coverage that are supported by an SDN/NFV enabled core, to showcase secure content delivery and low latency applications in large public-events.
- The Málaga Platform. Automated orchestration and management of different network slices over multiple domains, on top of the 5G NR and fully virtualised core network to showcase mission critical services in the lab and in outdoor deployments.
- The Limassol Platform. Radio interfaces of different characteristics and capabilities, combining terrestrial and satellite communications, integrated to showcase service continuity and ubiquitous access in underserved areas.
- The Surrey Platform. Multiple radio access technologies that can support massive Machine Type Communications (mMTC), including 5G NR and NB-IoT, combined under a flexible Radio Resource Management (RRM) and spectrum sharing platform to showcase massive IoT services.
- The Berlin platform: Ultra dense areas covered by various network deployments, ranging from indoor nodes to nomadic outdoor clusters, coordinated via advanced backhauling technologies to showcase immersive service provisioning.

### Phase 3 Projects - Part 2: Automotive projects

Three projects have been selected from the six proposals received by the EC in response to the 5G -PPP ICT-18-2018 call. These three projects started in November 2018 and are running for different durations implementing and testing advanced cross order 5G infrastructures in Europe.

- **5G-Carmen:** Focusing on the Bologna to Munich corridor (600 km, over three countries), the objective of 5G-CARMEN is to leverage on the most recent 5G advances to provide a multi-tenant platform that can support the automotive sector by delivering safer, greener, and more intelligent transportation with the ultimate goal of enabling self-driving cars. The project will target automation level up to SAE L3 and L4. The key innovations proposed by 5G-CARMEN project are centred around a hybrid network,



combining direct short range V2V and V2I communications, long-range V2N network communications, and back-end solutions into a single platform. The platform will employ different enabling technologies such as 5G New Radio, C-V2X, Multi-access Edge Computing and secure, multi-domain, and cross-border service orchestration to provide end-to-end network services to be tested along the corridor.

- **5G-MOBIX:** 5G-MOBIX project is an integral EU's 5G Action Plan for Europe (5GAP) that brings together a united commitment and bold initiatives to ensure that the EU can use 5G connectivity as a strategic advantage to lead digital transformation and in particular in the area of Connected and Automated Mobility (CAM). 5G-MOBIX aims to match the benefits of the 5G technology with advanced CCAM use cases in order to enable innovative, previously unfeasible, automated driving applications with high automation levels, both from a technical and a business perspective. 5G-MOBIX is executing CCAM trials along two Cross-Border Corridors (CBC) and six urban Trial Sites. The trials allow 5G-MOBIX to conduct impact assessments, including business impact and cost/benefit analysis, particularly in sparsely populated cross-border areas with mild market failures of mobile network connectivity. As a result of these evaluations and international consultations with the public and industry stakeholders, 5G-MOBIX will identify new business opportunities for 5G enabled CCAM and propose recommendations and options for its deployment. Through its findings on technical requirements and operational conditions, 5G-MOBIX will define deployment scenarios and is expected to actively contribute to standardization and spectrum allocation activities.
- **5G-Croco:** The vision of cooperative, connected and automated mobility (CCAM) throughout Europe can only be realized when harmonized solutions that support cross-border traffic exist. The possibility of providing CCAM services throughout different countries when vehicles cross various national borders has a huge innovative business potential. However, the seamless provision of connectivity and the uninterrupted delivery of real-time services along borders also pose technical challenges which 5G technologies promise to solve. The situation is particularly challenging given the multi-country, multi-operator, multi-telco-vendor, multi-car-manufacturer, and cross-generation scenario of any cross-border layout.

### Phase 3 Projects - Part 3: Advanced 5G Validation Trials Across multiple Vertical industries

Eight projects have been retained from the 32 proposals received by the EC in response to the 5G PPP ICT-19-2019 call. These eight projects started in June 2019 and are running for about three years to get the European 5G Vision of "5G empowering vertical industries" closer to deployment

- **5G SMART:** The manufacturing sector is entering a period of disruptive change and digital transformation towards what is termed Industry 4.0. Smart manufacturing is at the heart of this, enabling the transformation of today's factories into factories of the future, making the vision of highly efficient, connected and flexible factories become reality. For this, future manufacturing systems require the implementation of a reliable communication system capable of handling diverse types of information exchange that is found in a manufacturing environment and which can require low reaction times and deterministic performance. 5G is foreseen as a key enabler for this future manufacturing ecosystem.
- **5G Solutions:** 5G-SOLUTIONS is one of the seven EU-funded H2020 5G-PPP projects supporting EC's 5G policy by implementing the last phase (Phase 3b) of the 5G-PPP roadmap. It addresses the challenge of the call 'H2020 ICT-19-2019: Industry heavyweights drive advanced 5G validation trials across multiple vertical industries' and the consortium from EU telecom and vertical industries and renowned research organizations, the majority of which participate in 24 out of the 43 5G-PPP projects and in several 5G-PPP Working Groups. 5G-SOLUTIONS aims at proving and validating that 5G provides prominent industry verticals with ubiquitous access to a wide range of forward-looking services with orders of magnitude of improvement over 4G, thus bringing the 5G vision closer to realization. The project is going to setup several living labs to cover the majority impact of 5G revolution. Each of said living labs will be organized in different use cases.

- **5G TOURS:** As the early pioneering platforms of 5G start to mature the wireless industry will seek to enable growth in markets beyond its existing and growing mobile broadband sector. 5G-TOURS focuses on three significant economic value creation sectors for Europe; namely Tourism, Health and Transport and seeks to evidence growth potential through 5G platforms. Through a sharp focus on the trials of thirteen use cases, 5G-TOURS will demonstrate the advantages of 5G technology in pre-commercial “friendly customer” trials environments. However, with the emphasis of the value propositions of the use cases on end users like tourists, citizens and patients, the challenge for the project goes beyond proving of technology and towards establishing proof points through recognized validation techniques that point to business models that have potential to gain traction in the market.
- **5G-HEART:** The 5G for HEalth, AquacultuRe and Transport (5G-HEART) validation trials project performs vertical validation trials on top of all three ICT-17 facilities (5G-VINNI, 5G-EVE and 5Genesis) and two national 5G test platforms (5GTN and 5Groningen) with use cases from three different vertical domains: healthcare, transport and aquaculture. In the health area, 5G-HEART validates pill cams for automatic detection in the screening of colon cancer and vital-sign patches with advanced geo-localization as well as 5G AR/VR paramedic services. In the transport area, 5G-HEART validates autonomous/assisted/remote driving and vehicle data services. Regarding food, the 5G-based also focus on the transformation of the aquaculture sector. 5G-HEART takes important steps for progressing the synergy between telecom and vertical industries. These three vertical industries and related connectivity use cases pose diverse technical requirements on wireless network connectivity.
- **5G-VICTORY:** The main goal of 5G-VICTORI is to conduct large-scale trials for advanced use case (UC) verification in commercially relevant 5G environments for a number of verticals. These include Transportation, Energy, Media and Factories of the Future, as well as some specific UCs involving cross-vertical interaction. The project will exploit extensively the existing ICT-17 5G Testbed Infrastructures interconnecting main sites of all ICT-17 infrastructures, namely 5G-VINNI, 5GENESIS and 5G-EVE and the 5G UK test-bed in a Pan-European Network Infrastructure. Minor enhancements will be provided to these infrastructures, extending their coverage towards the integration of the 5G-VICTORI UCs
- **5G!Drones:** The main goal of the 5G!Drones project is to enable safe and secure Beyond Visual Line of Sight (BVLOS) flights using 5G mobile networks. The project will deliver the solutions to enable better business models for the use of 5G networks in Unmanned Aerial Vehicle (UAV) operations. 5G networks leverage the mission planning, automation of flight operations, and post-flight data analysis, all of which is within the scope of the use cases and scenarios being carried out in the project. Alongside the use cases, the project also aims to deliver viable and sustainable business models for the use of 5G networks in the context of UAVs.
- **5GGROWTH:** The key objective of 5G is to provide the vertical industries with an infrastructure that is able to support more efficiently connectivity needs. At the same time 5G aims at enabling new innovative digital use cases and facilitating the creation of cross-industry partnership. The vision of the 5GGROWTH project (<http://5growth.eu/>) is to empower verticals industries, in particular covering Industry 4.0, transportation, and energy domains with an AI - driven automated and sharable 5G end-to-end solution that will allow these industries to simultaneously achieve their respective key performance targets.
- **Full5G:** The Full5G project has a prime objective to facilitate the activities of the European 5G Initiative, as outlined in the 5G contractual Public Private Partnership (5G-PPP), during its third phase from June 2019 to September 2021. In addition to this, the Full5G project has a second prime objective to capture and promote the achievements of the 5G-PPP and monitor the impact these results have had on the evolution of 5G in Europe over the period of lifetime of 5G-PPP. This work will also look to the future and consider what additional actions are necessary to maintain the European momentum and leadership in 5G, as it moves towards Smart Networks, and facilitates the uptake of 5G by the European vertical sectors.

### Phase 3 Projects - Part 4: 5G Long Term Evolution

Eight projects have been retained from the 66 proposals received by the EC in response to the 5G-PPP ICT-20-2019 call. These eight projects started in November 2019 and will run for about three years to work on the longer-term vision.

- **5G-ZORRO:** The 5G-ZORRO envisions the future 5G networks as composed of distributed heterogeneous resources by different operators across diverse geographical areas, who in turn form an end-to-end secure chain of trust in which 5G radio, spectrum, edge and core computing, storage and networking can be shared and chained thanks to efficient and flexible mechanisms to discover, broker, trade, instantiate and monitor resources and services across the different operators' domains. However, to ensure robust, reliable, and secure communications in future 5G, the industrial and research community needs to maintain a laser focus on the joint realization of zero-touch security & trust framework and fully automated network management. 5GZORRO will develop these envisaged solutions for zero-touch service, network and security management in multi-stakeholder environments (ubiquitous), making use of Smart contracts based on Distributed Ledgers Technologies to implement required business agility.
- **5G-CLARITY:** It is a 5G-PPP Phase III project, started on November 1, 2019, and is planned to be concluded on April 30, 2022. The consortium consists of 12 strong industrial and academic partners from across EU and UK. 5G-CLARITY brings forward the design of a system for beyond-5G private networks by addressing the specific challenges in this area, such as: the need to coexist with, and effectively integrate to, non-3GPP technologies such as Wi-Fi and LiFi, essentiality for novel management systems that simplify the operation and maintenance of 5G networks, design of mechanisms for combining private and public 5G networks, to allow vertical users to decide the level of 5G functionality that they want to maintain on-premises, and, incorporation of value-added services that have not been traditionally a priority for mobile network operators, such a cm-level positioning, that may be strategic for vertical users. 5G-CLARITY investigates how the concept of private 5G networks should evolve beyond the 3GPP Release 16, by bringing innovation in two main pillars.
- **5G-COMPLETE:** It aims to revolutionize the 5G architecture, by efficiently combining compute and storage resource functionality over a unified ultrahigh capacity converged digital/analog FiberWireless (FiWi) Radio Access Network (RAN). By employing the recent advances in Ethernet fronthauling introduced by the eCPRI standard as a launching point, 5G-COMPLETE introduces and combines a series of key technologies under a unique architectural proposition that brings together: i) the high capacity of fiber and high-frequency radio, ii) the audacity of converged FiWi fronthauling, iii) the spectral efficiency of analog modulation and coding schemes, iv) the flexibility of mesh self-organized networks, v) the efficiency of high-speed and time-sensitive packet-switched transport, vi) the rapid and cost-efficient service deployment through unikernel technology and finally vii) an enhanced security framework based on post-Quantum cryptosystems.
- **ARIADNE:** The ARIADNE project is going to enable efficient high-bandwidth wireless communications by developing three complementary but critical new technologies for Beyond 5G networks in an integrated and innovative way: (a) ARIADNE will develop new radio technologies for communications using the above 100Ghz D-Band frequency ranges, (Pillar 1), (b) ARIADNE will exploit the opportunities emerging for advanced connectivity based on metasurfaces where objects in the environment can become tuneable reflectors for shaping the propagation environment in D-band. (Pillar 2) and (c) ARIADNE will employ Machine Learning and Artificial Intelligence techniques to management necessary for the high-frequency communications and dynamic assignment and reconfiguration of the metasurfaces to provide continuous reliable High Bandwidth connections in the Beyond 5G scenario (Pillar 3).
- **INSPIRE-5Gplus:** INSPIRE-5Gplus makes a revolutionary shift in the 5G and beyond security vision. It is advancing 5G security and devising a smart, trustworthy and liability-aware 5G security platform for future connected systems. INSPIRE-5Gplus will enable advancing the 5G and beyond security vision by adopting a set of emerging trends and technologies, such as Zero-Touch Management (ZTM),

Software-Defined Security (SD-SEC), Artificial Intelligence/Machine Learning (AI/ML) techniques and Trusted Execution Environment (TEE). A new breed of SD-SEC assets will be developed to address some known challenges, e.g., adaptive slice security, and new ones like proactive security.

- **LOCUS:** The goal of LOCUS is to design and develop a location management layered infrastructure not only capable of improving localization accuracy and security, but also to extend it with physical analytics, and extract value out of it, meanwhile guaranteeing the end user's right to privacy. To this end LOCUS will build upon the work of 3GPP (Rel. 16 and Re. 17), which has started to address the cellular localization functionality and to which some LOCUS partners are directly contributing. In more detail, 3GPP Rel. 17 is currently extending the functionality of 5G infrastructures to enable positioning reference signals, measurements and procedure information. Building on top of these components, adequate low-complexity algorithms and scenario-dependent deployment designs can enable future versions of 5G networks to: (i) provide accurate and ubiquitous information on the location of physical targets as a network-native service, and (ii) derive complex features and behavioral patterns from raw location and physical events, which can be exposed to application developers. Localisation, appropriate dedicated analytics, and their combined provision "as a service" will greatly increase the overall value of the 5G ecosystem and beyond and allow network operators to dramatically expand their range of offered services, enabling holistic sets of user, location- and context-targeted applications.
- **MonB5G:** MonB5G aims at deploying a novel autonomous management and orchestration mechanism framework by heavily leveraging distribution of operations together with state-of-the-art Artificial Intelligence (AI) based mechanisms. The developed system is based on a hierarchical approach that allows the flexible and efficient management of network tasks, while at the same time, introducing a diverse set of centralization levels through an optimal adaptive assignment of monitoring, analysis, and decision-making tasks. The MonB5G approach focuses on the design of a hierarchical, fault-tolerant, automated data driven network management system that incorporates security as well as energy efficiency as key features, to orchestrate a massive number of parallel network slices and significantly higher types of services in an adaptive and zero-touch way
- **TERAWAY:** TERAWAY project is designed to complement 5G vision for a fully mobile and connected society and to address the ultra-high capacity, ultra-broadband connectivity, reliability and latency requirements imposed by 5G verticals. More specifically, TERAWAY, by leveraging optical concepts and photonic integration techniques, targets to develop a technology base that combines the generation, emission and detection of wireless signals with selectable symbol rate and high bandwidth within an ultra-wide range of carrier frequencies covering the W-band (92-114.5 GHz), D-band (130-174.8 GHz) and THz band (252-322 GHz). In parallel, aiming to get the most out of the THz technology and enable its commercial uptake, a new software defined networking (SDN) controller and an extended control hierarchy will be developed for the management of the network and the radio resources in a unified manner, capable of providing network slices to the support of diverse services. TERAWAY started on November 2019 and by its completion will make available a set of ground-breaking transceiver modules with 4-channel modules operating from 92 up to 322 GHz, offering up to 241 Gb/s total data rate with transmission reach more than 400 m in the THz band. Four (4) independently steered wireless beams will be used to establish BH and FH connections between fixed terrestrial and moving network nodes.



## 5 Market analysis

### 5.1 NG-IoT market analysis

#### 5.1.1 The Global IoT market

According to Fortune Insight and IDC, the global IoT market is expected to reach approximately \$1.4k billion by 2027 [MA-1]. The number of IoT connections is expected to increase dramatically, from 7 billion in 2017 to 25 billion in 2025, with a Compound Annual Growth Rate (CAGR) of 17%. The largest growth of IoT connections (both cellular and non-cellular) can be expected because of industrial IoT applications, responsible for more than 50% of the connections, followed by Smart Offices and Healthcare.

The overall expectation is that the largest growth of IoT connections will take place in Asia-Pacific, estimated at 10.9 billion by 2025, followed by North America, Europe, and the Middle East. The Middle East is expected to experience rapid growth with a CAGR of 15.7% over the 2017-2025 period.

Estimating the economic impact and Gross Domestic Product (GDP) growth from IoT on business production has been and remains difficult. In many models, calculations include the number of IoT connections and the associated values. Conservative estimates show a growth of € 370 billion in 2025, equivalent to 0.34% of global GDP. Split by region, this means for 2025: North America 0.46%, Asia-Pacific 0.36% and Europe 0.27% in GDP growth.

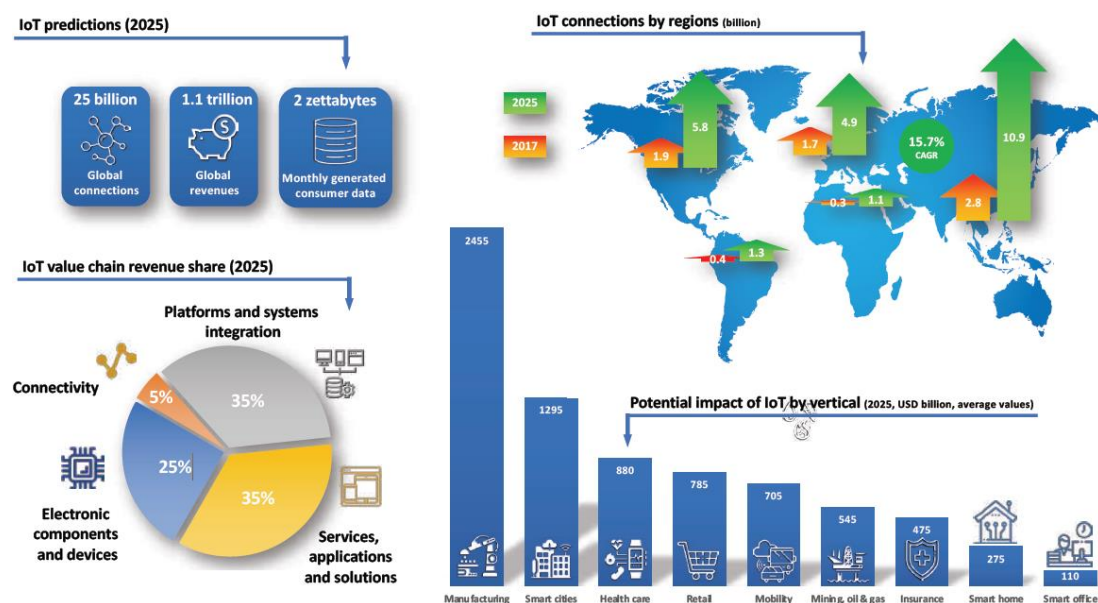


Figure 84. Global market estimations [MA-2]

#### 5.1.2 IoT value chain analysis

The IoT value chain explains the building blocks of IoT, how value is created, who the players are, and how they interact with each other to deliver the value. As illustrated in Figure 85, six main players conform the IoT value chain:

- *Electronic Component Providers*: Chips / module segment consists of embedded chipsets, IoT modules, sensors, transponders, etc.
- *Device suppliers*: industrial edge controllers, smart devices such as smart thermostats, smart meters, smart parking sensors, IoT gateways, etc.
- *Telecom operators and connectivity segments*: consist of network equipment and devices for facilitating end-to-end connectivity of IoT devices installed in the network.
- *Platform providers and System integrators*: different software platforms for aggregating, processing, securing, storing, analysing, visualizing, controlling, monitoring, and understanding IoT devices / data.



- *The Application and Solutions segment:* Consists of software and domain-specific applications and services that use IoT data to integrate and end-to-end ecosystem, operationalize the services and deliver managed these services to the clients.

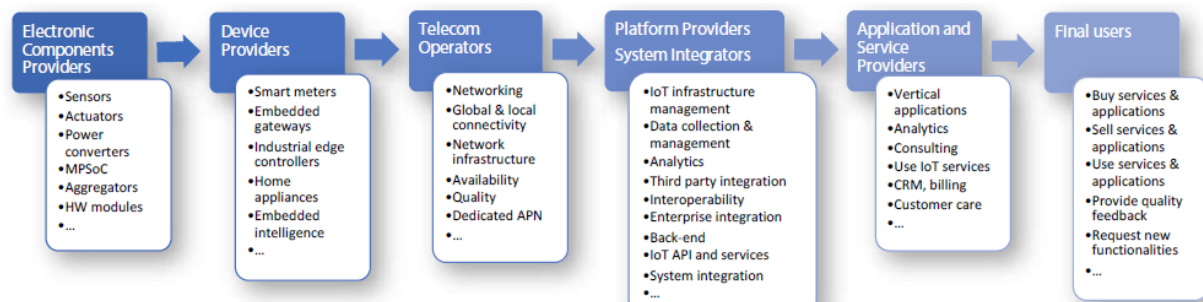


Figure 85. Simplified vertical domains stakeholders' value of the IoT value chain.

According to the analysis of Artemis [MA-2] and EY-Analysis [MA-3], the share of value within the IoT value chain is built up with the following components. Hardware such as electrical components represent 25% of the total IoT value chain. Network and device providers represent 20%. Connectivity and telecom operators have 5%. Platform providers and system integrators represent 15%. Most of the IoT value chain, 35% goes to the application and service providers.

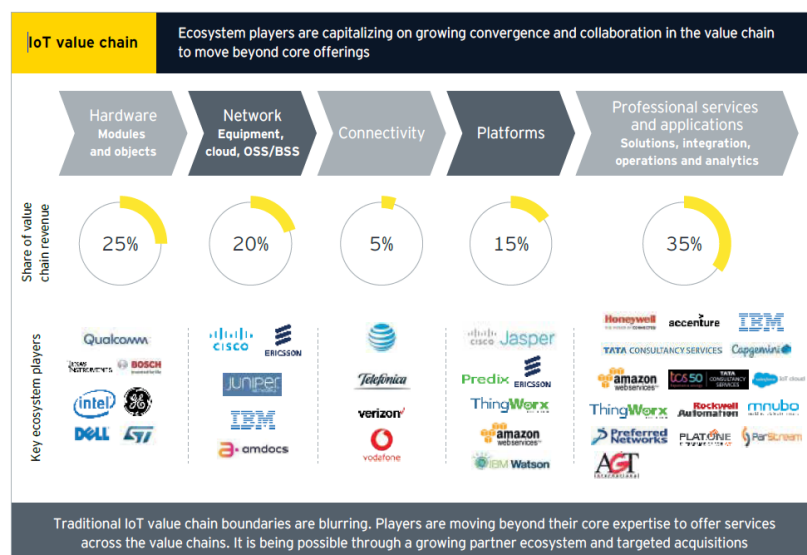


Figure 86. IoT value chain [MA-3]

## 5.1.3 Market Size and Forecast

### 5.1.3.1 Global edge computing market size

The global edge computing market size was estimated by Grand-View-Research (GVR) [MA-4] at \$3.5 billion in 2019 and will grow at a compound annual growth rate (CAGR) of 36.9% from 2020 to 2027 to reach \$43.36 billion by 2027. The market size figures given by Allied Market Research [MA-5] are more conservative. They estimate the edge computing market size was valued at \$1.7 billion in 2017, and is projected to reach \$16.6 billion by 2025, growing at a CAGR of 32.8% from 2018 to 2025. Table 29 illustrates this global edge market forecast from different Market forecasters.

Table 29. Expected global edge market size and CAGR from different consultancy enterprises

Global Edge Computing Market	Markets and Markets (2020)	Allied Market Research (2019)	Market Research Future (2019)	Grand View Research (2019)
Market Size 2017		\$1.7 billion		
Market Size 2019				\$3.5 billion

Global Edge Computing Market	Markets and Markets (2020)	Allied Market Research (2019)	Market Research Future (2019)	Grand View Research (2019)
Expected Market Size 2020	\$3.6 billion			\$4.7 billion
Expected Market Size 2024			\$22.5 billion	
Expected Market Size 2025	\$15.7 billion	\$16.6 billion		
Expected Market Size 2027				\$43.4 billion
CAGR	34.1% from 2020 to 2025	32.8% from 2018 to 2025	28.4% from 2018 to 2024	36.9% from 2020 to 2027

### Hardware segment review

The hardware segment dominates the global edge computing market with a 47.7% share in 2019. This is attributed to the growing cloud-based applications in which the server plays a crucial role, acting as the invisible computing backbone for the services on which users are dependent. Furthermore, data center operators and enterprises in the Asia-Pacific region are expected to build edge data centers that better connect to the use of IoT devices and edge computing over 5G networks and, according to market researchers, the region is expected to have the highest CAGR from 2020 to 2027. With respect to Europe, it is predicted that it will have the second largest share of the global edge computing market. Among other things, the increasing adoption of edge computing solutions in countries such as Sweden, Italy, Spain, France, Germany, and the UK contributes to the global growth of the edge computing market in the region. In summary, as it can be seen in Figure 87, McKinsey [MA-6] estimates that edge computing hardware segment includes sensors, on-device firmware, storage, and processors, and will represent a potential value from \$175 billion to \$215 billion in hardware by 2025.

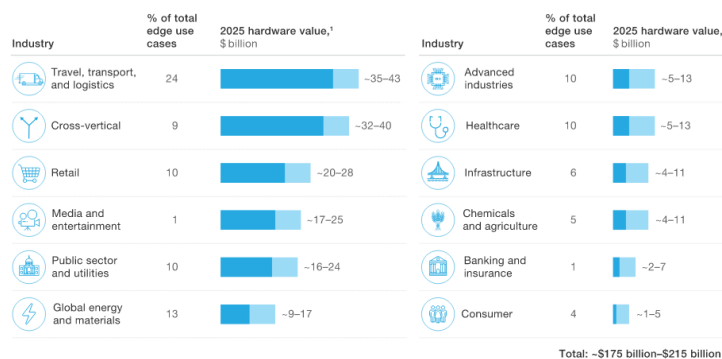


Figure 87. Global IoT Edge computing hardware per application segment [MA-6]

### Application segment review

The global edge computing market is often divided into components, applications, organization size, industry vertical, and region. The components segment includes services and solution for applications such as connected cars, smart grids, critical infrastructure monitoring, traffic management, environmental monitoring, augmented reality, asset tracking, security & surveillance, and others. According to Allied Market Research [MA-5], the largest growth will take place in the application areas security & surveillance, smart grid, connected cars and environmental monitoring.

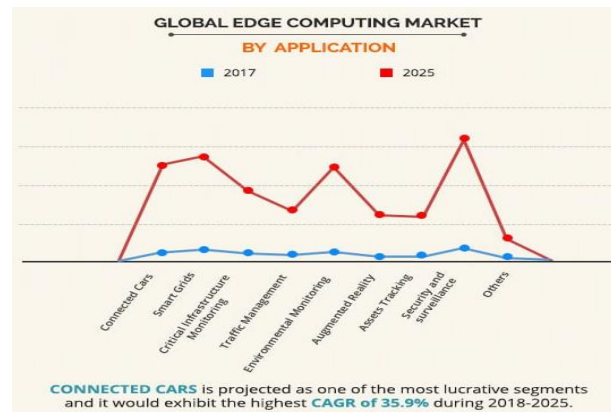


Figure 88. Global Edge computing market per application segment [MA-5]

### 5.1.3.2 Global Fog computing market size

The terms Fog and Edge computing are frequently used interchangeably. In Fog computing the intelligence, processing power and communication takes place in a Fog-Node or an IoT gateway at the local network level or network architecture. Whereas in Edge computing, the intelligence, processing power and communication take place in the edge gateway or device and then directly forwarded to programmable automation controllers (PACs). Many IoT software companies have launched products that push the limits by embedding complex event processing, Machine Learning and Artificial Intelligence in the Fog- and Edge-Computing nodes catering to this expanding market segment. IDC predicts that by 2025, nearly 45% of the world's data will move closer to the network edge. Fog Computing architecture is a key to being able to process, store and transport this large amount of data and enables emerging technologies such as IoT, 5G and AI. The total market opportunity for Fog Computing is expected to rise to \$18.2 billion by 2022, up from \$3.7 billion in 2019 (see Figure 89).

Global Fog-Computing market revenue	International Data Corporation
Market Size 2018	USD 1.0 billion in 2018
Market Size 2019	USD 3.7 billion in 2019
Expected Market Size 2020	USD 8.1 billion by 2020
Expected Market Size 2021	USD 12,7 billion by 2021
Expected Market Size 2022	USD 18.2 billion by 2022

Figure 89. IDC global fog computing market estimations.

### 5.1.3.3 Global hyper-connectivity communication system market size

Hyper-connectivity, along with edge / fog computing, embedded intelligence (AI / DL), security awareness and sustainability, will be the main key factors leading to the massive scale IoT evolution ASSIST-IoT partners envisioned. NG-IoT should be an information tool that can improve business efficiency, but more importantly, unlock new opportunities that, with an appropriate business model, can generate high-quality revenue streams.

Connectivity is a fundamental factor in the existence of IoT, but it is not enough to support and manage the avalanche of information collected by globally used sensors and send it in real time to the processing nodes of the IoT infrastructure, directly to the cloud or data centres. While edge computing could significantly reduce the amount of transferred data, connectivity scalability remains a critical aspect of IoT adoption. The communication systems will have to efficiently manage hundreds of billion connected devices and generate tens or hundreds of zettabytes of data per month. Key factors that hyper-connectivity will need to support are a wide range of protocols, geo-controlled switches, strong service, and price customisation. According to the Artemis-IA whitepaper [MA-2] a global and high-quality hyper-connectivity is a crucial factor for the adoption of NG-IoT system solutions. According to Cisco, five quintillion bytes of data are produced every day. At present, only a small part of this data goes via the IoT infrastructure to the cloud or data centres for data analysis.

For the very near future, efficient data transfer via hyper-connectivity is required. 5G technology is in the spotlight, with high expectations. According estimates made by IDC, the global 5G services will drive 70% of

businesses to spend \$1.2 billion on connectivity management solutions [MA-4]. Satellite communications are a complementary approach to connectivity hitting hype: more than 2500 satellites were launched by the end of 2020. This marks a new era of broadband internet that is expected to rely on a satellite network, consisting of more than 12,000 satellites by 2023.

The forecast is that hyper-connectivity communication systems will need to efficiently manage the more than 100 billion connected devices that generate tens or hundreds of zettabytes of data per month. As a result, the use of IoT technology will greatly increase in the number of applications such as satellite technology, mobile network, Wi-Fi connectivity, Bluetooth connectivity, NFC, RFID, LPWAN, and others. As the number of connected IoT devices grows from 7 billion in 2018 to 22 billion in 2025, LPWANs are expected to be a major driver of growth. IoT Analytics [MA-7] estimates that LPWAN will be the fastest growing NG-IoT communication technology over the next 5 years, with the number of LPWAN connected devices growing 109% per year and forecast to exceed the 1 billion mark in 2023. Consequently, LPWAN will be the fastest growing IoT connectivity technology over the next 5 years.

### Global 5G market size

The global market for 5G technology, estimated by PR Newswire<sup>109</sup> and Allied Market Research [MA-8], is projected to reach \$5.53 billion in 2020, reaching \$667.90 billion by 2026, showing a CAGR of 122.3 percent from 2021 to 2026. Asia-Pacific would be the highest contributor to the global market, with \$2.20 billion in 2020, and is estimated to reach \$329.09 billion by 2026, registering a CAGR of 130.7% during forecast period. The increasing number of IoT devices and edge computing are one of the major drivers for the 5G market.

The 5G Infrastructure market was valued by Mordor Intelligence [MA-9] at \$3.47 billion in 2020, and it is expected to reach \$53.82 billion by 2026, registering a CAGR of 53.01%, during the forecast period 2021-2026. On the other hand, the 5G infrastructure market is estimated by Market & Markets [MA-10] to be valued at \$784 million in 2019 and is projected to reach \$47,775 billion by 2027, at a CAGR of 67.1%. Increasing M2M connections across various industries are also expected to drive the 5G infrastructure growth during the forecast period. Table 30 illustrates the global 5G market forecast from different market analysis reports.

Table 30. Expected global 5G market size from different consultancy enterprises

Global Edge Computing Market	PR Newswire	Allied Market Research	Mordor Intelligence	Markets & Markets	Grand View Research
Market Size 2019				\$0.79 billion	\$1.83 billion
Market Size 2020	\$5.53 billion	\$5.53 billion	\$3.47 billion		
Expected Market Size 2026	\$667 billion	\$667 billion	\$54 billion		
Expected Market Size 2027				\$48 billion	
CAGR	122.3% from 2021 to 2026	122.3% from 2021 to 2026	53% from 2021 to 2026	67.1% from 2019 to 2027	59.6% from 2020 to 2027

The continuous development and evolution of 5G networks is expected to provide great opportunities for the edge computing market. Notably, the number of connected devices is expected to increase significantly with the launch of the 5G network. In addition, the connected device and 5G networks are expected to cause massive data loads on physical data centres and result in increased bandwidth demand and lower latency. Therefore, all these factors are expected to create great growth opportunities for the market.

<sup>109</sup> <https://www.prnewswire.com/news-releases/5g-technology-market-size-is-expected-to-reach-usd-667-90-billion-by-2026--valuates-reports-301007406.html>

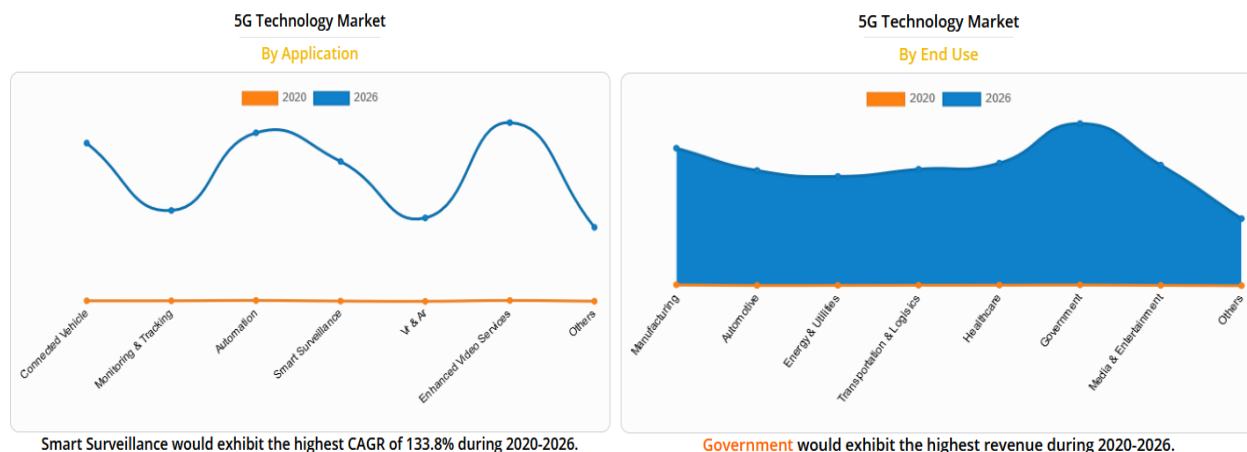


Figure 90. 5G Technology Market by application segment.

For 2020-2030, Ericsson [MA-11] forecast the share and growth rate for global total 5G activated B2B opportunities for service providers. Today, healthcare and the manufacturing have the largest share with 21% and 19% respectively. Based on this forecast, the largest share in 2030 will be occupied by Manufacturing with +76%, Healthcare with +75% and Media & Entertainment with +86% respectively.

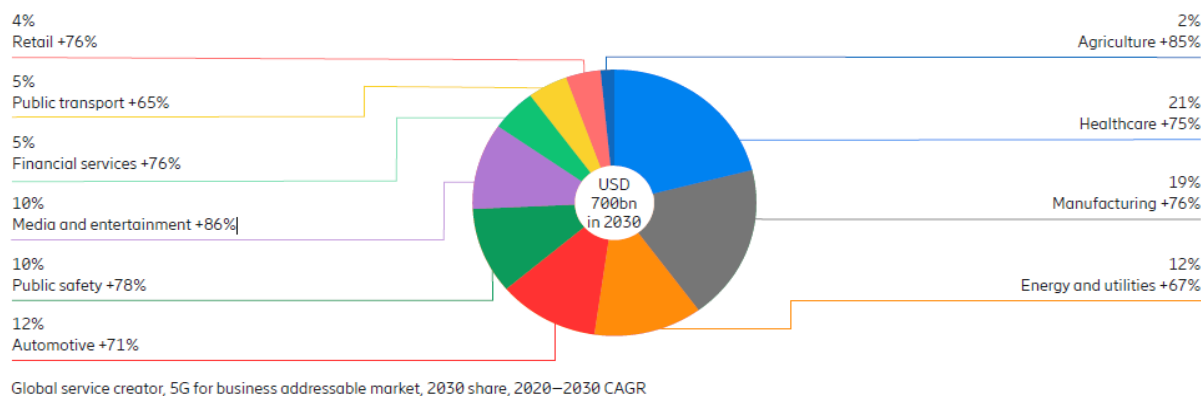


Figure 91. 5G market compass 2020-2030 - ericsson.com

### Global High-speed Industrial Ethernet market size

IoT Analytics' latest report [MA-12] finds that by 2020, approximately 50% of industrial assets in factories will be connected to some form of on-premises or remote data collection systems. The proportion of connected assets is projected to continue to rise and will be a key growth driver of the 5% CAGR that will grow the industrial connectivity market from \$ 38.2 billion in 2018 to \$ 51.4 billion in 2024. Table 31 summarises the Industrial connectivity market size from 2018 to 2024.

Table 31. Expected global industrial connectivity market size from 2020 up to 2024

Global Industrial Connectivity Market Size	2020	2021	2022	2023	2024	CAGR
Business value (\$ B)	42.1	44	46.2	48.6	51.4	
Growth		4.5%	5.0%	5.2%	5.8%	5%

### 5.1.3.4 The global Artificial Intelligence market size

Adding intelligence to IoT solutions is seen as one of the key drivers to bring the IoT market to all its size and vertical domains. AI will soon become part of our daily lives, offering functionalities and services that are seamlessly integrated with human activities. Thanks to built-in intelligence, IoT solutions will evolve from simple data collection to a more valuable collection of knowledge. Built-in intelligence allows these smart objects to learn from experiences, adapt to new input, and perform specific tasks without human intervention.



Artificial intelligence has a profound impact on computers and remains a fundamental technology for the evolution of IoT.

Analysing the data from the various market researchers, the difference between the figures presented is striking. The big differences arise when taking the derived business value or just the external spending for the AI solution or AI software. According to a Gartner [MA-13] report the global AI-derived business value growth will slow from 2018 through 2025 — dropping from a peak of 70% to 7% by 2025; enterprises between 2017 and 2022 will use niche solutions that address one need very well. Gartner estimates that by 2022, more than 80 percent of the enterprise IoT projects will rely on embedded intelligent components, while IoT Analytics estimates a growth of the industrial AI market size from \$11 billion of 2018 to \$72 billion by 2025, with a CAGR of the 31%.

Allied Market Research [MA-15] expect, according to a 2018 report: “Artificial Intelligence (AI) Market Outlook: 2025”, that the artificial intelligence market accounted for \$4,065.0 million in 2016, and is expected to reach \$169,411.8 million by 2025, growing at a CAGR of 55.6% from 2018 to 2025. In 2016, North America dominated the global market, in terms of revenue, accounting for about 49.0% share of the global market, followed by Europe. The machine learning segment has the highest share, approximately 52.0%, within the artificial intelligence market in 2016 and is expected to grow at a CAGR of 56.4% over the forecast horizon. Table 32 illustrates the global AI market forecast from different consultancy reports.

Table 32. Expected global AI market size from different consultancy enterprises

Global AI Market	Gartner	Allied Market Research	IoT Analytics	Marketwatch
Market Size 2020	\$2.64 billion			
Expected Market Size 2021	\$3.34 billion			
Expected Market Size 2022	\$3.93 billion			
Expected Market Size 2023	\$4.36 billion			
Expected Market Size 2024	\$4.72 billion			
Expected Market Size 2025	\$5.02 billion	\$169 billion	\$72 billion	\$18 billion
CAGR	39% in 2020 7% in 2025	55.6% from 2018 to 2025	31% from 2018 to 2025	35.2% from 2018 to 2025

Allied Market Research believes that within the AI segment, the market size for ML has been the largest since 2016 and is expected to continue for 2025 due to the increasing demand for ML solutions to the AI industry.

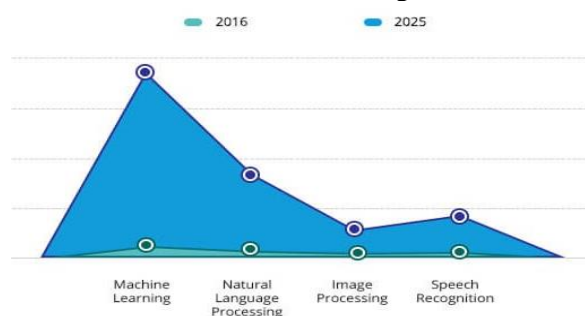


Figure 92. Global AI market by application

### 5.1.3.5 Global Distributed Ledger Technology market size

The global DLT (or blockchain) market is estimated to be \$3.0 billion in 2020 according to Markets and Markets [MA-16]. The expected CAGR is expected to be 67.3% resulting in a market size of \$39.7 billion by 2025. The market size figures given by Allied Market Research [MA-17] are more conservative. They project the DLT market size to reach \$5.43 billion by 2023 resulting in a CAGR of 57.6% from 2018 to 2023. The market size estimates from Grand View Research [MA-18] are closer to the estimates of Markets and Markets, with a market size estimation of 37.6 billion in 2025 with a CAGR of 69.4%.

### ***DLT Regional market size***

Within the DLT market, Allied Market Research [MA-17] predicts North America to hold the largest market share within the period up to 2023 due to key companies in the region. Advancements in internet payments are expected to boost the growth in China, Japan, South Korea, India, and other Asian companies. On the other hand, Europe occupied the second highest market share of 30% in the global DLT market. Blockchain technology is of increasing interest to citizens, businesses, and legislators across the European Union. Transactions in Europe are often fast, cheap, and secure enough for most purposes. Supporters of blockchain applications often see additional benefits in its transparency and immutability.

### ***DLT Segment overview***

#### **Private & public**

Two main segment types can be recognized, namely, private and public blockchains. A private blockchain is a shared database or ledger that is secured by traditional security techniques, such as limited user rights, and writing permissions are kept centralized to a single organization, providing more opportunities for B2B use cases. On the other hand, a public blockchain is a transparent database of transactions on an open network (an example of a public blockchain is Bitcoin) and is often used when a network needs to be decentralized. Figure 93 illustrates global DLT market (by type – left – and end-users – right).

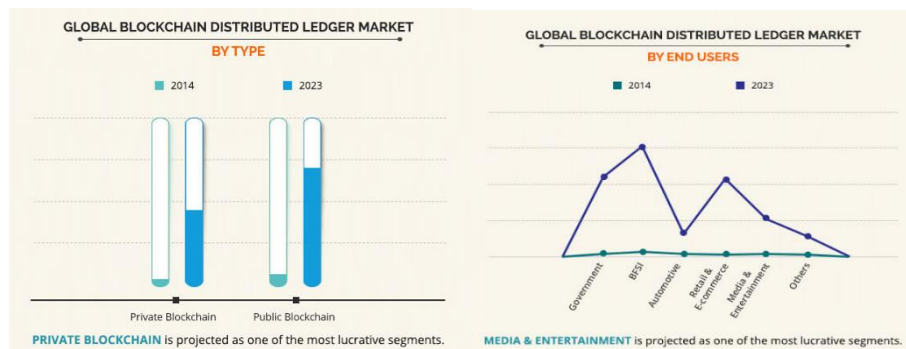


Figure 93. Global Blockchain DL by Type and End-users [MA-17]

### **Applications**

When the blockchain market is categorized by end applications the BFSI (Banking, Financial Services, and Insurance), automotive, retail & e-commerce, media & entertainment and other segments can be distinguished. The BFSI segment dominated the global market, in terms of revenue, and is expected to keep this market domination. This market segment has realized the significance of the blockchain technology for secure transactions between and with customers. Within the BFSI segment a worldwide rapid growth is expected mainly due to high compatibility with the financial services industry ecosystem, rising cryptocurrencies and Initial Coin Offerings (ICOs), rapid transactions and reduced total cost of ownership, reduced chance of theft and improved anonymity. Due to the risk of technical flaws, lack of awareness about crypto currency and limited acceptance growth may be less than expected. Government and retail & e-commerce segments are anticipated to grow at a significant rate during the forecast period.

### **Component insights**

Infrastructure and Protocol providers develop software building blocks, which are needed to deploy blockchain networks. GVR predicts that the rising demand for the blockchain protocol such as Ethereum, Hyperledger, Openchain, BigChainDB and open-source protocols are a major factor to support the growth of this segment. These protocols help developers to create customized DLT networks for users. Games developed based on the block chain protocol like CryptoKitties, Spells of Genesis or EtherWarfare are expected to support the infrastructure & protocol growth.

## **5.1.4 Market Drivers**

### **5.1.4.1 Adopting IoT-solutions**

IoT solutions are going to change our lives in the nearest time already, yet they set the challenges which are going to be faced and handled. Right now, the clear majority (91%) of companies are struggling to overcome

persistent barriers to transformation. A survey conducted by Dell Technologies [MA-19], among its business partners, found that the top 5 main barriers to entering the digital transformation were:

- Concerns about data privacy and security 34%
- Lack of budget and resources 33%
- Lack of the right internal skills and expertise 27%
- Regulation & legislative changes 24%
- Immature digital culture 23%

As it can be observed, privacy and security were the most burning problem, and it offers opportunities for companies and specialists from different spheres. Many customer surveys reveal that customers are even willing to pay extra to make sure their safety concerns have been addressed. It is the aspect with the most weight. When looking for application development services on the IoT experts will play an important role, with enough experience and expertise and eager to ensure the correct level of security of the solution created.

### ***Final user needs: End-to-end trustworthiness***

The impact of IoT on the end-user, society and the value chain are unprecedented, and, given the scale of IoT and the complexity of an end-to-end solution, it requires end-to-end reliability, including security, privacy, safety, control and management of equipment and information. End-to-end reliability is therefore fundamental from a technical perspective, but also for the existence of the value chain itself, so that alliances and partnerships can be created based on trust between the stakeholders involved.

### ***Drivers to meet final user IoT trustworthiness***

A tremendous effort has already been put into the EC-sponsored research programs "Trust in the IoT". This effort has yielded significant results, consolidating European expertise in IoT reliability and delivered several solutions that have already become part of IoT products on the market. However, they are far from finding definitive answers to IoT reliability. NG-IoT solutions are evolving rapidly, with unprecedented opportunities and challenges, and trust in these ubiquitous technologies must be continuously assured. Artemis mention in their IoT-SoS-Whitepaper [MA-2] that many technology issues remain open, including:

- Hardware solutions for trust.
- Protection of IoT devices to prevent IoT entry doors to systems for hackers and identity theft.
- Security, privacy protection, safety, reliability, and societal acceptance of IoT and SoS.
- Promote a "Trusted IoT label" defined by the EC.
- Solutions for trustworthy AI-based systems.
- Blockchain for decentralised IoT application and SoS.
- Blockchain-based solutions and blockchain-enabled integrated access management.
- IoT trust awareness and training.
- Distributed M2M business platforms, nano payments, trusted logs, and secure monetisation.
- Self-X trust technologies.
- Trust by design.
- Trust composability.
- Trust in SoS integration.

### ***Barrier: key market***

Energy consumption would increase enormously because of the expected NG-IoT evolution with the growing need for edge/fog computing, hyper-connectivity, 5G networks and the large number of new energy-consuming datacentres. All of this puts a heavy strain on our carbon and energy-consuming footprint. This means that if something does not change within the IoT evolution in the field of energy consumption, an energy-intensive consumption process is set in motion, with a high energy and CO<sub>2</sub> footprint. On the other hand, geopolitical barriers and constraints can be used to prevent our global and local substantial sustainability goals from not

being achieved. Nowadays there are already movements at a local level that are incensed that the total locally generated green electricity is completely consumed by energy-guzzling data centres.

#### 5.1.4.2 Edge Computing market drivers

As it has been explained in previous sections, edge computing is an important driving factor in the NG-IoT evolution. Edge computers will be used indefinitely; remember that it will be the conditions in which they operate will be the driving factors for this new field in application technologies such as:

- *Data mobility and connectivity:* Edge technologies will mainly be applied where we can limit or require interactive connectivity to the cloud for services such as computing, storage, backup, and analysis.
- *The need for real-time decision making:* With these edge use cases, it is desirable that data is processed immediately, such as with self-driving cars or automatic cranes in civil infrastructures. These devices and platforms need to be able to perform analytics locally, without sending data to the cloud first, so decisions can be made rapidly.

Consequently, the key edge computing market drivers for NG-IoT adoption are:

##### ***IoT data***

Most IoT devices are currently sending their collected data to the cloud. This creates an enormous amount of data that is generated in the cloud, which entails high storage and management costs. In many cases, this data is centrally processed, analyzed and, if necessary, sent back to the IoT device. There is a need to keep data storage and processing closer to the edge and only push relevant and critical data to the cloud. This saves a lot of time because the round trip to the cloud is no longer necessary and a decision can be made right at the edge. All of this is the driving force behind the productive growth of Edge computing. The general expectation is that between 45% - 55% of that IoT data will be stored, analyzed, and acted on at the edge<sup>110</sup>. At the same time, Gartner predicts Edge data will comprise 75% of enterprise data by 2022, up from 10% in 2018<sup>111</sup>.

##### ***Market needs***

IoT technology has already been widely embraced and implemented by many market segments such as: hospital, retail, manufacturing, home automation, drones, agriculture. The importance will only increase and with it the value of edge computing. The real-time response of IoT edge computing is one of the main drivers that will play an important and crucial role in: industrial IoT automation, the growth of autonomous vehicles, mission-critical applications such as oil and gas extraction, and the energy and utility market.

##### ***IoT-Edge computing adoption***

The growth of edge computing is strongly fueled by the market growth of components (hardware, software, and solutions) and applications (IoT, data caching, analytics, environment monitoring, AR, location services and others). The gateway is an important link as a central link at the edge of the IoT architecture, between the sensors and the cloud, for the management of the data upstream and downstream. In the simplest architecture, the edge gateway stores data from the sensor, stored in the local database. The function of the edge gateway will in many cases consist of sending data in batches to the cloud and edge computing for data processing, running AI and ML algorithms to predict future behavior. The availability of innovative and custom software and applications for edge networks will accelerate the adoption of edge computing. Cloud providers such as Amazon and Microsoft are major players delivering optimized edge application software that supports the edge computing gateway in multiple sensor and network protocols, lightweight ML, and AI. In addition, the use of 5G is expected to finally boost the adoption of edge computing in networking.

#### 5.1.4.3 Artificial Intelligent market drivers

AI is an important driving factor in the evolution of NG-IoT and will drive the demand for the digital (Edge/Fog) computing power, data technology, communication, and digitization of the various industries worldwide. AI market is segmented based on:

<sup>110</sup> [https://medium.com/@mobodexter\\_inc/key-drivers-of-the-edge-computing-market-a9bdb770878e](https://medium.com/@mobodexter_inc/key-drivers-of-the-edge-computing-market-a9bdb770878e)

<sup>111</sup> <https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/>

- *Solutions:* hardware (HW), software (SW) and services
- *AI technology uses:* adaptive learning, deep learning, machine learning, natural language processing, machine vision and computer vision.
- *End User:* Healthcare, BFSI, Law, Retail, Advertising or Media, Auto & Transportation, Agriculture, Manufacturing, and others.

Within healthcare, AI will play a crucial role in analysing of different types of diseases, diagnosing, and tracking and predicting the health status of patients. But will also be applied in scientific research into new types of medicine. This is expected to give a boost in the better and faster development of medicines.

Among the key markets for AI explosion, it can be foreseen a growing need for analysing and interpreting large amounts of data, a growing adoption of IoT across industry verticals, and a growing investment in AI technologies, such as availability of EU funds, for supporting the digital transformation of the PA -through the adoption of disruptive technologies (including AI) -in line with EU priorities. On the contrary, key market restraints can be considered the lack of trained and experienced staff on AI industry, and that training AI are an energy-intensive process with a high carbon footprint. Advances in AI are possible thanks to the powerful GPU we have today, these GPUs typically consume a lot of electricity. According to NVIDIA, the maximum power dissipated by a GPU is equal to 250W, which is 2.5 times higher than that of the Intel CPU.

#### 5.1.4.4 Distributed Ledger Technology market drivers

Market drivers for DLT successful adoption in NG-IoT systems could be explained because of being solutions that contribute to the fundamental support and reliability of IoT device protection, to prevent IoT entry doors to systems for hackers and identity theft, security, privacy protection, safety, human interaction, and social adoption of IoT solutions. However, due to the risk of technical flaws, lack of awareness about crypto currency and limited acceptance growth may be less than expected, as well as the lack of trained and experienced staff is for the time being expected.

### 5.1.5 Competitive landscape

#### 5.1.5.1 Edge Computing Technology landscape

The following chart delivers a comprehensive analysis of the components segment including services, solution, platform, software, and hardware.



Component	Technology	Description	Maturity	Typical vendor(s) or solutions
Connectivity	Network Virtualization	Abstracts network elements & resources into a logical virtual network that runs independently on top of a physical network	Early adopter	Oracle, VMWare, Juniper Networks
Connectivity	5G	The fifth generation of cellular networks, commercially launched in 2019	Early adopter	Huawei, Ericsson, Nokia
Connectivity	Wifi 6	The newest version of the Wi-Fi protocol, also known as IEEE 802.11ax	Early adopter	Qualcomm, Cisco, Huawei
Connectivity	TSN	Time-Sensitive Networking is a set of standards defined by IEEE for the time-sensitive transmission of data over deterministic Ethernet networks	Early adopter	ABB, Bosch, Cisco, Siemens
Connectivity	6G	The sixth generation of cellular networks	Emerging	Huawei, Ericsson, Nokia
Connectivity	WLAN	Wireless Local Area Networks, includes Wi-Fi and its different versions	Mainstream	Cisco, Aruba, Extreme Networks
Connectivity	WPAN	Wireless Personal Area Networks, incl. very short-range (up to ~100 m) connectivity technologies (e.g. BLE, Zigbee)	Mainstream	DiGi Int., NXP Semiconductors, Silicon Labs
Connectivity	Cellular IoT (2G/3G/4G)	Provides connectivity to IoT applications via traditional cellular networks	Mainstream	China Mobile, Vodafone, Orange
Connectivity	WNAN	Wireless Neighborhood Area Networks, includes medium-range (~500-2,000 km) mesh connectivity technologies based on the IEEE 802.15.4 standard (e.g. Wi-SUN)	Mainstream	Itron/Silver Spring Networks, Wirepas
Connectivity	LPWAN	Low-Power Wide-Area connectivity for IoT applications (e.g. Sigfox, LoRa, NB-IoT, LTE-M)	Mainstream	Semtech, Sigfox
Connectivity	Pub/Sub	Form of asynchronous service-to-service comm. used in IoT messaging protocols e.g. MQTT, XMPP	Mainstream	Amazon-AWS, Google Cloud, PubNub
Connectivity	eSIM	A SIM-card embedded into mobile devices that enables remote SIM provisioning, allowing storing of multiple operator profiles simultaneously and switching between them remotely.	Mainstream	ST Microelectronics, Gemalto, Giesecke & Devrient, ARM
Connectivity	Lifi	Wireless communication technology that uses light to transmit data.	Mainstream	Panasonic
Connectivity	Satellite IoT	Provides connectivity to IoT applications via satellite networks	Mainstream	Iridium, Inmarsat, Eutelsat
Connectivity	APL (Advanced Physical Layer)	Developing industrial Ethernet standard that seeks to leverage the work of the IEEE 802.3cg (10BASE-T1L) task force to achieve a single twisted-pair industrial Ethernet standard for hazardous areas	Mainstream	Pepperl+Fuchs, Endress+Hauser, Analog Devices
Hardware	Neuro-synaptic chip	Brain-inspired computer chip, in which transistors simulate neurons and synapses	Early adopter	IBM
Hardware	Quantum computing	Computation using quantum-mechanical phenomena e.g., superposition entanglement	Emerging	IBM, Microsoft, Rigetti
Hardware	CPU	Central processing unit	Mainstream	Intel, HPE, AMD
Hardware	Security chips	Security-enhancing low-powered modules, include various security-sensitive functions	Mainstream	Apple, Alphabet
Hardware	Edge gateways	Physical devices that serve as the connection point between the cloud and controllers, sensors and intelligent devices	Mainstream	Dell, HPE
Hardware	GPUs	Graphic processing unit	Mainstream	NVIDIA, AMD, Asus, Intel
Hardware	NAND	Non-volatile flash memory	Mainstream	Micron, Samsung, Toshiba
Hardware	ASIC	Application-specific integrated circuit	Mainstream	Fujitsu, Honeywell, Advanced Linear Devices
Hardware	DRAM	Dynamic random-access memory	Mainstream	Samsung, Micron, SK Hynix
Hardware	FPGA	Field programmable gate array	Mainstream	Xilinx, Intel, Altera
Hardware	Smart sensors	Sensors that take some predefined action when they sense the appropriate input	Mainstream	Texas Instruments, TE Connectivity, Broadcom
Hardware	ML-optimized gateways	Controllers that are optimized for ML algorithms	Mainstream	Adlink, Intel
Hardware	Energy harvesting for LPD	Supplying electricity to LPDs from one or several forms of available energy from the ambient environment instead of using disposable batteries or a connection to the electricity grid	Mainstream	STMicroelectronics, ABB
Hardware	Cloud-connected sensors	Sensors that are sending data directly to the cloud	Mainstream	Schneider Electric
Software	IoT Marketplaces	A one-stop click-and-buy-store, offering complete Internet of Things solutions ready to deploy smart applications including hardware, software, and cloud connection.	Early adopter	PTC, Siemens, ABB, Schneider Electric, Inductive Automation
Software	Digital Twins	Digital representation of physical assets, processes, systems, and devices	Early adopter	GE, Azure, Siemens, Honeywell, Emerson
Software	Container Security	Solutions that protect the integrity of containers	Early adopter	Cloud Vendor Solutions, Palo Alto Networks
Software	IoT Security platforms	Platform offering security solutions for any IoT device class	Early adopter	Mocana, Bayshore Networks, Device Authority
Software	Real-time database	Database that uses real-time processing to handle constantly changing workloads	Early adopter	MongoDB, Couchbase
Software	Serverless / FaaS	Developing, running, and managing application functionalities without the complexity of building and maintaining the infrastructure associated with developing and launching an application	Early adopter	AWS Lambda, IBM OpenWhisk, Google Cloud Functions
Software	Deep Learning	Part of a broader family of machine learning methods based on artificial neural networks	Early adopter	TensorFlow, Apache Mahout, Caffe, Deepmind, CuriousAI
Software	Cloud computing	Using a network of remote servers to store, manage, and process data.	Mainstream	AWS, Microsoft Azure, Alibaba Aliyun
Software	IoT Platforms	Form of modular software that allows easy connection of various IoT devices & other value-added functionality (e.g. remote device management, application enablement, analytics)	Mainstream	AWS IoT, Microsoft Azure IoT, PTC Thingworx
Software	Edge analytics	Collection and analysis of data at the sensor, device, gateway or edge data center rather than waiting for the data to be sent back to a remote cloud.	Mainstream	AWS IoT Greengrass, Microsoft IoT Edge, Foghorn, Crosser
Software	IoT-based streaming analytics	Real-time processing of streaming of data from IoT devices	Mainstream	Cloud vendor solutions, Hortonworks Dataflow, SAS, Software AG
Software	Supervised machine learning	ML method where training data for the algorithm includes desired outputs.	Mainstream	Uptake, Sparkcognition, Senseye
Software	Containers	Containers are processes with their own virtual resources and filesystems (memory, CPU, disk, etc.), isolated from other applications and containers	Mainstream	Docker, Kubernetes, OpenShift

Figure 94. Competitive IoT Edge Computing Technology [MA-20]

### 5.1.5.2 Global Market Key Players for Edge Computing Market

The global edge computing market is dominated by key players such as: Cisco, HPE, Huawei, IBM, Dell Technologies, Ericsson, Nokia, Litmus Automation, Amazon Web Services (AWS), FogHorn Systems, SixSq, MachineShop, Saguna Networks, Vapor IO, ADLINK, Altran, Axellio, GE Digital, Moxa, Sierra wireless, Digi International, Juniper Networks, Clearblade, EdgeConneX, Edge Intelligence, Edgeworx, AT&T Inc., Fujitsu Limited, Microsoft Corporation, Intel, Huawei Technologies Co. Ltd.

### 5.1.5.3 Artificial Intelligence Competitive analysis

The main market leaders in AI include Alphabet (Google), Apple, Albert Technologies, Amazon, Baidu, IBM, IPsoft, Microsoft Corporation, MicroStrategy, NVIDIA, Salesforce, Sentient Technologies Holdings, Qlik Technologies and Verint Systems (Next IT). In the period 2015 to 2018, the main strategies of these players focused on product launches, acquisitions, and partnerships.

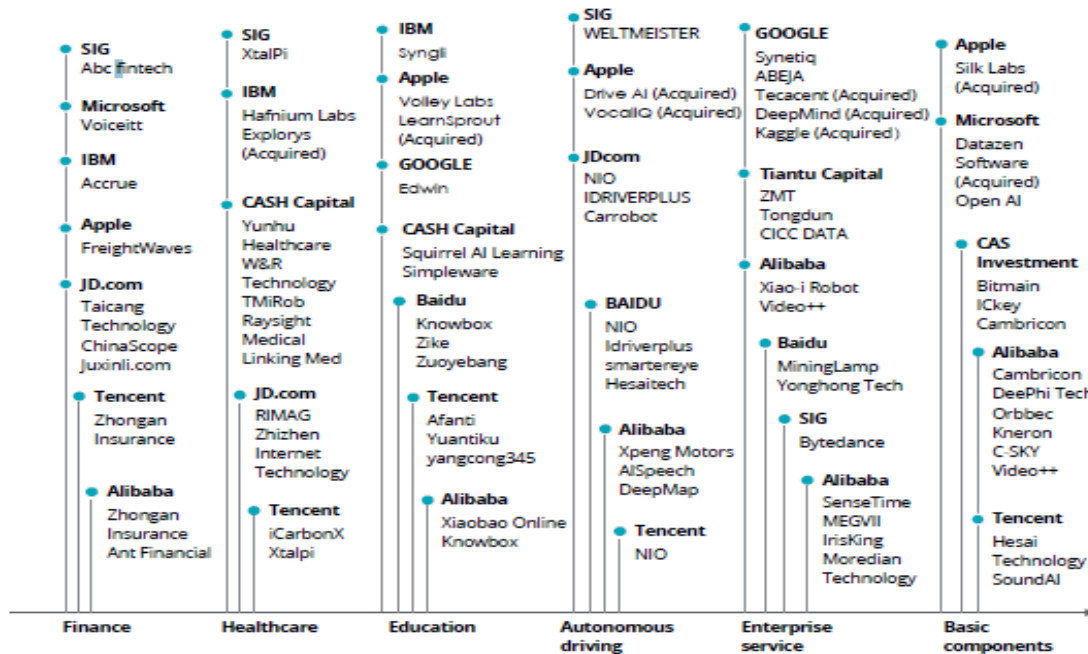


Figure 95. Major fields of investment by leading AI enterprises [MA-21]

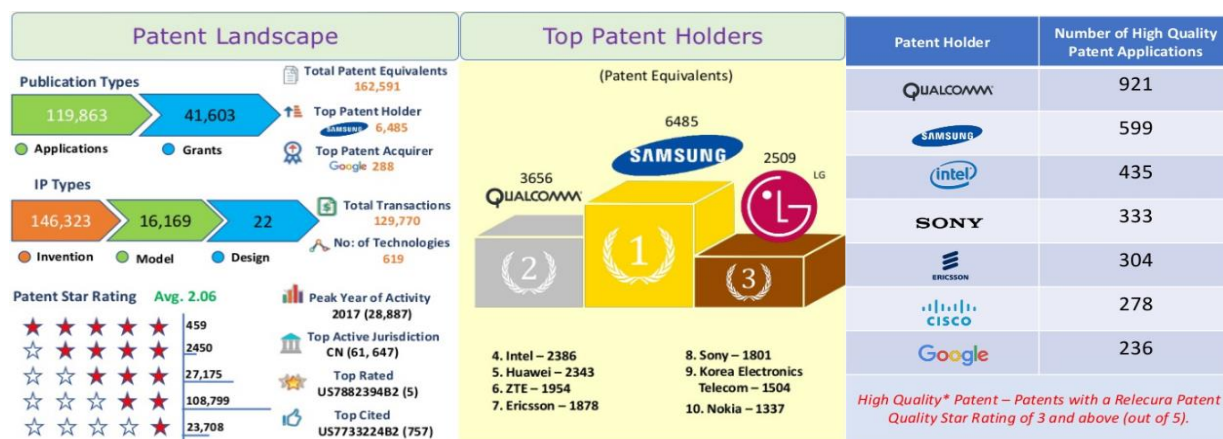
### 5.1.5.4 Global DLT market key players

Key players in the global blockchain market are IBM, AWS, Microsoft, SAP, Intel, Oracle, Bitfury, Cegeka, Earthport, Guardtime, Digital Asset Holdings, Chain, Huawei, BlockCypher, Symbiont, BigchainDB, Applied Blockchain, RecordsKeeper, BlockPoint, Auxesis Group, BTL Group, Blockchain Foundry, AlphaPoint, NTT Data, Factom, SpinSys, ConsenSys, Infosys, iXLedger and Stratis.

### 5.1.6 The IoT global intellectual property landscape

According to studies by Relecura<sup>112</sup>, Moeller Ventures [MA-22], and others, on the IP landscape, it is clearly emphasized that the best patent holders belong to various sectors, such as consumer electronics (Samsung, LG, Sony), telecom (Huawei, Ericsson, Korea Electronics Telecom, ZTE) and software (IBM, Microsoft). The patent-filing trend is characterised by steady growth until 2015- 2017, with a consistent reduction in the following years that is coherent with the IoT hype cycle. China, USA, Korea, Europe, and Japan account around the 75% of the patents filed. With more than 10,000 patents, Samsung is the major patent holder, covering many technological areas of IoT and many IoT vertical applications. The second position is occupied by Qualcomm, with around 9000 patents: Qualcomm is the major patent filer in multiple jurisdictions and the major PCT filer. A group of large companies, including Qualcomm, LG, Huawei, and Intel, follows with several patents between 2200 and 1700 patents while a larger group, including Sony, Ericsson, Nokia, Siemens, NEC, Panasonic, Philips, CISCO, Microsoft, IBM, Fujitsu are positioned in the range of 1700-600 patents. The top 10 of high-quality patents applications holders are: Qualcomm, Samsung, Intel, Sony, Ericsson, Cisco, and Google.

<sup>112</sup> <https://relecura.com/2017/05/18/iot-patents-landscape-commercialization-trends-report/>

Figure 96. Global IoT Patents landscape <sup>112</sup>.

According to these studies, consumer electronics is the largest vertical application domain covered by patents, followed by industry and telecom, and the automotive sector behind. From a technology perspective, networking is the most discussed topic (with over 80,000 patents), followed by discovery (around 50,000), security (40,000), power management (30,000), data analytics (25,000), data storage (7000) and cloud computing (5000).

Rank (based on # of equivalents held)	Home	Utilities	Factory Automation	Automotive	e-commerce	Health	Wearables	Agriculture	Mining
1	SAMSUNG(1386)	STATE GRID CORPORATION OF CHINA (SGCC)(530)	STATE GRID CORPORATION OF CHINA (SGCC)(227)	SAMSUNG(308)	SAMSUNG(391)	SAMSUNG(401)	SAMSUNG(250)	SAMSUNG(27)	HALLIBURTON(64)
2	HUAWEI(826)	LG(406)	SIEMENS(205)	GM(204)	QUALCOMM(202)	PHILIPS(187)	INTEL(71)	ZHEJIANG UNIVERSITY(24)	CHINA UNIVERSITY OF MINING AND TECHNOLOGY(50)
3	ZTE(726)	QUALCOMM(294)	QUALCOMM(121)	HYUNDAI(172)	NOKIA(98)	GE(83)	QUALCOMM(53)	CHINA AGRICULTURAL UNIVERSITY(15)	SCHLUMBERGER(44)
4	LG(686)	SAMSUNG(291)	SAMSUNG(118)	TOYOTA(160)	SONY(97)	QUALCOMM(77)	PHILIPS(49)	NANJING AGRICULTURAL UNIVERSITY(15)	BAKER HUGHES(25)
5	ERICSSON(460)	INTEL(201)	ABB(113)	CONTINENTAL(136)	LG(83)	COVIDIEN(67)	LG(48)	WUXI TONGCHUN NEW ENERGY TECH(15)	ANHUI UNIVERSITY OF SCIENCE AND TECHNOLOGY(24)
6	SONY(384)	KOREA ELECTRONICS TELECOMM(177)	INTEL(90)	DENSO(126)	INTEL(81)	SIEMENS(67)	MICROSOFT(46)	JOHN DEERE(13)	SHELL(17)
7	QUALCOMM(373)	SIEMENS(154)	FISHER ROSEMOUNT SYSTEMS(82)	FORD(118)	CISCO(75)	HILL-ROM(61)	KOREA ELECTRONICS TELECOMM(44)	HUSQVARNA(11)	SELMAN AND ASSOCIATES LTD(9)
8	PANASONIC(330)	ERICSSON(140)	ROCKWELL AUTOMATION(82)	BOSCH(95)	IBM(73)	MEDTRONIC(56)	SONY(32)	SOUTH CHINA AGRICULTURAL UNIVERSITY(11)	UNANIMOUS A I INC(9)
9	NOKIA(309)	CISCO(136)	NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS(69)	QUALCOMM(87)	AUTOCONNECT HOLDINGS LLC(71)	INTEL(51)	NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS(30)	GOOGLE(10)	STIMLINE AS(8)
10	KOREA ELECTRONICS TELECOMM(291)	SONY(124)	ZTE(67)	GE(81)	HUAWEI(70)	MICROSOFT(38)	SOUTHEAST UNIVERSITY(30)	IROBOT(9)	XIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY(8)

Figure 97. Global IoT Company Patens ranking <sup>112</sup>.

## 5.2 Verticals addressed in ASSIST-IoT

### 5.2.1 Port automation – Maritime logistics

#### 5.2.1.1 Problems and needs

When one talks about the health of the port and shipping sector, they start with volumes and growth, since so much of the total cost of production is tied up in large, expensive fixed assets. Volume growth leads to many good things: mounting revenues, high asset utilization, approvals for new investments, good pricing behavior among competitors, and win-win relations between management and labor. Bad things happen when you do not have growth. Historically, the maritime sector has done well—with short-term cyclicalities but consistent expansion over time. In the 1950s, trade started to grow faster than GDP, and in the 1980s it really took off, growing twice as fast as GDP and sometimes faster. However, this trend has changed lately. Demand is not increasing as fast as it was. GDP growth has slowed down, while the trade multiple—the ratio between GDP and trade—has fallen to one, as shown in Figure 98 [MA-23]. Therefore, an extraordinary turn of events would be needed to get the trade ratio back above two.

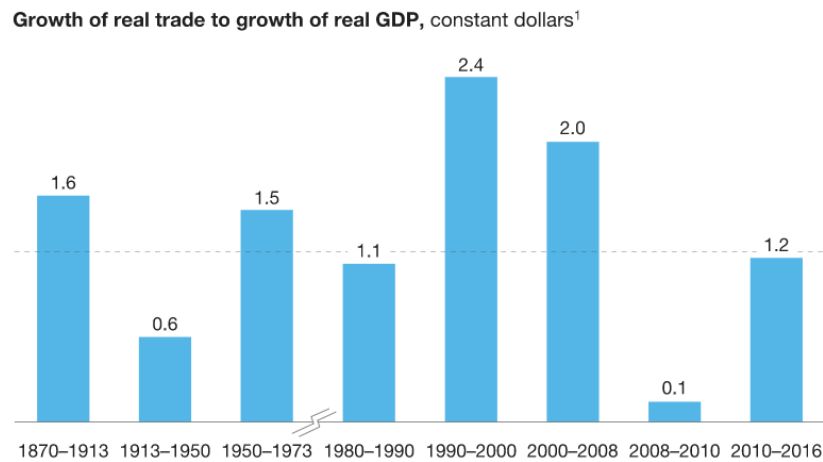


Figure 98. Growth of real trade to growth of real GDP [MA-23].

Ports, terminals, and port-service firms have responded to lower growth by investing in cranes, dredging equipment, and other things to accommodate the larger vessels. Some of the investments replace older assets, but mostly they increase capacity—or supply. However, two additional complications are raising.

1. Shipping alliances, as a means of capacity and service rationalisation, are further concentrating international maritime flows along particular routes, decreasing number of ports of call. Considering the schedule low reliability problems (fluctuating between 25-95% within 2018 [MA-24]) less ports are being required to serve more ships, while at the same time trying to manage in a more efficient way the delayed ship arrivals.
2. The dimensions (and resultant capacity) of ships are permanently increased. The average size of new containerships delivered has increased from 1,100 TEUs in the 1970s to 7,700 TEUs ordered today [MA-25]. The impacts of this trend are to be felt by all ports, as cascading of 14,000+ ships are expected to be deployed on the major lines, with up to 8,000-10,000 TEUs ships in the secondary ones, also impacting feeder operators due to increased transshipment times. Bigger ships mean bigger volumes unloaded and assuming similar small time-windows, this will lead to transferring congestion pressures towards the hinterland connections (road and rail). Therefore, the efficiency challenge becomes also relevant for medium and small ports, which will have to address it with limited resources and capabilities.

As technological gaps are among the main sources of inefficiencies across ports, during the last decade a strong drive towards the automation of port operations supported by new handling technologies and equipment, information systems (PCSs, TOSs, etc.) is being witnessed [MA-26]. Container ports seem ideal places to automate. The physical environment is structured and predictable. Many activities are repetitive and straightforward. They generate vast amounts of readily collected and processed data. Better still, the value from automation includes not only performance efficiency but also cost and safety gains for ports and the companies that do business there.

### 5.2.1.2 Existing solutions

The first automated container port was developed in Europe in the early 1990s. Since then, many ports have installed equipment to automate at least some of the processes in their terminals. Automation has five main components in ports. They can create value by implementing each component individually but will unlock the full benefit only if all five are integrated and coordinated:

- **Automated decision making (yard management):** Account for the earliest implementations of automation since they improve terminal managerial aspects and the performance of existing assets without automating them. This can involve berth planning, stowage and yard planning, or inland

predictability. By 2015, about 40% of the world's container terminals were using a form of automated decision making<sup>113</sup>.

- **Automated gates:** A basic Gate Automation System (GAS) must be capable of identifying and recording driver (via Driver Identification System – DIS), truck (via License Plate Identification System – LPIS – through OCR), and container (via Container Number Recognition System – CNRS with OCR technology as well) components accurately and promptly. Container terminal gates involved several transactions and were thus among the earliest terminal assets to be automated.
- **Automated tracking and tracing:** Focus on a higher level of integration of the components of terminal operation such as ships, cranes, containers, and yard equipment by accurately pinpointing their location within the terminal. Although GPS can be used, the placement of reference nodes across the terminal provides a higher level of positioning accuracy and are widely deployed in several ports around the world.
- **Automated yard and quay cranes:** Since the stacking of containers in a yard is an asset-intensive activity requiring the frequent movement of cranes, there is a high incentive to automate the process. Automated yard cranes (or automated stacking cranes; ASC) can store and retrieve containers along a stacking area automatically. Cranes are usually the most capital-intensive superstructure in a port terminal. The growing size of ships has placed pressures to improve ship to shore productivity, and automated quay cranes are starting to be introduced. The best estimates suggest that at least 10 billion has been invested in basic infrastructure and automation equipment in such projects. The momentum will probably accelerate: an additional \$10 billion to \$15 billion is expected over the next five years [MA-27].
- **Automated horizontal transport:** Involves the use of AGVs to move containers within the terminal. The most common use involves the transfer of containers from pier-side crane operation to yard storage. This is a complex operation due to the high number of containers moves, particularly in high throughput terminals.

As it can be observed in the figure below, their diffusion within port terminal varies among the different categories. While automated yard, gate and tracking management is already wide established in the industry, horizontal and cranes automation is still in its infancy.

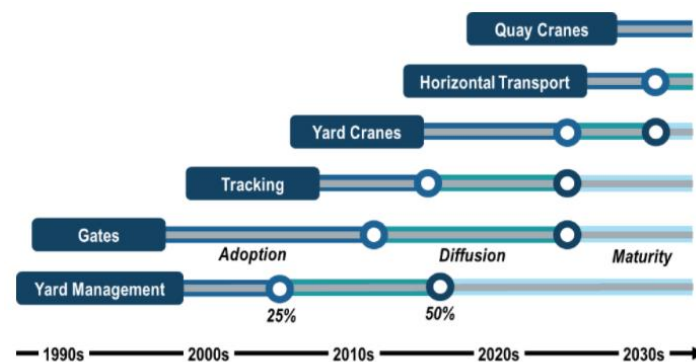


Figure 99. Diffusion of key port terminal automation technologies<sup>113</sup>

### 5.2.1.3 Customer segment and end-users

The transport industry spans all actors related to the production and provision of transport services including transport companies and supplementary businesses. The goods are transported along nodes where they are handled and often transferred from one mode to another such as road, rail, or sea. The maritime transportation industry stakeholders can be listed as:

**Consigner (also called shipper/seller/exporter) and Consignee (also called buyer):** The consigner is the party which by contract sends goods from one place to another, and the consignee is the party to which the goods are

<sup>113</sup> <https://porteconomicsmanagement.org/pemp/contents/part3/terminal-automation/diffusion-port-terminal-automation-technologies/>



consigned. Shippers are responsible for loading, closing, and sealing of the cargo container. Shippers and consignees are the most numerous actors in the transport chain and are normally SMEs.

**Freight forwarders:** A freight forwarder picks up, hub-handles and ground handle the goods and transports it to the port, where the cargo needs to go through customs clearance before it is loaded onto a ship by the terminal operator. From the shipper's perspective, the freight forwarder is usually responsible for all aspects of the container transportation from the origin to the destination.

**Shipping lines:** The shipping lines accommodate the transport and reports to the necessary authorities about its arrival and cargo.

**Customs and regulatory authorities:** Customs and regulatory authorities are not directly involved in the physical transportation of containers but supervise the cargo and information flow in order to detect unlawful acts that could harm the security and safety of the supply chain.

**Terminal operators:** Terminal operators handle the logistics of containers between ships and other modes of transportation. Loading and unloading of container ships are mostly done by private companies which are also often responsible for the terminal operations, infrastructure, and IT systems. In that sense, and within ASSIT-IoT context, containerized port traffic (today mostly handled by global terminal operators such as COSCO Shipping Ports, China Merchant Port Holdings, PSA International, Hutchison Ports, APM Terminals and DP World) of the top 5 container terminal operators together accounted for more than 50% of the total global throughput, reaching 748 million TEUs in 2016 [MA-28].

#### 5.2.1.4 Market size and growth

The first automated container port was developed in Europe in the early 1990s. Since then, many ports—more than 20 in the past six years—have installed equipment to automate at least some of the processes in their terminals. Almost 40 partly or fully automated ports now do business in various parts of the world, and the best estimates suggest that at least \$10 billion has been invested in such projects (most of them in China South-East Asia, and North-Western Europe, see Figure 100). The momentum will probably accelerate: an additional \$10 billion to \$15 billion is expected over the next five years [MA-27]. On the face of it, container ports seem ideal places to automate. The physical environment is structured and predictable. Many activities are repetitive and straightforward. They generate vast amounts of readily collected and processed data. Better still, the value from automation includes not only cost savings but also performance and safety gains for ports and the companies that do business there.

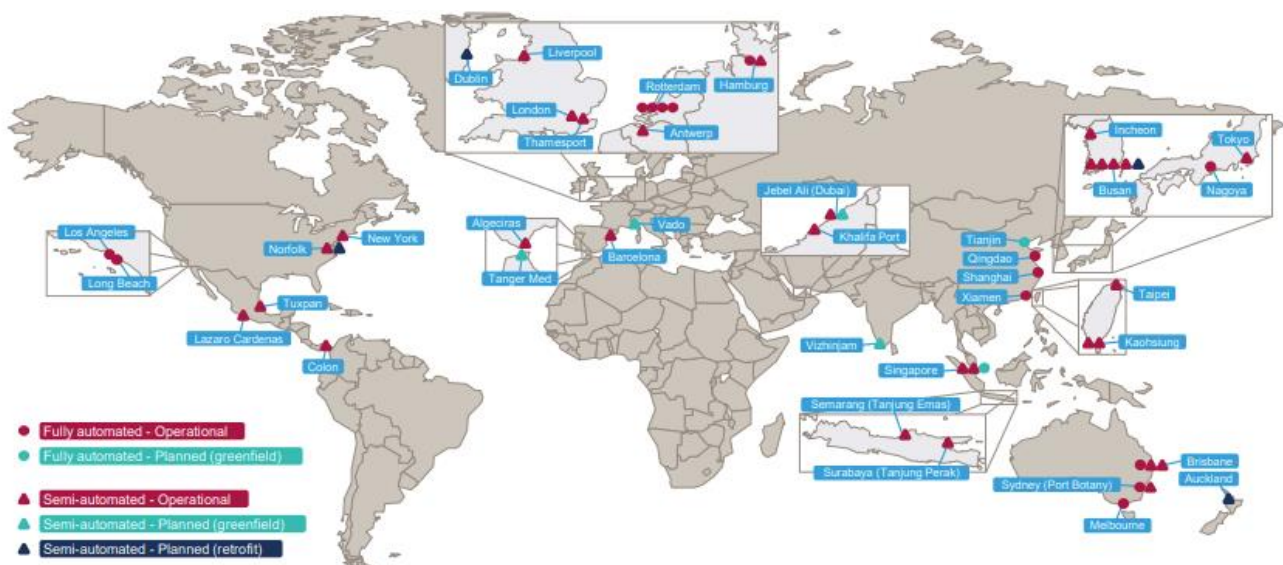


Figure 100. Existing and planned automated container terminals [MA-29]

To date, most of the 44 automated container terminals already in operation around the world have been developed as new projects, that is; built from scratch on a blank canvas. However, there are notable exceptions

where existing manual terminals have been retrofitted with automation as part of a major redevelopment, such as the case at terminals in Germany and the USA for example. With the number of greenfield terminal projects in the pipeline reduced, the opportunity to develop these terminals as automated facilities is similarly affected. However, the flip side of terminal operators' reduced interest in greenfield terminals is a much greater focus on optimising their existing terminals. Part of this may well involve consideration of conversion to semi or full automation, but how big is the potential global market for such retrofit terminal automation. Image below shows the proportion of existing container handling terminals worldwide that are automated. Of the 1,300 or so facilities, only just over 3% can be classed as automated. The natural focus for retrofit automation is the larger terminals around the world, of which there are over 300 not yet employing automation. While they are in the minority in terms of the overall industry total, they account for the vast majority of global throughput [MA-29].

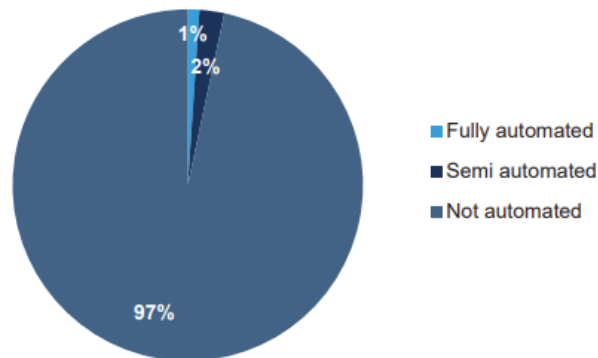


Figure 101. Proportion of automated container terminals worldwide [MA-29]

### 5.2.1.5 Barriers to entry

Nonetheless, ports are moving more slowly in automation than other industrial sectors with comparable complexities such as mining or warehousing. Responses to McKinsey survey suggest that the major barriers (in descending order of importance) are capabilities, data quality, siloed operations, and the handling of exceptions. Furthermore, investments in machinery have amortization periods of 10 years for light vehicles, 20 for semi-heavy cranes and 30 for large cranes. No business allows a drastic change in the process with these amortization periods pending during the lifetime of the equipment.

#### *A shortage of capabilities*

Respondents who had previous experience with automation say that the top problem is filling the specialized technical positions it requires. Moreover, even experienced engineers can take as long as five years to train. Many ports have apparently underestimated the challenge of acquiring the needed capabilities, especially in planning and implementation. Port and terminal operators must therefore step up their efforts to acquire talent and build these capabilities.

#### *Poor data quality*

Like organizations in other sectors, ports find that data silos and a lack of data standards are basic problems in automation. McKinsey survey indicated clearly that the quality of data and the data analytics is not sufficiently strong to run automated ports efficiently. The first reason is that the lack of a structured, transparent data pool makes it hard to monitor and diagnose the operations and performance of equipment quickly. Second, the standards, formats, and structures of the data may be misaligned or even wholly absent, so ports cannot collect and exchange data efficiently.

Data-infrastructure applications have huge potential. They can help to predict and forecast demand and the arrival-and-departure patterns of container ships. They can schedule the maintenance of equipment for optimal availability, allocate equipment and frontline staff, and adjust the allocation in real time. They can also use machine intelligence to make plans ever more accurate. Standardizing data so that they can be used in these ways will help to make ports and terminals more efficient. Ports are not only becoming more aware of this reality but are also starting to upgrade and harmonize their terminal operating systems. Nonetheless, the IT setups of most terminal operators remain fragmented.

### Siloed operations

Breaking down silos between functions is always a challenge, but it is especially difficult for ports: the basic principle of automation requires integration across the end-to-end terminal process chain and important interfaces. Automated ports, unlike conventional ones, cannot contain problems at individual functions or process steps. They must therefore ensure close collaboration among activities ranging from marine operations to crane movements to the control of yards and gates.

### Handling exceptions

Many ports find that exceptions are the greatest single challenge for raising productivity. More than 60% of the operators in McKinsey survey agreed that when ports have large numbers of exceptions, the likely culprit is a mistaken approach to automating manual processes. Such ports skip an important step: simplifying processes before automating them. These processes therefore remain cumbersome even after they are configured by automated systems.

## 5.2.2 Smart safety of Workers – Construction

### 5.2.2.1 Problems and needs

An accident at work is defined in ESAW (European Statistics on Accidents at Work) methodology as a discrete occurrence during the course of work, which leads to physical or mental harm. Fatal accidents at work are those that lead to the death of the victim within one year of the accident taking place. Non-fatal accidents at work are defined as those that imply at least four full calendar days of absence from work (they are sometimes also called ‘serious accidents at work’). Non-fatal accidents at work may result in a considerable number of working days being lost and often involve considerable harm for the workers concerned and their families. They have the potential to force people, for example, to live with a permanent disability, to leave the labor market, or to change job.

In 2018, there were 3.1 million non-fatal accidents that resulted in at least four calendar days of absence from work and 3,332 fatal accidents in the EU-27 (see Figure 102) [MA-30], a ratio of approximately 940 non-fatal accidents for every fatal accident. There was an increase between 2017 and 2018 in the total number of non-fatal accidents at work in the EU-27 (equivalent to growth of 0.3 %), as well as an additional 60 fatal accidents increase at work in the EU-27 during 2018 compared to a year before (equivalent to an increase of 1.8 %).

	Non-fatal accidents at work involving at least four calendar days of absence from work			Fatal accidents at work
	Total	Men	Women	
<b>EU-27</b>	<b>3 124 828</b>	<b>2 137 935</b>	<b>986 107</b>	<b>3 332</b>
Belgium	72 059	49 584	22 472	77
Bulgaria	2 255	1 530	725	87
Czechia	44 241	29 856	14 385	123
Denmark	50 185	30 338	19 643	37
Germany	877 501	652 992	224 062	397
Estonia	6 230	4 743	1 486	12
Ireland	18 090	11 542	6 478	34
Greece	4 493	3 137	1 356	37
Spain	465 227	327 385	137 842	323
France	771 837	469 791	302 046	615
Croatia	12 047	7 845	4 185	44
Italy	291 503	212 995	78 508	523
Cyprus	2 147	1 587	560	9
Latvia	2 168	1 413	755	30
Lithuania	3 834	2 398	1 391	37
Luxembourg	7 315	5 687	1 628	16
Hungary	23 510	14 926	8 584	79
Malta	2 001	1 607	394	4
Netherlands	91 179	54 849	36 331	45
Austria	63 229	49 393	13 836	124
Poland	77 949	50 152	27 797	211
Portugal	130 434	85 802	44 632	103
Romania	4 623	3 253	1 370	235
Slovenia	13 126	9 744	3 382	15
Slovakia	10 145	6 705	3 440	40
Finland	41 038	27 636	13 402	25
Sweden	36 457	21 041	15 416	50
United Kingdom	220 985	139 330	81 621	249
Norway	10 525	6 259	4 266	37
Switzerland	92 890	72 703	20 187	51

Figure 102. Fatal and non-fatal accidents at work in EU-27 in 2018 [MA-30].

Regarding gender analysis, men were considerably more likely than women to have an accident at work. In 2018, more than two out of every three (68.4 %) non-fatal accidents at work in the EU-27 involved men. Factors that influence these statistics are the proportion of men and women who are in employment, the different types of work that men and women carry out, the activities in which they work, and the amount of time spent at work. For example, there are far more accidents in the mining, manufacturing, or construction sectors, which tend to be male dominated. It is also generally the case that men tend to work on a full-time basis, whereas women are more likely to work on a part-time basis.

Regarding accidents from the point of view of working sector, within the EU-27, the construction, transportation and storage, manufacturing, and agriculture, forestry and fishing sectors together accounted for around two thirds (65.6 %) of all fatal accidents at work and more than two fifths (44.3 %) of all non-fatal accidents at work in 2018. It should be noted that between 2010 and 2018 there was a reduction in the number of fatalities at work in the EU-27 for all these activities in general (Figure 103). From the ASSIST-IoT perspective in particular, the largest absolute reduction in fatalities from accidents at work was in the EU-27's **construction sector**, with 317 fewer accidents in 2018 compared to 2010.

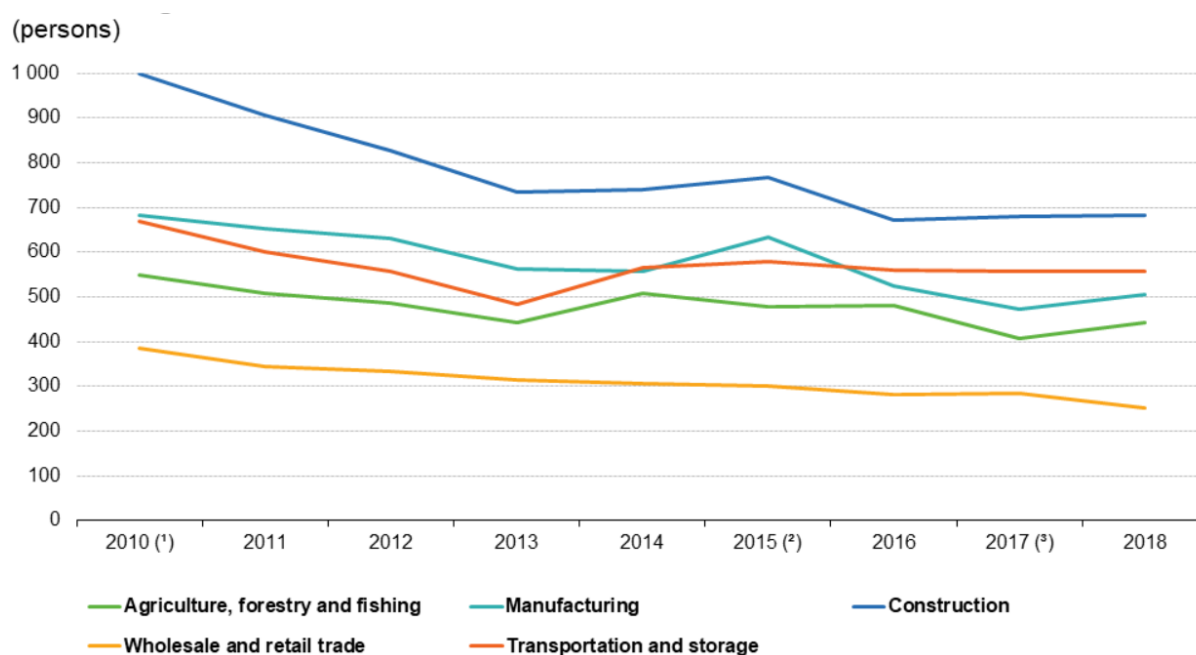


Figure 103. Fatal accidents trend at work for the five riskiest NACE sections in EU-27 from 2010 to 2018.

However, there is still a lot to do to improve safety at construction sites. **In 2018, 20.5 % of all fatal accidents at work in the EU-27 took place within the construction sector**, while the transportation and storage sector had the next highest share (16.7 %) (see Figure 104) [MA-30]. On the other hand, **non-fatal accidents** were relatively common within manufacturing (19.1 % of the total in the EU-27 in 2018), wholesale and retail trade (12.1 %), **construction (11.6 %)**, and human health and social work activities (10.8 %); these were the only European Classification of Economic Activities (NACE) sections to record double-digit shares of the total number of non-fatal accidents.

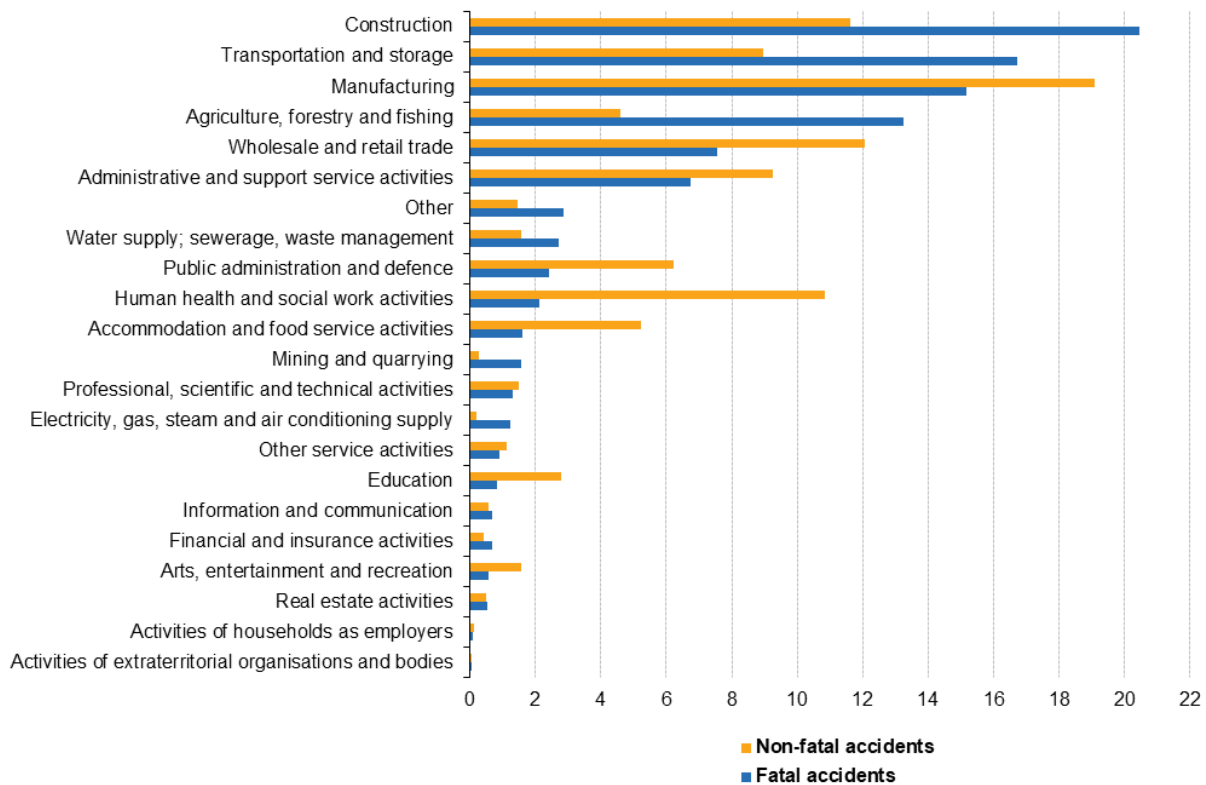


Figure 104. Percentage of fatal and non-fatal accidents at work in EU-27 in 2018.

Due to dynamic nature of construction site, uniqueness of each construction, and involvement of stakeholders, ensuring safety is challenging. Moreover, each worker has individual traits defined by health status, habit of body, preferences, and convictions. High latency of actuation and limited reliability can lead to tragic consequences. Thus, some issues may be addressed with the NG-IoT solutions envisaged in ASSIST-IoT:

- To increase computational capabilities for AI prediction of potentially dangerous situations and provide low-latency actuation.
- To develop innovative portable devices for industrial use providing prediction and detection of health issues (fatigue, stress, dehydration, etc.).
- To automate trusted data-sharing in such challenging environments.
- Reliable operation in changing working environment.

### 5.2.2.2 Existing solutions

The construction industry has already adopted some innovative technologies related to worker location tracking or warning signalisation. However, Occupational Safety and Health (OSH) performance remains on a low level. Some solutions are described below.

ELA Innovation is one of the dynamic leaders in the development of industrial wireless sensors and beacons, based upon a wide variety of long-range technologies like Active RFID and Bluetooth LE technologies. ELA Innovation offers solutions dedicated to protecting people's safety and security<sup>114</sup>. The localization solution is based on an extremely light infrastructure composed of router tags called **anchors**. These anchors, entirely battery-powered, offer a mesh communication network with several year autonomies. The positioning of the employee is done by localization of the **tag**. The mobile tags communicate with the platform thanks to a mesh network of anchors, connected to the cloud via **Gateways**, ensuring the connection between the local network and the cloud. The raw data collected by the tags are transformed into GPS data (latitude and longitude) by the Wirepas Positioning Engine tool and visualized on web application (see Figure 105).

<sup>114</sup> <https://elainnovation.com/security.html>





Figure 105. ELA innovation localisation suite. Anchors (left), tags (centre), and gateways (right).

**Extronics**<sup>115</sup> is the official industrial provider of AeroScout enterprise visibility solutions, which use standard Wi-Fi networks to provide data such as localization and status about assets and personnel in real time. The exact components may vary, depending on the type of site, size of project, and required system capabilities. The basic components include **active RFID tags**, which contain own batteries and transmit their ID signal at regular intervals, without needing external prompting. The active RFID tags can be used for tracking both assets and personnel; **tag excitors** use low frequency to trigger tags as they pass through, go into or out of a tightly defined area (e.g., a chokepoint, egress/entrance point, room, sub-room, bridge, stairwell). The tag excitors help set the exact location of people or assets, and even raise alarms if needed; **Wi-Fi access points** as core network infrastructure to pass wireless signals from tags to the network; and **MobileView software** enables to track, locate, monitor, and manage assets and personnel from a single platform.



Figure 106. AeroScout suite. Active RFID tags (left), Wi-Fi access points (centre), and MobileView software (right).

**nanotron**<sup>116</sup> is Germany company that provides electronic location awareness solutions. Nanotron's solutions deliver precise position data augmented by context information in real-time. In 2020, nanotron was acquired by Inpixon, a leader in Indoor Intelligence. Recognized as an industry leader in the Ultra-Wideband (UWB) market, nanotron's precision location awareness technology solutions enhance Inpixon's offering, homogenizing the positioning of people and assets, both indoors and outdoors. Together, nanotron's solutions and Inpixon's indoor data technology, sensors, video surveillance solutions, and GPS offerings, combine to deliver actionable indoor location data and intelligence. The following solutions are offered by Nanotron:

- Collision Avoidance (Proximity Detection between Vehicle/Personnel & Vehicle/Vehicle & Vehicle/Assets)
- Safety Zones (reduce fatalities around hazardous/heavy equipment).
- Real-Time Tracking (tracking of vehicles, people, and assets with an accuracy of <1m at 90% using Chirp-Technology and 10cm at 90% using UWB-Technology).

In a real-time location system, tags are wireless devices that send out blink packets to the infrastructure. These blinks are received by anchors, providing Time of Arrival and sensor data, that is forwarded to the location server for calculating tag positions. Together with anchors and nanoLES location servers, tags form the basis

<sup>115</sup> <https://www.extronics.com/rtls/>

<sup>116</sup> <https://nanotron.com/EN/>

for monitoring presence and movements of both people and assets in real time location applications by means of Time Difference of Arrival, which is pushed to higher layers of IoT platform. Real-Time data insight requires continuous data acquisition of location and sensor data at the edge. Nanotron's Edge Anchors seamlessly connect the What, Where and When from their location aware sensors with the value generated by nanotron's 360° Edge Analytics software. Edge Anchors provide the IoT interface to send any location and any context information to the analytics engine.

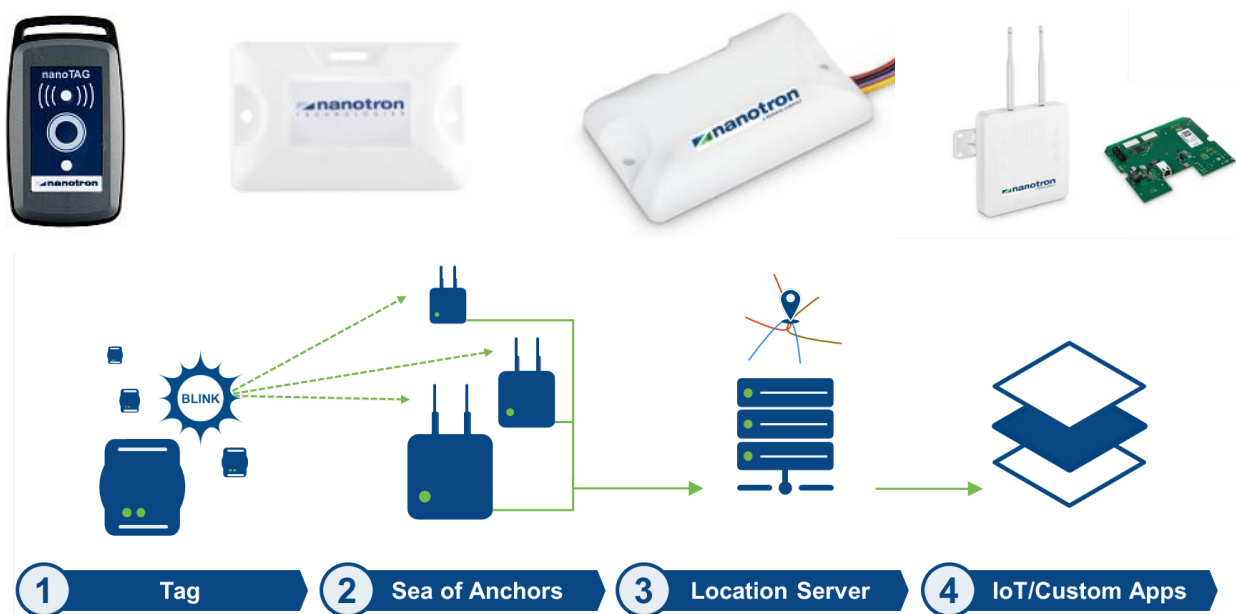


Figure 107. nanotron HW equipment, including nanoTAG, nanoTAG LP and nanoTAG RX, and nanotron edge anchor (top). Nanotron real-time localisation positioning working diagram (bottom).

### 5.2.2.3 Customer segment and end users

The smart safety stakeholders can be listed as:

- General constructors, which are responsible for the management and safety on the construction site.
- SME subcontractors from the construction sector.
- Labor inspectors.
- Insurance companies.
- Social insurance institutions.

### 5.2.2.4 Market size and growth

According to the findings from a major project carried out by the International Labour Organization (ILO), EU-OSHA, and several national OSH agencies, work-related ill-health and injury are costing €476 billion every year to the EU (representing 3.3 % of its GDP). Further findings included work-related illnesses account for 86 % of all deaths related to work worldwide, and 98 % of those occurred in the EU; 23.3 million disability-adjusted life years are lost globally (7.1 million in the EU) as a result of work-related injury and illness. Of these, 67.8 million (3.4 million in the EU) are accounted for by fatalities and 55.5 million (3.7 million in the EU) by disability; in most European countries, work-related cancer accounts for the majority of costs (€119.5 billion or 0.81% of the EU's GDP), with musculoskeletal disorders being the second largest contributor (see Figure 108) [MA-31].

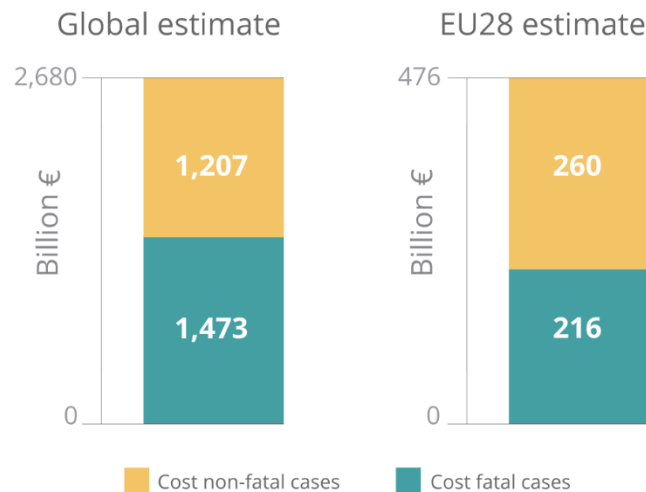


Figure 108. Work-related injuries and illnesses result to a cost in euros of approximately 2,680 billion globally and 476 billion in EU, respectively [MA-31].

These costs could be saved with the right occupational safety and health strategies, policies, and practices. While IoT has had a fairly slow start in the construction industry, many are realizing that in order to stay competitive, it is necessary that construction companies see the need to adopt new and innovative technologies into their business plans. While this presents a wealth of opportunity, building product brands are facing different obstacles in order to enhance their technologies:

Construction audiences are slow to change: According to a 2016 KPMG report, roughly two-thirds of construction and engineering professionals said that they do not use advanced data analytics to monitor project-related estimates and performance.

In connection with slow adoption practices, building professionals largely ignore R&D opportunities. According to McKinsey & Co, R&D spending in construction runs well behind other industries, with less than 1% of revenues, versus 3.5-4.5% for the auto and aerospace sectors (even though a number of new software solutions have been developed for the industry). For brands hoping to capture mindshare with architects, contractors and building owners, it is essential to educate and communicate the opportunity for innovation as a means for growing the entire category [MA-32]. In the same report, as it can be seen in Figure 109, five key trends that will shape the construction projects in the future were identified.

1. Higher-definition surveying and geolocation.
2. Next-generation 5-D building information modeling.
3. Digital collaboration and mobility.
4. Future-proof design and construction.
5. The Internet of Things and advanced analytics.

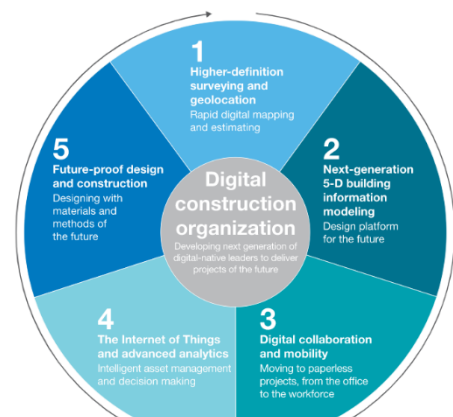


Figure 109. Digital construction future trends

### 5.2.2.5 Barriers to entry

Smart personal protective equipment is supposed to offer a higher level of protection. However, there are still some barriers to overcome before the promised benefits.

1. First of all, users must be aware that there is no guarantee of 100% protection, not even with smart equipment. Moreover, manufacturers must guarantee that the new equipment does not generate new risks (e.g., batteries usually worn very close to users' body must not catch fire or, even worse, explode, and information on who is not allowed to use them because of potential distortions with medical implants).
2. Smart equipment is often associated with data collection and transfer. It is understandable that users can perceive monitoring technology as an invasion of privacy, which is generally experienced to be a stressor (workers can be stressed if they feel that they have to meet challenging performance targets).

Consequently, the users must be well informed about what is done with the data collected. Additionally, the GDPR has to be followed.

3. A major obstacle to placing NG-IoT HW solutions on the market is the lack of testing methods against regulation. Since manufacturers must test products during the design phase, notified bodies must carry out tests to certify the products during conformity assessments. Therefore, stakeholders need to develop testing methods and incorporate them into standards.

More generally, the smart personal protective equipment sector is young, which can lead to immature products on the market. A degree of wariness about the selection, purchase and use of should be appropriate. Hence, it is recommended that all stakeholders exchange their experiences to optimise the products and applications.

Furthermore, the construction industry of ASSIST-IoT is one of the most conservative sectors. To the most common indicated barriers in implementation innovation technologies are as follow:

- High employment costs.
- A shortage of skilled workers.
- Savings in the project budget.
- Fear of new technologies by employees.
- Fear of being followed and monitored.
- High number of changing employees.
- Difficult implementation conditions (changing environment, difficult propagation conditions)

## 5.2.3 Cohesive Vehicle monitoring – Automotive

### 5.2.3.1 Problems and needs

First On-Board diagnostics (OBD) standards were enforced in 1988 by the California Air Resources Board (CARB) and, by the beginning of the 21<sup>st</sup> century, all major automotive markets require some sort of OBD. OBD is based on a series of embedded software routines, which verify sensor signals and engine behavior under certain known excitations. OBD procedures are run in the Engine Control Unit (ECU), which means that they must meet strict computation power and memory constraints. Thus, it is not possible for the method to analyze historic records of the considered vehicle and, obviously, getting access of the use data from other units in the fleet. As the OBD system must be developed and tuned during the vehicle design phase, little information is available about the system performance in real driving conditions, under ageing, manufacturing discrepancies or light to severe faults. While in its conception OBD is designed for detecting and identifying error sources, this identification is usually deficient, which results in time-consuming and expensive repair operations. Note that the system informs that there is a fault, but there is limited information about the effects of the fault or the situation triggering the fault detection event.

A second aspect to be considered is the extension of the mechanism of In-Service Conformity (ISC), where a sample of the vehicles is tested after several years of operation and may force a complete recall of the produced vehicles if the emission levels are significantly increased when compared with the certified emissions. Although the ISC mechanism is already in operation, the extension from the current 100,000 km or 5-year to 15-year period implies an increase in maintenance costs and significant financial risk for both the OEM and the final user. While today most emission regulations are centered on the design and development phase, this will serve for tackling the mismatch between real-life emissions and the certification levels [MA-33].

In addition, as explained in Section 3.2.3, connected features within the perimeter of automotive Propulsion System Controls are currently thinly spread across the market. Specifically, this means that connected vehicle monitoring systems or diagnostic features do not exist, or at least are not ready for production at this stage. Early day applications however do exist, while the focus is on service diagnostics and predictive maintenance.

Nevertheless, connectivity has become a state-of-the-art technology as it is already enhancing customer experience by allowing timely and frequent software updates. These updates not only allow the OEM to address potentially critical software deficits, but also offer the opportunity to increase customer satisfaction by improving existing content or even adding new features and functions. Examples for this additional software content range from in-vehicle games, adding new languages packages to simple visual updates of the HMI. As

a summary, it can be said that adding vehicle connectivity the OEM establishes an unparalleled level of freedom of access to the product, which benefits both the OEM and the customer. Therefore, it is a logical consequence to also include Propulsion System Controls within this new approach in order to address the unique challenges seen in this domain.



*Figure 110. ECU vehicle connectivity to the OEM will benefit both the OEM and the customer.*

In another vein, the automotive pilot as described in Task 7.3 includes an advanced connected propulsion controls system, which yet must be developed. It addresses the market segment of passenger cars and light to medium duty commercial vehicles.

In addition to this, OBD regulation will be probably modified: the current subsystem-based approach could be shifted to a tailpipe emission check, since production-ready sensors are available for most tailpipe emissions (note that sensors exist for NOx and particulate matter).

In this scenario, a complete re-design of the vehicle diagnostics procedure is possible, and leveraging on connectivity, the following functionalities at the unit and fleet levels may be attained:

- Monitoring of the fleet emissions levels; as a whole, the system should be able to provide metrics of fulfillment of the certification levels, and to assist the manufacturer about the need or convenience of performing a partial or total recall when needed.
- Identifying a given vehicle as an outlier of the fleet emission distribution.
- Allowing advanced logging and diagnostics function, understanding this as the capability of deploying diagnostic routines not affected by the limits of memory or computing power of current embedded diagnostics. This is significantly relevant when historic data is to be used, as opposed to a 10-ms step real-time controller with no logging capacity.
- Allowing the use of AI for developing new methods, based on real-life data provided by the system. Allowing over-the-air updates of the diagnostic functions, to include knowledge gained from the system as new data is available.
- Allowing the deployment of new control functions (recalibration), to optimize fleet emission profile, and to correct the behavior of those units affected by faults so that they can be corrected without needing a part to be replaced (e.g., recalibration of sensors).
- Including inputs from external technical and visual stations, and of contextual information for a complete observation of defects.

### 5.2.3.2 Existing solutions

To date, there is no extended solution covering the identified needs in a holistic way. Market segmentation and the lack of standards act as significant barriers for the development of this kind of systems. While mostly centered in exploring the benefit of adding connectivity to current OBD algorithms, several tools and developments are to be highlighted. The industry is already catching up and there is a limited number of existing connected Propulsion Control System features available, including a limited number of monitoring and diagnostic case studies, as known from competitor vehicle systems.

- **Over-the-air software updates:** Until recently, software update process for on-board electronic control modules did involve service station visits and hard-wired module flashing procedures. The latest generation of vehicles, however, include or will include electronic modules with embedded modems and over-the-air flashing capability. In the current early days of vehicle software updates, this kind of software updates occur typically in the field of infotainment or user convenience. However, vehicle operational software & calibration strategies are expected to follow within the near future [MA-34]. Electronic control system suppliers are currently offering, as an option to their products already in the



market, a selection of connectivity options and over-the-air update capabilities. For example, Robert Bosch GmbH. offers over-the-air updates (SOTA/FOTA)<sup>117</sup> and predictive diagnostics based on cloud analytics<sup>118</sup>, targeted to fleet operators and offered software as a service or as license model. Similar features and approach are present in Continental portfolio<sup>119</sup>, including services as OBD based vehicle diagnostics, vehicle tracking, geofencing, vehicle shared access, location-based services, or accident notification.

- **Connected service diagnostics:** Predictive maintenance and repair thanks to connected prognostics, statistical modelling, and application of AI/ML. Key advantage: User habits can be tracked, analyzed and appropriate service actions can be taken and/or automatically scheduled. Such schemes already exist in the world of commercial vehicles, primarily to reduce downtime and to increase operational efficiencies. Features can go as far as checking part availabilities in nearby workshops up to booking time slots for repair at dealership workshops [MA-35].
- **Electronic horizon:** Combining on-vehicle sensor data with map data, which is already widely used within the domain of advanced driver assist features (ADAS) and more recently also on advanced range prediction algorithms in battery electric vehicles [MA-36].
- **On Board Monitoring:** Proposals exist to mandate additional monitoring functions beyond the layout of existing on-board diagnostic schemes. Leveraging connectivity for this is not currently seen as a firm requirement, but it seems to be under consideration.

While these features and services are also marketed to the vehicle manufacturers, to date the imbrication into ECU architecture and software development process has been limited. In some cases, manufacturers have developed applications targeting final users, as Volkswagen's We Connect Go<sup>120</sup>. As in most cases, OBD standard codes are profited and no real re-shaping of the diagnostics has been performed.

There is a significant quantity of software vendors providing access to the OBD codes of the vehicle. For example, pioneer Torque<sup>121</sup> app targeting personal use has had downloads exceeding 1 million. Other software vendors integrate OBD access into fleet management software suites. In many cases the software focused on optimal fleet management, but some functionalities are sometimes included for registering and logging OBD fault codes.

Note that most of the solutions in the market act as a simple bridge between the embedded diagnostics code and a cloud service. Only solutions marketed by electronic control system suppliers or vehicle manufacturers could (to date) offer solution to the needs listed in the previous section.

### 5.2.3.3 Customer segment and end-users

Main players for this pilot are the following:

- **Vehicle manufacturers.** Major global manufacturers, ordered by vehicle sales, are Toyota, Volkswagen Group, Hyundai / Kia, General Motors (with SAIC-GM-Wuling), Ford, Nissan, Honda, FCA, Renault, Groupe PSA, Suzuki, SAIC, Daimler, BMW, Geely, Changan, Mazda, Dongfeng Motor, BAIC, and Mitsubishi (recently merging of FCA and Groupe PSA has not been considered).
- **Electronic control system suppliers (Tier 1 suppliers).** Electronic control unit (ECU) production is controlled by a few manufacturers in Europe, North America, and Japan (e.g., Bosch, Siemens, Continental, Delphi Electronics, Denso, Magneti Marelli, Hitachi Automotive or Hyundai Kefico) - market in developing regions like China and India are more fragmented. These ECU providers also own and develop software bundles, which are usually licenced to the vehicle manufacturer. In some cases,

<sup>117</sup> [https://www.bosch-mobility-solutions.com/media/global/highlights/connected-mobility/updates-over-the-air/internetconnectivity\\_summary\\_manufacturer.pdf](https://www.bosch-mobility-solutions.com/media/global/highlights/connected-mobility/updates-over-the-air/internetconnectivity_summary_manufacturer.pdf)

<sup>118</sup> [https://www.bosch-mobility-solutions.com/media/global/products-and-services/mobility-services/predictive-diagnostics/summary\\_predictive-diagnostics.pdf](https://www.bosch-mobility-solutions.com/media/global/products-and-services/mobility-services/predictive-diagnostics/summary_predictive-diagnostics.pdf)

<sup>119</sup> <https://www.continental-automotive.com/en-gl/Passenger-Cars/Vehicle-Networking/Software-Solutions-and-Services/vAnalytics-Incar-Data-as-a-Service>

<sup>120</sup> <https://play.google.com/store/apps/details?id=de.volkswagen.vwconnect&hl=en&gl=US>

<sup>121</sup> <https://play.google.com/store/apps/details?id=org.prowl.torque&hl=en&gl=US>

the control and diagnostics algorithms are propriety of the vehicle manufacturer, or they introduce significant modification to the software provided by the ECU supplier.

- **Fleet management software vendors.** While most of the fleet management software is based on location services (GPS, GNSS, etc.) and optimal routing services and freight management tools, many software providers also offer to some extent diagnostics and vehicle service planning. Usually, the vehicle OBD interface is profited for this. Since most of the software solutions rely on public OBD codes, there is no dedicated diagnostic tools development. Some of the software vendors also target to personal users. Some of the companies offering SaaS, without pretending being exhaustive, are ARI Fleet Management, Azuga, Chevin Fleet Solutions, Inseego, Donlen Corporation, Geotab, GPS Insight, Masternaut, MiX Telematics, Nextraq, Omnitrac, Teletrac Navman (Director Fleet Software), Trimble, Verizon Connect, Wheels Inc., Samsara, Bestmile, Tourmaline Labs, KeepTruckin, Avrios, ThingTech, Automile Inc., Fleetonomy, Fleetroot, Autofleet, ClearPathGPS, Fleetio, Capterra, Smartrak, Arvento, US Fleet Tracking, Onfleet, Innovative Maintenance Systems (Fleet Maintenance Pro), TomTom (Telematics), Wialon, GPSTrackIt (Fleet Manager), GPS Insight (Fleet Tracking Solution), RTA (Fleet Management Software), and Arvento (OBD-II Tracking Package).

Concerning the end users, the following may be identified:

- **Fleet managers:** Medium to big size fleets, with the need of scheduled, predictive, and corrective maintenance will benefit from an increase on diagnostics system performance. Example of these managers are major car rental companies, long-distance hauling companies, and last-mile delivery companies.
- **Repair services providers:** either those managed by the vehicle manufacturer or third parties.
- **Individual drivers:** While indirectly instructed by software vendors or vehicle manufacturers, drivers are the final users of the vehicle, and they will need to interact with the diagnostic service.

#### 5.2.3.4 Market size and growth

Automotive industry represents 6.1% of total EU employment. 2.6 million people work in direct manufacturing of motor vehicles (8.5% of EU employment in manufacturing), with 13.8 million people including indirect jobs<sup>122</sup>. In addition to the employment share in the EU, automotive industry has an important multiplier effect in the economy, as it is important for upstream industries such as steel, chemicals, and textiles, as well as downstream industries such as ICT, repair, and mobility services.

According to ACEA<sup>123</sup>, 15.8 million passenger cars were manufactured in the EU in 2019, plus 2.7 million commercial vehicles<sup>124</sup>. That accounted for 25% and 19% of world production, respectively. Trade surplus calculated as export minus import of motor vehicles accounted for 73.9 billion EUR<sup>125</sup>, with an aggregated R&D investment of 60.9 billion EUR.

Prospects from EU and independent market analysis firms expect a significant contribution of the digital services in the automotive sector, as to reach 30% to 40% of the value in the automotive value chain [MA-37]. According to McKinsey & Co report, new business models could expand automotive revenue pools by about 30% by 2030, identifying shared mobility, connectivity services, and feature upgrades as the driving factors.

<sup>122</sup> [https://ec.europa.eu/growth/sectors/automotive\\_en](https://ec.europa.eu/growth/sectors/automotive_en)

<sup>123</sup> <https://www.acea.be/statistics/article/eu-passenger-car-production>

<sup>124</sup> <https://www.acea.be/statistics/article/eu-commercial-vehicle-production>

<sup>125</sup> <https://www.acea.be/statistics/tag/category/key-figures>

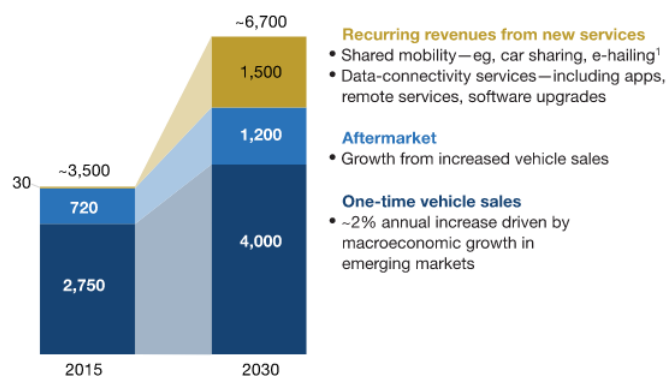


Figure 111. Automotive revenue pool in high-disruption scenario, USD billion [MA-38]

Finally, global fleet management market size is expected to grow from USD 19.9 billion in 2020 to USD 34.0 billion by 2025 [MA-39], with a CAGR of 11.3% per year. Main drivers for this growth are government regulations; *Software-as-a-Service (SaaS)* and *cloud-based deployments* of fleet management solutions; decreasing hardware and software costs; the need of optimization of fleet operation expenses; and growing need of operational efficiency among fleet owners.

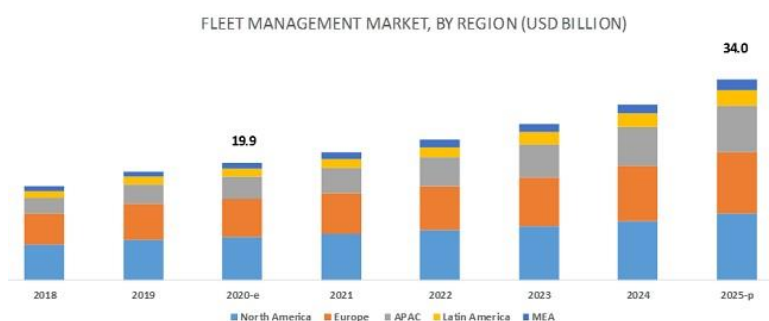


Figure 112. Forecast of fleet management market, by region in USD billion [MA-39].

### 5.2.3.5 Barriers to entry

Except where enforced by legislation (OBD-II, EOBD or similar standards), ECU software and measurements are kept closed by the vehicle manufacturer or the ECU manufacturer. This is a significant entry barrier for third parties, as fleet management software providers: these companies are not granted any access to sensitive data beyond the public codes available through OBD, or via manufacturer specific diagnostic tools. As per our knowledge, big fleet owners are neither able to specify (or are not interested in specifying) advanced diagnostic protocols and software.

Market fragmentation probably is the major significant barrier of entry: while most manufacturers are starting to develop tools and services based on connectivity, there is no established industry-wide standard specifying system requirements, data access and exchange protocols, and granting access for third party service providers. Note that safety and data security concerns are paramount when considering deploying uncontrolled pieces of software, and even use data contains sensitive data according to EU regulations. The European Data Protection Supervisor [MA-40] explicitly lists the following sources of data protection issues: lack of transparency, excessive data collection, data retention, lack of control, lack of purpose limitation, collection or inference of sensitive information, and security and access control.

Competition between main actors and brands can also act as a significant barrier for new technologies and the adoption of industry-wide standards. Main friction areas are data management and control over its value, human-machine interface, and customer ties to strong brands.

Finally, regulatory aspects may deter the application of some technologies affecting internal combustion engine control. EU regulation explicitly bans ‘defeat devices’ [MA-41], which are defined in a way that could prevent the use of many adaptive, optimal or context-aware control. Current regulation must be modified for gaining

the full potential of the connected vehicle, and that needs restoring the trust between manufacturers and the regulatory bodies following recent years of stress [MA-42].

### 5.2.3.6 Standardization and Legislation

Counterweighting the market fragmentation, the Association for Standardization of Automation and Measuring Systems ASAM<sup>126</sup>, and AUTomotive Open System Architecture AUTOSAR<sup>127</sup> are example of industry led initiatives with focus in standardization of the ECU and related services. ASAM is a non-profit organization focused on developing standards for ECU development tools, ECU software and data exchange; ASAM is open to international car manufacturers, suppliers, tool vendors, engineering service providers and research institutes from the automotive industry.

While not directly considering cloud-edge computation, ASAM's project SOVD - Service Oriented Vehicle Diagnostics is centred in the definition of a standardized service API for HPC (high performance computers) diagnostics, which includes new HPC-related and conventional diagnostic use-cases (and distinguish between use-cases for onboard, proximity and remote diagnostics).

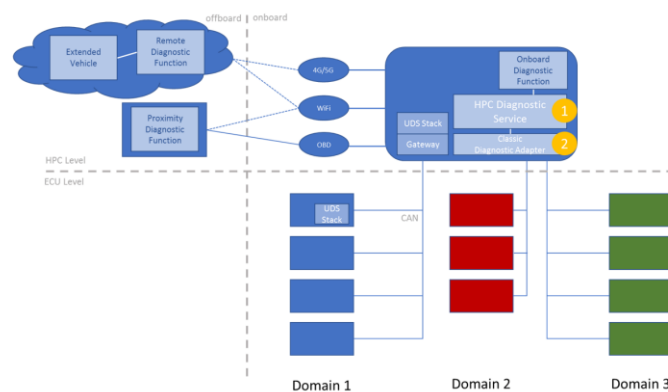


Figure 113. SOVD - Service Oriented Vehicle Diagnostics project by ASAM<sup>128</sup>

AUTOSAR was created by an effort of the German industry to allow interoperability of the ECU software. As such, the group is centred in managing the software complexity associated with growth in functional scope, supporting flexibility for product modification, upgrade, and update, and to increase scalability and flexibility to integrate and transfer functions across product lines. Current core members are BMW Group, Bosch, Continental, Daimler, Ford, GM, PSA Group, Toyota, and Volkswagen, while many relevant manufacturers or tool vendors are also members of different nature.

Other cross-industry associations are the Car Connectivity Consortium<sup>129</sup> or the Open Automotive Alliance<sup>130</sup>.

There are indications that the legislators are intending to leverage or even mandate connected monitoring functionalities in the future. Known proposals in regard to the upcoming post EU6 legislation in Europe are OBM. The need for such enhancements is resulting from the expected, significantly higher stringency of the post EU6 legislation for passenger cars and light commercial vehicles. At this point, the future legislation is not yet set, but detailed proposals are existing, thus OEM's and suppliers are starting to work against assumptions. Criteria emission and diagnostic limit thresholds will be further reduced, the boundary conditions for homologation procedures enlarged and the horizons for full useful life and ISC will widen up. A way to accommodate all these upcoming requirements is to further increase the technology content of the system, by adding sensors, by deploying more durable components or utilizing improved materials and manufacturing processes. In mass production however, the overall system costs need to be tightly controlled. So, another option is to become smarter within the operation of the system.

<sup>126</sup> Association for Standardization of Automation and Measuring Systems ASAM <https://www.asam.net/>

<sup>127</sup> AUTomotive Open System Architecture AUTOSAR <https://www.autosar.org/>

<sup>128</sup> ASAM. SOVD - Service Oriented Vehicle Diagnostics <https://www.asam.net/project-detail/sovd-service-oriented-vehicle-diagnostics/>

<sup>129</sup> Car Connectivity Consortium <http://carconnectivity.org/>

<sup>130</sup> Open Automotive Alliance <https://www.openautoalliance.net>

## 5.3 Stakeholders engagement

### 5.3.1 Workshop

The first webinar-workshop of the project was held on 18<sup>th</sup> January 2021. It was a one-hour and a half fully online live event using the Microsoft Teams conferencing tool. It was attended by 51 participants, coming from both industrial and academic stakeholders' consequence of the dissemination activities carried out by the ASSIST-IoT Consortium through social media channels as well as direct contacts reached by the staff (see figures below). Finally, the workshop has been uploaded to the media channel<sup>131</sup> of the Project so that it could be also reviewed in offline.

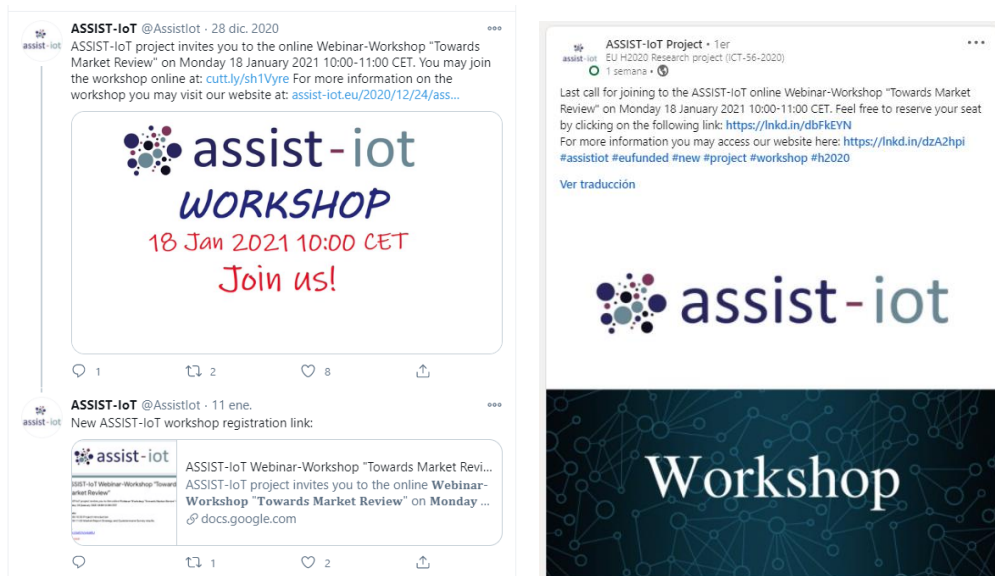


Figure 114. ASSIST-IoT 1<sup>st</sup> workshop communication on social media channels.

#### 5.3.1.1 General description

The workshop aimed at getting insights regarding the envisioned needs of Next Generation IoT by welcoming different technological and industrial stakeholders that could provide input to and exchange ideas with the project partners on key message formulation, share relevant resources, and give individual feedback on issues of importance to the chapter topic. Those insights will be considered throughout project's lifespan and will be included within market analysis section of this deliverable "D3.1 - State-of-the-Art and Market Analysis Report" of the project. The objective pursued by this workshop was to (1) introduce the ASSIST-IoT framework and (2) to set up an open discussion with industrial partners to share needs, requirements and real-live experiences/pains which could feed the ASSIST-IoT staff before starting up the use case definitions in detail. It is important to mention here that, whilst the testbeds we are going to carry out during the ASSIST-IoT timeframe are clear and they were properly described in the Document of Work, any business plan survives first contact with a customer, that's why as a Consortium we all have decided to try to involve our expected users since the very beginning of the Project. To participate in the workshop, a public website was launched for giving the end-users the opportunity to book the date and read (and approve) the inform consent (Figure 115).

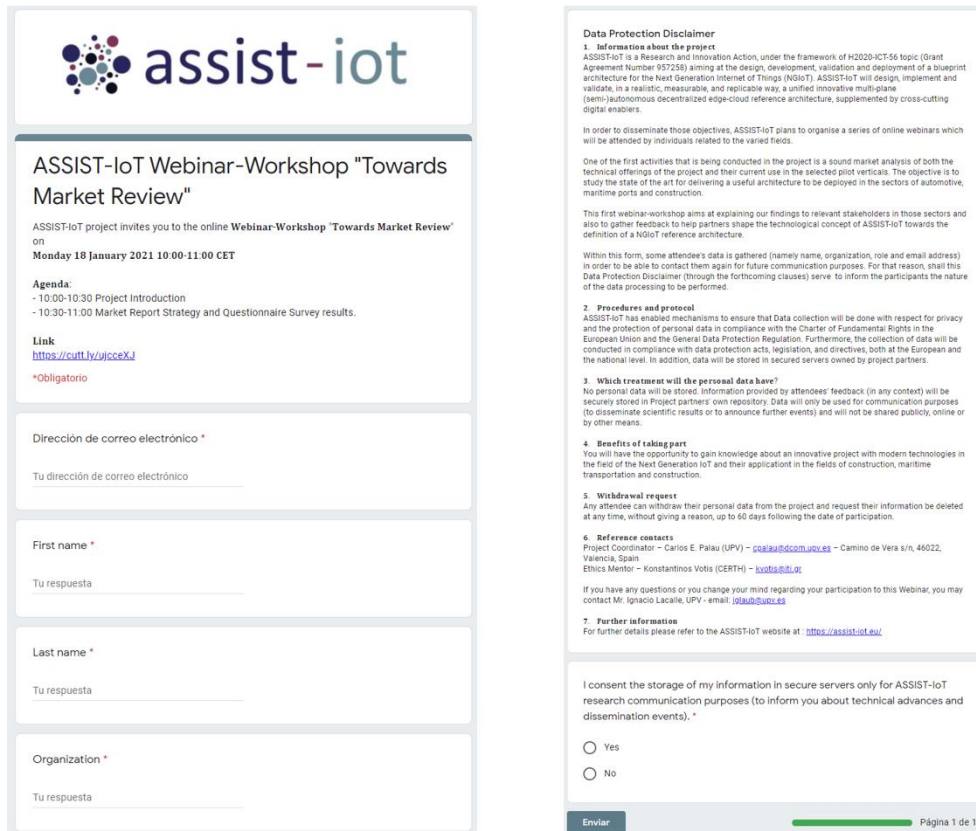
The detailed agenda for the workshop was as described below:

- UPV will carry out the warm welcome and broadly will introduce the audience to the workshop which are the objectives pursued by the call as well as the polite rules to interview.
- The Project Coordinator will introduce the Project: objectives, testbeds, and timeframe.
- The Innovation Manager (i.e., Prodevelop) will introduce the slot where the industrial partners will present the pilots for testing and validating the developments carried out within the project.

<sup>131</sup> [https://www.youtube.com/channel/UC8Sedd5UyB8R61d9YDkkeGg?view\\_as=subscriber](https://www.youtube.com/channel/UC8Sedd5UyB8R61d9YDkkeGg?view_as=subscriber)



- The Innovation Manager will take the floor to present the online survey we are going to carry out for the next two weeks (since January 18<sup>th</sup> onwards).
- UPV will close the session with a wrap-up and ask the audience for specific questions.
- Questions from the audience will be addressed and the workshop conveniently closed.



**assist-iot**

### ASSIST-IoT Webinar-Workshop "Towards Market Review"

ASSIST-IoT project invites you to the online Webinar-Workshop "Towards Market Review" on  
**Monday 18 January 2021 10:00-11:00 CET**

**Agenda:**  
 - 10:00-10:30 Project Introduction  
 - 10:30-11:00 Market Report Strategy and Questionnaire Survey results.

**Link**  
<https://cutt.ly/vjccexJ>

**\*Obligatorio**

**Dirección de correo electrónico \***

Tu dirección de correo electrónico

**First name \***

Tu respuesta

**Last name \***

Tu respuesta

**Organization \***

Tu respuesta

**Data Protection Disclaimer**

**1. Information about the project**  
 ASSIST-IoT is a Research and Innovation Action, under the framework of H2020-ICT-56 topic (Grant Agreement Number 957258) aiming at the design, development, validation and deployment of a blueprint architecture for the Next Generation Internet of Things (NGIoT). ASSIST-IoT will design, implement and validate, in a realistic, measurable, and replicable way, a unified innovative multi-plane (semi-)autonomous decentralized edge-cloud reference architecture, supplemented by cross-cutting digital enablers.

In order to disseminate those objectives, ASSIST-IoT plans to organise a series of online webinars which will be attended by individuals related to the varied fields.

One of the first activities that is being conducted in the project is a sound market analysis of both the technical offerings of the project and their current use in the selected pilot verticals. The objective is to study the state of the art for delivering a useful architecture to be deployed in the sectors of automotive, maritime ports and construction.

This first webinar-workshop aims at explaining our findings to relevant stakeholders in those sectors and also to gather feedback to help partners shape the technological concept of ASSIST-IoT towards the definition of a Ngiot reference architecture.

Within this form, some attendee's data is gathered (namely name, organization, role and email address) in order to be able to contact them again for future communication purposes. For that reason, shall this Data Protection Disclaimer (through the forthcoming clauses) serve to inform the participants the nature of the data processing to be performed.

**2. Procedures and protocol**  
 ASSIST-IoT has enabled mechanisms to ensure that Data collection will be done with respect for privacy and the protection of personal data in compliance with the Charter of Fundamental Rights in the European Union and the General Data Protection Regulation. Furthermore, the collection of data will be conducted in compliance with data protection acts, legislation, and directives, both at the European and the national level. In addition, data will be stored in secured servers owned by project partners.

**3. Which treatment will the personal data have?**  
 No personal data will be stored. Information provided by attendees' feedback (in any context) will be securely stored in Project partners' own repository. Data will only be used for communication purposes (to disseminate scientific results or to announce further events) and will not be shared publicly, online or by other means.

**4. Benefits of taking part**  
 You will have the opportunity to gain knowledge about an innovative project with modern technologies in the field of the Next Generation IoT and their application in the fields of construction, maritime transportation and construction.

**5. Withdrawal request**  
 Any attendee can withdraw their personal data from the project and request their information be deleted at any time, without giving a reason, up to 60 days following the date of participation.

**6. Reference contacts**  
 Project Coordinator – Carlos E. Palau (UPV) – [cpalau@discom.upv.es](mailto:cpalau@discom.upv.es) – Camino de Vera s/n, 46022, Valencia, Spain  
 Ethics Mentor – Konstantinos Votis (CERTH) – [k.votis@certh.gr](mailto:k.votis@certh.gr)

If you have any questions or you change your mind regarding your participation to this Webinar, you may contact Mr. Ignacio Lacalle, UPV, e-mail: [ilacalle@upv.es](mailto:ilacalle@upv.es)

**7. Further information**  
 For further details please refer to the ASSIST-IoT website at: <https://assist-iot.eu>

I consent the storage of my information in secure servers only for ASSIST-IoT research communication purposes (to inform you about technical advances and dissemination events). \*

☐ Yes  
☐ No

**Enviar** Página 1 de 1

Figure 115. ASSIST-IoT 1<sup>st</sup> workshop submission form webpage.

### 5.3.1.2 Minutes

Mr. Ignacio Lacalle-Úbeda kicked-off the workshop presenting Project Coordinator (PC) Prof. Dr Carlos Enrique Palau-Salvador, who provided an overview of ASSIST-IoT, highlighting that the project aims to overcome the lack of capabilities to handle the new requirements foreseen in Next Generation IoT technologies and scenarios, e.g., highly decentralised ecosystems, transversal security and privacy features among all architectural layers, or human centricity, etc. The project has identified several use cases or scenarios that will be demonstrated by means of the NG-IoT architecture of ASSIST-IoT in three different pilots: Port Automation in France/Malta, Smart Safety of Workers in Poland, and Cohesive Vehicle Monitoring in Germany/Spain.

The floor was passed to Ángel Martínez-Cavero, Innovation Manager (IM) of ASSIST-IoT. He highlighted the 3 key points of the project from an innovation and exploitation point of view:

1. The project not only wants to develop and deploy state-of-the-art technologies, but also going beyond, as the project is a H2020 Research and Innovation Action (RIA), which also demands to carry out scientific research beyond market solutions.
2. All the solutions to be used will have as a key pillar in mind, a human centricity approach.
3. The aim is to solve real problems/concerns from the specific industrial domains, so that we have involved relevant stakeholders of those domains.

IM also reminded that the online workshop was set up to get the thoughts and extract opinions of different experts and stakeholders across the three pilot environments of the project (Figure 116).

## Pilot environments

- Rationale, context, challenges and objectives pursued previously reviewed
- Developments and job carried out within the Project will be demonstrated and evaluated in three industrial verticals:
  - Port Automation (i.e. maritime industry)
  - Smart Safety for workers (i.e. building industry)
  - Cohesive vehicle monitoring and diagnostics (i.e. automotion Industry)
- Each pilot will include several scenarios where some KPIs and real problems/concerns from the specific domain will be demonstrated
- The aim of the next slot is to share with the Industrial attendants those testbeds so that we could discuss about them (e.g. expected benefits, pilot objectives, rationale, main motivation, etc.)
- Your participation is more than appreciated

*Figure 116. Pilot environments slide from the 1<sup>st</sup> ASSIST-IoT workshop.*

Then he gave the floor to the industrial leaders of the three project pilots, Francisco Blanquer from TERMINAL LINK (TL), Piotr Dymarski from MOSTOSTAL (MOST), and Daniel Roettger from FORD. The three of them presented the current state-of-the-art of their corresponding pilots / testbeds and explained why the latest advancements are not enough to fulfil their industrial and business needs. Among them, cybersecurity, privacy, network reliability and/or network redundancy, digital to physical alignment, or AR services to prevent in-work risks were pointed out. Based on the requirements mentioned above, two main common objectives were highlighted for reducing capital and operational expenditures, so that increasing their competitiveness: **1) continuous improvement, 2) process automation.**

At this point of the workshop and before starting the wrap-up of it and give the audience the opportunity to ask for specific questions, the Innovation Manager of ASSIST-IoT introduced the Online Survey (Figure 117), which was being carried out to gather more information from relevant stakeholders:

## Online survey

- As part of the job carried out in the Analysis stage of this Project we are asking interested staff (e.g. Industry partners, Academia, etc.) about their most important problems/concerns
- The objective pursued by this is to find out insights about IoT architectures, Edge/fog computing necessities, etc. which will give us the opportunity to feed our developments and put the focus on real problems and specs
- Findings will be published into a public deliverable which will be uploaded to our site (i.e. State of the Art and Market Analysis report)
- The Online Survey will be:
  - Reachable through the following link:  
<https://forms.office.com/Pages/ResponsePage.aspx?id=7Se5--njEES94SKTuPSAMmkxZ7MQxQpPc4yCeO3b9UNkUSR0RNSDJURkdINVRPVE9YTzdlTUtOMy4u>
  - Disseminated by our Social Media Channels
  - Open for the next two weeks (since today, onwards)
  - Please, spread the voice. We would really appreciate your help and support



*Figure 117. Online Survey announcement slide of 1<sup>st</sup> ASSIST-IoT workshop.*

Finally, the workshop ended with a Q/A session, in which the audience raised their opinions or doubts about potential solutions to overcome the presented challenges. The list included:

- **What the pilot owners think about exploring the use of 5G as a single network of networks in order to on the one hand fulfil network reliability needs and, on the other hand, reduce expenses thanks of network slicing capabilities?** Francisco Blanquer (TL) considered that it may be used in the long-term, but in short-term 5G would not be enough due to the very challenging environments of terminal ports, and on the other side, they the infrastructure solutions provided by mobile vendors are not free as e.g., WiFi.

- **Have pilot owners identified the AR tools to be used for the tactile internet solutions of the project? Will they be developed within the project or will make use of available commercial solutions?** As the idea of the project is to improve operational efficiencies in the pilot scenarios of the project, both Francisco Blanquer (TL) and Piotr Dymarski (MOST) mentioned that the plan is to reuse as much as possible the most up-to-date AR software and HW solutions, and not focusing on carry out a dedicated immersive interface development to address some of their particular needs, which would end in a siloed solution not suitable for exploitation.
- **How open are the Electronic Circuit units on-board in FORD cars?** Klaus Schusteritz (FORD) commented that within FORD route map, enabling potential Over-The-Air software update solutions is expected. However, for the time being they are reluctant to it and cannot put a specific available date due to potential cybersecurity and privacy threats/attacks.

### 5.3.1.3 Key takeaways

As explained in the workshop minutes, participants raised several questions and provided comments regarding the project's scope and how it will be linked with real business needs. The key takeaways for the workshop are listed below and will be taken into consideration in the innovation and exploitation of the project.

- 1) Continuous improvement and process automation: Although IoT is well deployed in several industrial premises, it is in its infancy, and several challenges will be needed to be tackled in the upcoming years. To do so, pilot owners agreed that their business line should consider that they are not still exploiting all the capabilities that IoT could offer, so that the continuous improvement should be in their route maps. This will allow exploiting the huge volume of unused data extracted from heterogeneous IoT sources, helping to realize an authentic process automation that will improve their efficiency and effectiveness.
- 2) Cybersecurity, privacy, and network reliability are the initial cornerstones that the project should analyse. If those limitations are not well overcome, the rest of benefits that NG-IoT can support will be useless.
- 3) The Unique Value Proposition of the core architecture of ASSIST-IoT is not clear enough so it was very difficult for the audience to ensure that outcomes of the Project would be deployed in their live environments because they fix a real problem/pain they already have.
- 4) For future workshops it is important to change the strategy/approach which will give the audience more relevance so that they could take the floor most of the time (and the Consortium staff talk less)

In addition, the organisers noticed that the workshop originally set up for 1h, surpassed that scheduled limit. For future workshops, it was agreed that the agenda should be strictly followed, so that external stakeholders that may not commit to stay until the end of the sessions, and therefore, limiting the engagement impact, would refuse joining future webinars-workshops.

### 5.3.2 Interviews

Additionally, 14 peer-to-peer interviews of around 30-60' were conducted with internal (e.g., experts from the ASSIST-IoT consortium or partner organizations who do not necessarily work in the project) and external (e.g., contacts from companies outside of ASSIST-IoT consortium) IoT domain experts or stakeholders for the project. Before conducting the interviews, the interviewees voluntarily signed the informed consent that among others included the right to access, rectification, erasure, refuse, and withdraw of their personal data and answers at any time, as well as a sample of the questions list that were going to be addressed during the interview. They were also informed that their answers will be served to inform the project's user requirements definition, design revisions and technology development, and that the anonymized summarized/aggregated information was going to be submitted to the EC as part of public reports and, potentially, be used to write articles for peer-reviewed journals and relevant industry magazines, for presentations at conferences and workshops, and in the promotion of the project in general.

Table 33. Peer-to-peer interviewees profile and their most relevant answers

Profile Description	Main answers
<b>ICT DOMAIN</b>	
Solution architect responsible for unifying business communication processes and tools in an ICT company, man, mid-age, more than 15 years of experience	<ul style="list-style-type: none"> <li>- The most important concern nowadays related to ICT systems is the elimination of systems with incompatible data models, as well as user interfaces.</li> <li>- He would feel blind and useless if he cannot longer use ICT applications, as he uses them very often for solving operational issues.</li> <li>- His company is facing several interoperability issues, but he is not able to estimate the cost of them in their technological and business departments.</li> <li>- According to his view, operational latency depends on business process specifics (ICT resources scalability automation in real time), so that he agrees that there is a real necessity of real-time (zero latency) applications or services for fulfilling future needs.</li> <li>- Their company relies on Azure for both data hosting and operational applications.</li> </ul>
Man, mid-age, manager of an ICT company which delivers warehouse management systems	<ul style="list-style-type: none"> <li>- The three most important features for them are: (i) A good quality connection is critical. The dynamically changing state of the warehouse essentially prevents accurate long-term planning, so the system must adjust its plans very often. Planned tasks can become "obsolete" very fast, new priority tasks may arrive suddenly, and the system must react in near real-time. Any loss of connectivity, or significant delays, result in desynchronization of the actual warehouse state, and the state perceived by the system. Good user experience is also highly dependent on good communication. Local connectivity between devices is not as important in their use-case, as good connection to the central system, (ii) stability of the system, which should be fault-resilient and highly available – fault in processing of one task, or one queue must not halt other processes. Fault-tolerance is a mission critical feature; (iii) Data security is also critical – not in the sense of access restrictions, but rather in the sense of data loss prevention. All data must be collected and never lost. If data e.g., from the last hour of warehouse operations is lost, or otherwise unavailable, the whole warehouse state may need to be manually re-verified, and re-synchronized, which must be avoided.</li> <li>- The company uses existing warehouse IoT devices to deliver its solution or offers devices as part of its comprehensive solution. For device provision, the company uses reliable and verified partners to deliver IoT devices interoperable with the management systems. There is a certification process to make sure that the devices are compatible with the central system. Interoperability between devices themselves is not required, because communication goes through the central system.</li> <li>- However, lack of interoperability (e.g., a common interface, protocol, data model) in warehouse automatics (e.g., sorter, crane, conveyor belt) is a problem that is clearly visible. Every manufacturer has their own standards of communication. Interviewee's company needs to provide separate plugins for devices from different producers, even if the function of the devices is equivalent. An interoperability standard would save a lot of work for the company. Device manufacturers offer their own WCS systems, that are black-boxes and cannot be deeply interfaced with, which is a solution that poorly fits their business.</li> <li>- Fully autonomous solutions are not currently a priority, but under discussion for the (far) future.</li> <li>- Although there are AR glasses already used in warehousing, and also voice applications i.e., full voice interfacing, the company is open to exploring haptic feedback e.g., vibrations for additional communication (e.g. wrong code scanned).</li> <li>- Speed is important, but WiFi is enough (provided proper warehouse coverage). Penetration is also important and has strong influence on coverage. Other technologies</li> </ul>

Profile Description	Main answers
	<p>than WiFi (e.g. 4G) are used outside (in the yard). 5G could potentially be used inside as well as in the yard, but it's not a critical requirement.</p> <ul style="list-style-type: none"> <li>- Any cloud solution has to conform to real-time connectivity requirements. Cloud usage is promoted within the company, as long as the cloud solutions can meet the required low-latency communication standard.</li> <li>- Currently employed AI is not strongly reliant on model training or usage. Federated learning does not have an obvious place in the current solution. It can be potentially useful, but not planned currently.</li> </ul>
Man, Mid-age, working on a cybersecurity SME	<ul style="list-style-type: none"> <li>- Main concerns are the need for the standardization of the data exchange from different system providers for the extended connectivity between such different type of smart devices, the information security in a distributed ecosystem (offices and branches) in wider ICT systems, and the lack of a data exchange model in comparison with the local work model.</li> <li>- He uses traditionally ICT systems at all times (e.g., Microsoft Office, Salesforce, Baan), and will be frustrated if he would no longer use them, as they are mandatory nowadays and cannot imagine a proper well done job performance without ICT or applications daily.</li> <li>- On the one hand, he does not have any doubt that business operational processes could be improved with data analysis and estimated their turnover benefits around 40%. For instance, the possibility of aggregating data in real time. to later carry out more aggregated and specific processing with BI and AI techniques would allow them to have a more complete vision of the business (sales, production, etc ...) in real time, and with the frequency determined by each department, in order to make faster and / or anticipated decisions. However, on the other hand, he has had very bad experiences with vast amount of data, including interoperability issues which has a significant cost, as well as finding a different use for technologies. For example, the LATAM office that uses a CRM / ERP that is technologically different from the CRM / ERP of EMEA. For the Controlling department of the business, this means a headache, not having the information in a homogeneous way to analyse and exploit the data.</li> <li>- They have had the real experience of an IoT ecosystem with the integration of air quality sensors within a smart platform: in total about 10 devices. Normally the integration is not done to the device itself, but to the data source of the provider that has installed the sensors and collected the data. The problem is that as the smart platform is the last link in the chain, on many occasions the problem of the IoT ecosystem is transferred to it.</li> <li>- They are really keen on using cloud-based platforms because they could offer different enhanced features, such as access to all information in real time, ease of administration and use, and safety and security. Furthermore, they have accepted the deployment of operational applications in the cloud. A proof of this is that SalesForce is already used for commercial management.</li> <li>- Due to the type of projects that they execute, the HMI developed must meet a series of requirements in terms of being Web Responsive and with functions in multiple channels: Mobile, Tablet. Portable, Operator Station and Videowall. Hence, they try to have as intuitive and comfortable as possible their interfaces. To do so, they also try to consider international recommendations and standards of usability and accessibility, trying to reach at least the "AA" Level of Conformity.</li> </ul>
<b>RESEARCH &amp; ACADEMIA</b>	
Full professor in Computer Science school focused on edge-fog	<ul style="list-style-type: none"> <li>- Different from what the common line of thought is, the latency/real-time is NOT the main problem. Only few specific cases the latency does matter. According to the respondent, the most worrying aspect is data volume. Not the data produced by</li> </ul>



Profile Description	Main answers
<p>computing architectures, man, mid-age, more than 20 years of experience in the field, H2020 project coordinator</p>	<p>specific sensor, but by the combination of large number of sensors together. In IoT, to achieve connectivity between device to fog node to cloud, the usual fact is to create kinds of “commodity networks”, which are not prepared to deal with large volumes of data from different sources, lacking scalability and flexibility, not being prepared for dynamic demands of bandwidth or data load to be managed. This is of paramount importance (and must be solved) as the main motivation for using fog computing is to alleviate the network by sending much less data through it towards the cloud centre.</p> <ul style="list-style-type: none"> <li>- Another crucial concern is the lack of flexibility when using available networking technologies and how they fit the “edge-to-cloud continuum” paradigm. As an example, the ironic situation occurring when using 3G or 4G access network in fog-computing deployments, during which the data generated by the sensor reaches the base station, goes to e.g., Paris and then comes back to the original location to be derived to the fog node to make some processing. The solutions are there to use alternative communication technologies, specific for IoT (e.g., LoRa, Sigfox, NB-IoT), which are currently not widely spread and not mature enough for large, ambitious IoT deployments.</li> <li>- The lack of semantic interoperability, as well as the variety of formats (second V in Big Data) is one of the main concerns regarding data interpretation. Even with quality data, the semantic differences make a proper interpretation of the data really difficult. For instance, a feed of tweets cannot be analysed properly without considering different languages (syntactic) and different shortcuts of expressions, concepts, etc.</li> <li>- One of the main features mission in IoT devices is battery life. There are very promising projects that are achieving to provide long battery life to sensors thanks to solar panels or taking advantage of mechanical energy of rain. Another most improvable aspects of IoT devices are their difficulty to be configured and sometimes they do not even offer enough range of features that would be desirable. Finally, despite of the theoretical “wide and easy availability” of IoT sensors, devices, gateways, etc... the reality sends a different message. Usually, the hardware providers and manufacturers take too much time to deliver equipment (if not cancelled completely) ranging from devices to network equipment, etc. (e.g., LoRa gateways), so that, at the end “IoT is not easy to buy”.</li> <li>- Regarding the two trends for edge/fog computing deployments (all-in-one HW+SW nodes, or the utilisation of virtualisation and containers) he thinks that the future of edge/fog deployments will (and must) rely on cloud-oriented techniques like containerisation and virtualisation, since having hardware-software coupled for single applications, many problems of scalability arise, no matter where the most part of computing is placed. Whenever a peak of demand arrives, there is not enough elasticity to adapt. The key, then, must be on understanding the fog as an extension of the cloud (downwards) and not the other way around, assuming that multi-tenancy in fog nodes must be a mandatory feature to comply with.</li> </ul>
<p>Professor in Computer Science school, leading several H2020 5G-PPP projects, man, mid-age, with more than 15 years of academic and research experience</p>	<ul style="list-style-type: none"> <li>- Current ICT systems should support the current technology trends, such as virtualization, orchestration, and automation. In his opinion, as we are moving towards the self-organised networks (SON) and the ICT systems, the advent of 5G, should also move forward this direction. Such an evolution will allow the realisation of novel business cases of the vertical industries, resulting to even higher performances. Especially the use of data analytics together with AI techniques will be a key enabler and decision maker process for such SON networks.</li> <li>- Almost every day they use technology in order to solve operational issues and improve business decision processes. Today all the decisions are information-driven, therefore technology is needed in order to transform data to useful information and patterns from raw data.</li> </ul>

Profile Description	Main answers
	<ul style="list-style-type: none"> <li>- He considers that the future is the haptic Internet and the zero-latency applications. Currently 5G opens the path towards supporting low-latency applications and already this latency has transformed the related vertical industries, from autonomous cars to industry 4.0 and beyond. It seems the breaking further the limit of &lt;10msec towards to B5G systems will further allow the provision of more sensitive applications and use-cases.</li> <li>- Currently the companies are reluctant to host their data outside the company, but the future mandates this. The current trend of edge computing, supported by various vendors, will bring the low latency experience to every company, making more affordable the use of edge cloud (i.e., close proximity cloud) than a private cloud, both in terms of reliability and security.</li> <li>- Following the IaaS and PaaS models, his organisation has already accepted the provision of specific services to be offered from a cloud infrastructure, which has resulted to a more reliable provision. The security of the service depends on the reputation of the IaaS provider and therefore the procurement process for the selection of the provider is of outmost importance.</li> <li>- He considered that the training of AI models, especially in the field of automated networks management is very interesting, since the orchestration of the network resources is a pre-requisite in order to reassure that the expected KPIs from 5G and B5G networks can be met.</li> </ul>
<p>Professor in Computer Science school experienced on edge computing, IoT, big data, cloud computing and blockchain-based services</p>	<ul style="list-style-type: none"> <li>- Three main concerns in the following order: (1) Connectivity. At many parts of developing countries, network connectivity coverage is not guaranteed. Alternative systems making use of usual networks agnostic technologies would be advisable; (2) Cost. While IoT deployments (as a whole) are widely available and are getting cheaper and cheaper in well financed countries and regions, the developing countries encounter huge problems of affordability. Certain companies opt for purchasing just a part of the whole IoT chain /solution (device gateway edge cloud service) while the others remain own crafted, which clearly affects the capacity and innovation pace; (3) Quality of measurements: due to the diversity and quality of devices, quality of measurements is varying (quality of data), strongly impacting on the analytics.</li> <li>- The answer to the question of “making an architecture that will base on IoT, edge, Big Data, AI etc. to be scalable and applicable to cover next generation requirements” should be approached two-fold: <ul style="list-style-type: none"> <li>- The problem of hardware heterogeneity: Nowadays, IoT networks, despite looking like the same (device-&gt;LoRa, Wifi-&gt;Server via MQTT, CoaP or similar), rely on a wide variety of communication technologies, which entail the use of many different equipment. Additionally, single deployments are designed to use specific components for storage, networking, or data encapsulation. In order to cope with this problem, an architecture like ASSIST-IoT’s should design an IoT gateway ultra-flexible, with outstanding capacity for configuration and supporting a myriad of protocols, access technologies, etc. This is an extremely complex challenge.</li> <li>- The problem of software ecosystem constraints: Currently, there are too many software ecosystems applied in IoT deployments. Each of them opts for using one type of processing or another, selecting specific messaging techniques, databases (e.g. Cassandra, InfluxDB, etc.) and tend to be too tailored for specific customers. The objective of ASSIST-IoT should be, there, to develop a flexible software platform with enough connectors and based on open source components to let a wide variety of end-users or customers to configure the tools/software to be used.</li> </ul> </li> <li>- From the viewpoint of pure research, the support of a “zero-latency” system is crucial. From the viewpoint of practical deployments, especially considering the</li> </ul>

Profile Description	Main answers
	<p>Industry/Maintenance field, in most cases, the “zero-latency” is not needed. Only in few application domains like surgery or autonomous cars, a zero-latency system would be required. Additionally, it must be acknowledged that, more often than not, the data generation (sensors, end devices, etc.) and the processing that must be performed over it take longer than network or system-related delays, being more constraining. A clear gap between research and reality is observed here.</p> <ul style="list-style-type: none"> <li>- Bandwidth optimisation will be useful in future IoT deployments for covering other needs than pure “zero-latency”. Bandwidth use reduction must be approached with the purpose of: (i) enabling more end devices to be included in the IoT deployment and (ii) clearing it for peaks of data that will need to be sent under specific conditions. The key aspect here falls to leverage the ever-smarter IoT gateways, that must incorporate software capabilities to specifically select which data (and when) to be delivered through the network. A clear example here is the video camera in one corner of a street. A long period of footage of absolute calm is useless -then the GW should not send any info-, however, a 60-seconds cut when certain events happen is worth to be reported – thus the GW sends the information to the cloud. An additional paramount goal here is a proper and efficient coordination of those decisions between the cloud and the edge/gateway, that must be accurate, dynamic, flexible and with enough amount of configuration margin.</li> <li>- This problem of data accessibility is a sad reality that current developers of IoT systems must assume as unsolvable. If companies (e.g., manufactures) base their functioning on old, inaccessible equipment, the IoT deployment must look to other functionalities and avoid investing heavy effort with those, in many cases.</li> <li>- The most important advance that IoT devices should have is the decoupling from the software ecosystem to be used. If sensors are attached to a specific framework and cloud solution to work with, it is very difficult to use or interconnect them. Other relevant features that IoT devices will need to have are more security, security-by-design (e.g., no one can just eject a SD card and stop the work of the GW and steal the info), reliability, and accuracy.</li> <li>- The resources-federation field is an interesting research topic that, however, is and might be in the future for the academic field. The fact of allowing different entities/locations to take advantage of others’ hardware to compute local processing would make much sense in real industries, but he is not fully confident about that, since the problems of trust that this might generate would generate many ethical and technological issues</li> </ul>
<b>PORT &amp; MARITIME SECTOR</b>	
Site director of Terminal Operator, woman, mid-age, more than 15 years of experience	<ul style="list-style-type: none"> <li>- The most important concerns are IT Security, Lack of Connectivity, Data conversion, and management and control of business processes will be the processes that would benefit the most from a well deployed fully functional ICT solution.</li> <li>- Her impressions regarding unstructured data are that they are very costly and inefficient, as sometimes it only gives a vague answer on which decisions need to be based. Nevertheless, she sees a quite big potential on operational processes improvement based on data analysis, although cannot estimate the percentage.</li> <li>- Despite her sector is improving, they have not achieved a single common source of truth yet.</li> <li>- Hosting company data on cloud-based nodes is always an IT security barrier, but also from the point of view cost, as it sounds cost effective in short term, but is often more expensive than on-premises solutions at the end.</li> <li>- For automation there is a necessity of “zero latency” to control the business, as well as there is a big room for improvement on comfortability of HMI. She believed that a 1-</li> </ul>

Profile Description	Main answers
	minute latency would do. She envisages some operational issues or bottlenecks that may be solved by means of real-time prediction.
CIO of a container terminal holding, man, mid-age, with technical skills but market/business oriented	<ul style="list-style-type: none"> <li>- What we need is to create one universal and open architecture. 5G is seen as the technology which will solve everything, but it is not clear yet, as it should address different machines, which in the case of terminals should be seen as unique devices. In another vein, to have automated operations in our terminals (objective of 5G) there are several challenges, such as speed, latency (the level we have nowadays is not enough for having better applications), bandwidth, or network failures.</li> <li>- Security is not so important for them because they have several an isolated network. With real separation: one network for enterprise devices, other for normal ones, one network not reachable via Internet, etc.</li> <li>- The QoS level is also important in order to have automation container terminals. For instance, redundancy and latency are not enough today in order to have remote control machinery in the whole terminal. To do so, processing data next to the device is important to avoid latency.</li> <li>- They are not comfortable enough with moving to the cloud, even though they do already have some operational applications running in private clouds. They work well the 90% of the time, but cloud-based applications are very complex to be fixed when they have a problem.</li> <li>- The sector needs some homogeneity. They need scalability in order to be able to connect several container terminals (not only the systems we have in one terminal), but at the same time each manufacturer has its own private solution, so that sharing data is very difficult, and there is not one source of truth.</li> </ul>
Responsible of terminal operations in lot of terminals around the world, man, mid-age, telecom engineer, with more than 20 years of experience in the maritime sector	<ul style="list-style-type: none"> <li>- Pain problems for priority order on terminal operations are connectivity with equipment (cranes), safety and security (exchange of data without risks), and the risk to re-invent the wheel trying to increase network capabilities in the industrial environment.</li> <li>- Based on the introductory explanation of ASSIST-IoT objectives, he wondered if is not 5G the standard which will fix the project's needs and requirements. In his opinion, there is no need to create something new or extra to already available communication standards. In fact, diversity of IT solutions across terminals is a big problem. For instance, nowadays does not exist any prospect or reference paper/architecture/standard for the port automation industry. The current problem the sector has today is that each crane manufacturer is trying to create/design a solution by themselves without standards and involving anyone else in the decision. Providers have a bunch of options or possibilities and at the end makes the integration complex.</li> <li>- The problems regarding low layers, which are near to the data access, should be transparent for the terminals. The objective of the terminals should be to develop apps and services with good performance taking advantage of 5G networks and data access protocols. The OSI approach from the ISO is a good example: the suppliers should put the focus in the higher layers without considering previous layers (low level ones). However, there is a risk if those devices and IoT equipment does not fulfil safety parameters and regulations which makes easier their deployment.</li> <li>- The main problem of this industry is the architecture – integrations patterns (who the applications will exchange and interconnect between them) and data consistency models. He foresees ECS as the future in port automation.</li> </ul>
Telecom engineer of the R&D department of a port authority,	<ul style="list-style-type: none"> <li>- In port environments there are many stakeholders with different solutions, so it is difficult to exploit the data extracted from each solution, and therefore, carry out business intelligence developments.</li> </ul>



Profile Description	Main answers
man, mid-age, 1-5 years of experience in the sector	<ul style="list-style-type: none"> <li>- Ports are limited in digitization because they present challenging connectivity scenarios (moving elements, steel containers stacked vertically (with different heights) that block electromagnetic waves transmission, etc). It must also be included that it is somehow an outdated sector in which there is a clear lack of training and an evident rejection to the progress.</li> <li>- Security / privacy is a relevant concern in ports, as at the end, they logistics hub with interconnections among several stakeholders. However, from his point of view, perhaps there is too much overprotection. Furthermore, from the point of view of competitiveness between the different actors in a single port, there is not any data sharing between terminals and port authorities. In his opinion, the first step must start from the necessary harmonization from the port authority, through some common framework.</li> <li>- The final investment by the industrial sector in IoT deployments requires a first real-live contact. For this, the demonstrations carried out withing R&amp;D projects, such as ASSIST-IoT, can help to convince those reluctant parties to consider an IoT Proof-of-Concept as a long-term product commercial solution.</li> <li>- There are certain situations or use cases where it is true that low latencies are needed (such as in automation) which initially are not fulfilled with current systems. It seems that 5G tries to address them, but it is still in its infancy and there are not enough tangible trials that guarantee these automation requirements. In another vein, other lines of research that require ultra-low latencies such as Augmented Reality services do not have a sufficient business area for their final implementation.</li> </ul>
<b>CONSTRUCTION SECTOR</b>	
Transformation manager of a development oriented and technology consulting company that offers end-to-end solutions for smart textiles, woman, mid-age, more than 20 years of experience in the sector	<ul style="list-style-type: none"> <li>- In the case of firefighting/rescuing smart devices are not reliable enough, their reliability in real utility conditions is not confirmed yet. Another issue is related to lack of serial production of such devices, production of such devices is a niche and therefore the production costs are high. The third concern is logistics, as production of Occupational Safety and Health related ICT systems usually requires cooperation of companies with different expertise (e.g., ICT, textiles). The above problems could be solved if there were specifications including such solutions in national tenders.</li> <li>- Interoperability may be an issue which can be solved at the company level. Company should be aware of e.g., potential interferences caused by Bluetooth module to automated production lines.</li> <li>- At the construction site, ICT systems with real-time data processing may have an influence on OSH in prevention of dehydration and overheating by monitoring of skin temperature and skin relative humidity, as well as identification of heart failures. For this purpose, AI methods can be supportive. However, trainings are needed on how to maintain, calibrate sensors, charge batteries etc.</li> <li>- Data management should be compliant with GDPR. An issue is which data company can see and use to avoid actions against the worker.</li> </ul>
Head of digital transformation department of a civil engineering company, man, mid-age, with more than 10 years of experience in the sector	<ul style="list-style-type: none"> <li>- The main challenge in the construction sector is being able to monitor human movements and potential hazardous actions within an ever-changing environment, as opposed to completed fully operational buildings. Some solutions for localisation and asset tracking exist for construction sites, but there is no complete safety IoT systems, only some simple small-scale implementations. To its success, cost and ease of deployment and usage are the decisive factors when considering adopting IoT systems for safety purposes in these construction sites.</li> <li>- Connectivity and speed are also crucial, so that 5G availability would be also very important, as real-time information will be also required in order to manage hazard risks and workers medical and training permits (e.g., risky situations, such as falls,</li> </ul>



Profile Description	Main answers
	<p>need to be detected and acted upon in real time). Hence zero-latency is very important for health and safety applications in the construction sector.</p> <ul style="list-style-type: none"> <li>- There are many parameters of interest to be monitored in order to generate and update a Digital Twin. No commercially available platforms that can host Digital Twins are currently in use by the company or have been considered for any of the company's projects</li> <li>- The company is using the Dalux Field web-platform, hosted on 3<sup>rd</sup> party servers, is used for reporting issues related to quality as well as health and safety; these were previously saved on Excel spreadsheets. The information is primarily used for managing the issues and oversight of subcontractors, but no further analysis is currently performed on these datasets. Within the context of a single construction project, up to a couple of thousand records, which are tagged and searchable, can be manually reported. The company uses the VR headset Oculus Rift to present building information models for marketing purposes or to stakeholders when bidding for tenders, but they are not used within day-to-day BIM workflows.</li> </ul>
<b>AUTOMOTIVE SECTOR</b>	
<p>Technical expert on propulsion systems of an OEM, man, mid-age, industrial engineer, more than 20 years of experience in the sector</p>	<ul style="list-style-type: none"> <li>- Most important concerns: security, safety, and privacy (GDPR).</li> <li>- Their business area is relatively new, and their department are in a ramp up phase, so that still does not rely a lot on ICT systems, but it will be for sure in the future.</li> <li>- The analysis of future data is definitely a tool for improving operational processes, but how long is not clear yet.</li> <li>- There is not really need for zero-latency solutions in their field.</li> <li>- There are sometimes that for the same data value, the technical department analyses it in a way completely different than the financial department.</li> <li>- There are many Python and Python for Edge solutions related with data analysis in the market that they are using or would like to use. However, in the market they are involved, any modification on their products (i.e., cars) based on data analytics is not so easy, as drivers' safety is the most important concern.</li> <li>- There are some positive thoughts about cloud-based company's data hosting, and they indeed they are using some (e.g., Office 365), but it depends on the data type like for instance there should be some kind of GDPR/privacy guarantee for personal data. In addition, there is not an interest on deploying operational applications on cloud, only data.</li> <li>- Automotive industry is joining the IoT ecosystem later than other industry branches. However, when new emerging legislations arise in the future, probably around 2025 or later, the automotive world will probably need some type of dedicated IoT deployment.</li> </ul>
<p>Chief Technical Officer of an industrial automation company focused on automotive OEMs, man, mid-age, more than 15 years of experience</p>	<ul style="list-style-type: none"> <li>- The three most important features demanded for an ICT system are the required application functionality with affordable price, operational stability, and minimal maintenance needs.</li> <li>- A clear structuring of the data is mandatory for the meaningful usage of this data. From where it is coming, why, under which conditions, how trustful is it, for what purpose is it intended to be used, what information should be extracted from this vast amount. Also, an ergonomic usage of this data is very meaningful and helpful. His particular experience has to do with huge production data used to control the quality of the production as well as with training and evaluation data for AI-applications.</li> <li>- Data analysis is for sure supporting their processes. It is not just improving their turnover, but it is a prerequisite to generate it. An AI-based data analysis would additionally allow them to double their expected turnover during the next years.</li> </ul>

Profile Description	Main answers
	<ul style="list-style-type: none"> <li>- They are facing interoperability issues in both directions: having their products interacting with different heterogeneous IT-systems on both edge and cloud-levels of their customers.</li> <li>- There is a real necessity of nearly zero latency in their applications. If the operator is not getting the requested data in real-time, then it will be not able to use the system according to the defined digitalisation process of this workflow. For the various use cases of the different steps of the workflow they can accept latencies of 5-7 min (time from the scanner to the human operator starting the consulting to his next customer), or of a few seconds interaction (between the human data-retrieval-request and the expected answer on his display).</li> <li>- The amounts of the data acquired by their currently deployed IoT system (scanned images from many cars a day) are rather high for the currently typical IT-infrastructure of the final customers. This is true for both local network systems (Ethernet- or Wi-Fi-network) but also their interconnection to central information servers. Even over the night the data pathways are heavily used by several data and information services for other IT-applications running over the years, which creates more bottlenecks for the image transfer needs of their own application. Additional bandwidth upgrades would create non-negligible additional costs.</li> <li>- As they partially have to share the generated information with the final customers (pictures and corresponding annotations about potential vehicles surface defects), they have to use the final-customer storage solutions in addition to their own storage solutions for AI-engineering, so they partially accepts the deployment of operational services in cloud infrastructure, due to the typical application nature of our product.</li> </ul>

### 5.3.3 Online survey

Last, an online survey aiming at gathering participants' feedback regarding the core topics which will be under research during the whole timeframe of the project, and more specific to assess the current adoption and actual needs for the adoption of NG-IoT technologies was carried out. The survey was created with MS Forms tool and was completely voluntary and free. It was published from 15<sup>th</sup> January 2021 until 1<sup>st</sup> February 2021 (Figure 118). The ASSIST-IoT consortium requested to electronically accept an informed consent from any participant who took part, allowing to researcher staffs to gather and analyse participants' inputs, asking for permission to use related observations, or comments as data in project's research, and committing to maintain the confidentiality of the research records or data.



Figure 118. ASSIST-IoT online survey form webpage

Figure 119. ASSIST-IoT social posts for attracting attention to project's online survey

The list of questions (both mandatory and optional) included in the survey were:

1. Which is your current position or role in your company?
2. Which is the core business of your company (e.g., maritime sector, automation, etc.)?
3. How many years are you working on this industry?
4. According to your view, in which category does your company fit better with regards to the level of digitalization and ICT services?
5. Do you use data to make business / operational decisions? What is the temporal range you usually analyse? How is the data you mainly use in your analysis?
6. What is the primary benefit that you receive from the use of ICT services or applications?
7. What are the main tasks you achieve with the support of ICT solutions?
8. What payback you typically ask for an ICT solution? (In years)
9. Please order by importance concerns about ICT systems and data exchange between systems. How do you solve the above problems today?
10. Which departments or organization processes would benefit the most of a well deployed fully functional ICT solution?
11. What is the most important issue or pain you could solve by using ICT if budget were not a problem?
12. What are the three most important features you demand on an ICT system?
13. What is your experience working with vast amount of unstructured data?
14. How often do you use technology in order to solve operational issues or take better decisions?
15. How would you feel if you could no longer use ICT or applications on a daily basis?
16. Do you have to liaise with several heterogeneous sources of information? If so, how often?
17. Do you have to manage different profiles and accounts in order to access different ICT systems for fulfilling your daily duties? Which ones?
18. Do you have the feeling that your business operational processes could be improved if data analysis is performed?
19. Could you estimate the benefit in terms of percentage over your turnover?
20. Do you think that your company is having interoperability issues due to the availability of different heterogeneous sources of information (e.g., each stakeholder owns a different stack of technologies)? If so, does this have a relevant cost for your company?
21. Do you think that there is a real necessity of real-time (zero latency) applications or services for fulfilling your real needs and requirements?
22. In case you have to exchange data with several stakeholders, is there one source of truth common and shared which gives you the opportunity to share information and improve KPIs? Are all the departments in your company aware of that single source of truth?
23. Do all departments agree on numbers (e.g., costs, productivity) or there are disagreements on how each department sees the company KPIs?
24. Have you had any real expertise working with an IoT ecosystem? If so, could you please describe it a little bit (i.e., motivation to set it up, number of devices, etc.)
25. Is the current architecture of IoT devices (if available) deployed in your infrastructure suffering bottlenecks due to the high rate and important amount of data? Do you think these bottlenecks have a significant cost?
26. Do you miss features in current IoT devices?
27. Are the current market features (security, battery life, reliability) adequate for your use cases?
28. Is there any solution for data analysis and processing data in real-time available in the market which you would like to have at your disposal nowadays?
29. Are you confident enough if the data of your company would be sent to a cloud-based node (outside your network)?

30. Would your company accept the deployment of operational applications and services in a cloud infrastructure (outside your network)?
31. What is your main motivation in order to acquire an IoT system which gives you the opportunity to gather and process a lot of data in real-time?
32. If you do not have such systems but you think they would be useful and cost-effective, in which time span do you plan to start the procurement?
33. According to your experience, are you envisaging some kind of scenarios which will solve one of your main problems based on the prediction (in real-time) of hazards or possible dangerous situations?
34. According to your experience, are you envisaging some kind of scenarios that will solve one of your main problems based on the prediction (in real-time) of operational issues, optimization, bottlenecks...?
35. Are the traditional interfaces of the applications and services deployed in your company comfortable enough for you and the rest of your staff (please, bear in mind all the possible roles already available in your company)?
36. Do you have any comments that could help us in researching better and more user-friendly applications for next generation internet for the industry?

The survey was filled in by 25 participants and as it can be seen in the below graphs the majority are or have been working around 1-5 years in the technology/innovation/research departments of software and telecommunications companies, which are considered with respect to their level of digitalization as emerging (i.e., organizations that embrace digital slowly and have modernized some aspects of their business but are largely reactive and only make changes when they have to), or competitive (i.e., companies that have a digital roadmap in place and are starting to combat disruption).

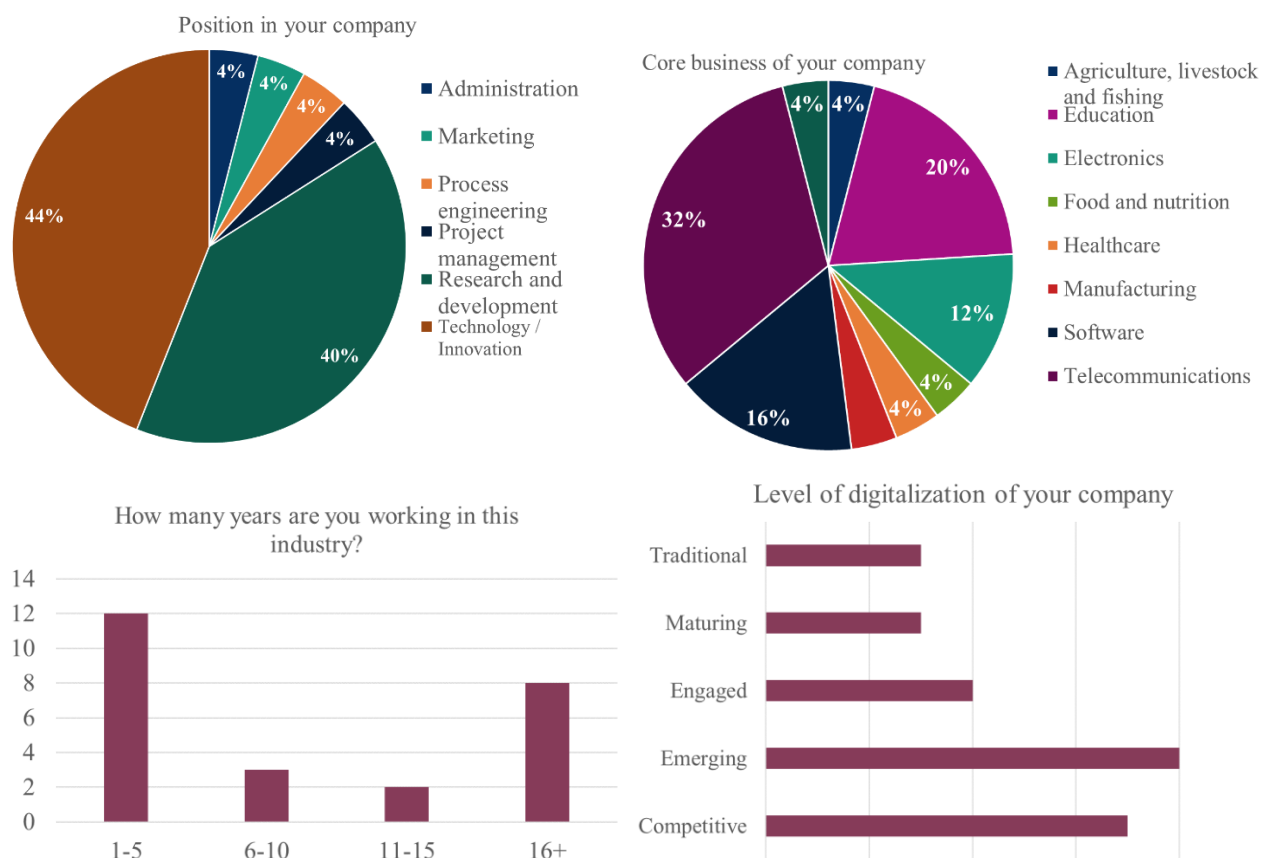
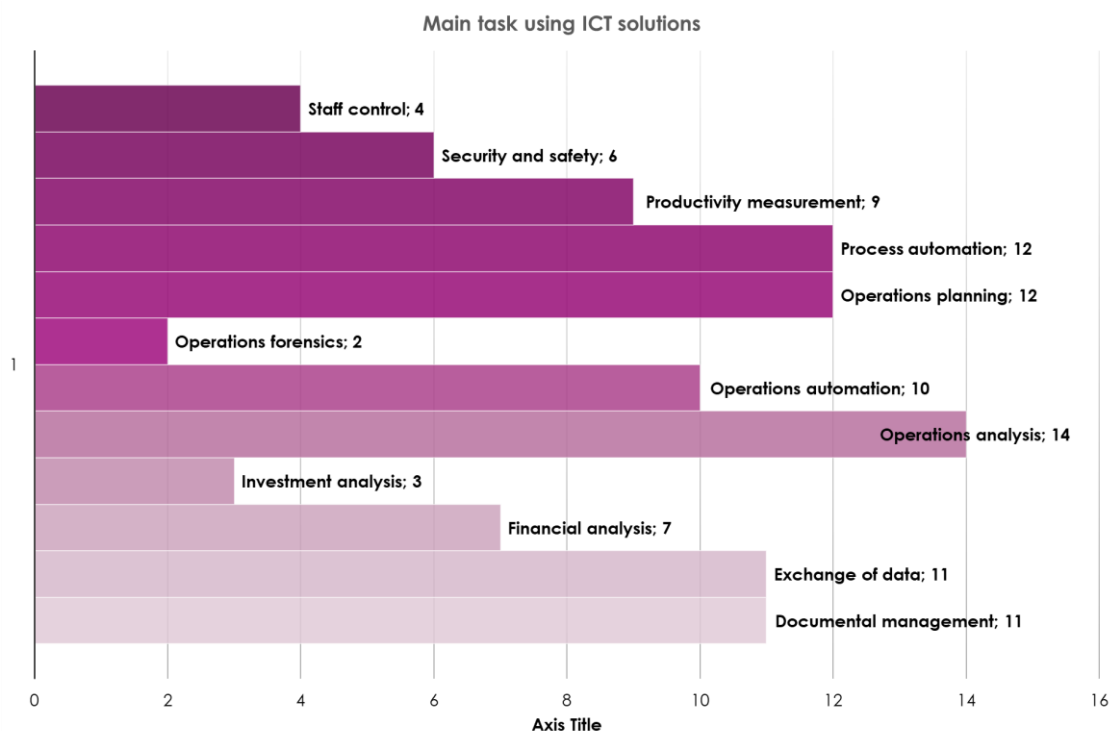


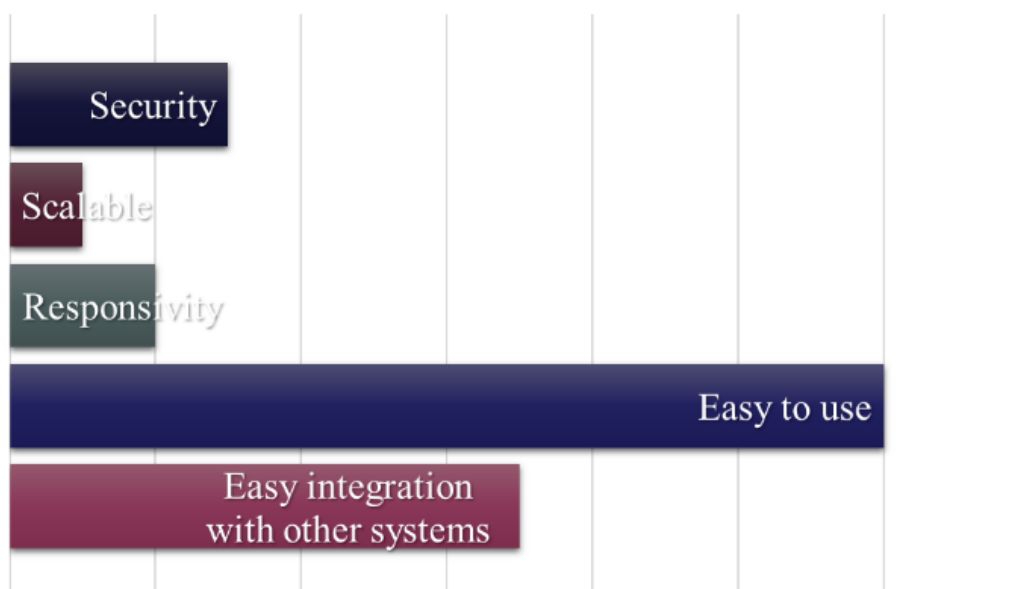
Figure 120. ASSIST-IoT survey participant profiles.

Despite their level of digitalization among their companies, as it can be seen in Figure 121, the three main tasks that are or will be enhanced by making use of ICT solutions are in this order, Operation analysis (which will enable the early identification of needs and requirements before the real need arrives), Operations planning

(which will ensure and accurate and efficient operational task execution), and Process automation (which will enable the automatic execution of some operational tasks without human intervention). To do so, according to the responses in the right side, the most important features demanded for an ICT system is its easiness in the sense of using (i.e., usability), and in the sense of integration with other systems (third-party integration).



### Most important features for an ICT system?



*Figure 121. Main tasks using ICT solutions (top), and most important features required for the successful deployment of an ICT system (bottom).*

The survey respondents agreed that if they could no longer use ICT or applications on a daily basis, they will be either totally blocked (40% of the answers) or would have difficulties to complete their jobs (52% of the answers). On the other hand, for guaranteeing an uninterrupted functioning of their deployed ICT systems, it has been observed that the lack of connectivity and data models' incompatibilities are the most important



concerns (as it can be observed in the spider chart at the right side of Figure 122). Generally, their businesses solve these problems by acquiring new equipment, adding new systems or by subcontracting.

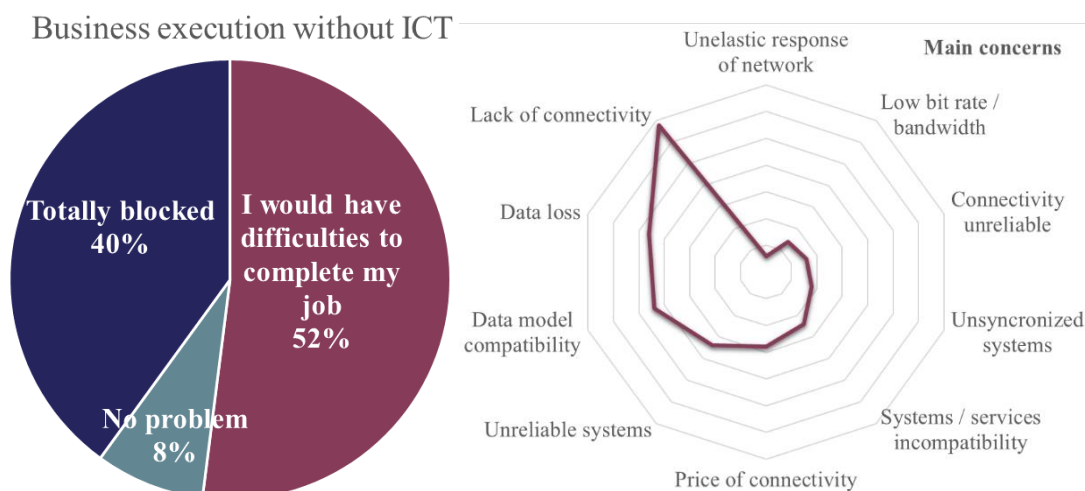


Figure 122. Execution efficiencies without ICT systems (left), and main concerns for ICT proper functioning and deployment (right).

Regarding data heterogeneity, as it can be seen in Figure 123, according to their responses, the 64% of the participants stated that they generally have to liaise with several heterogeneous sources of information (e.g., each stakeholder owns a different stack of technologies), which leads to face with interoperability issues that in the 60% of the cases lessens business and operational decisions. Furthermore, beyond this interoperability stoppage, in case they have to exchange data with different stakeholders, in the 84% of scenarios, there is not a common source of truth, so that they cannot share the information in order to improve their corresponding KPIs.

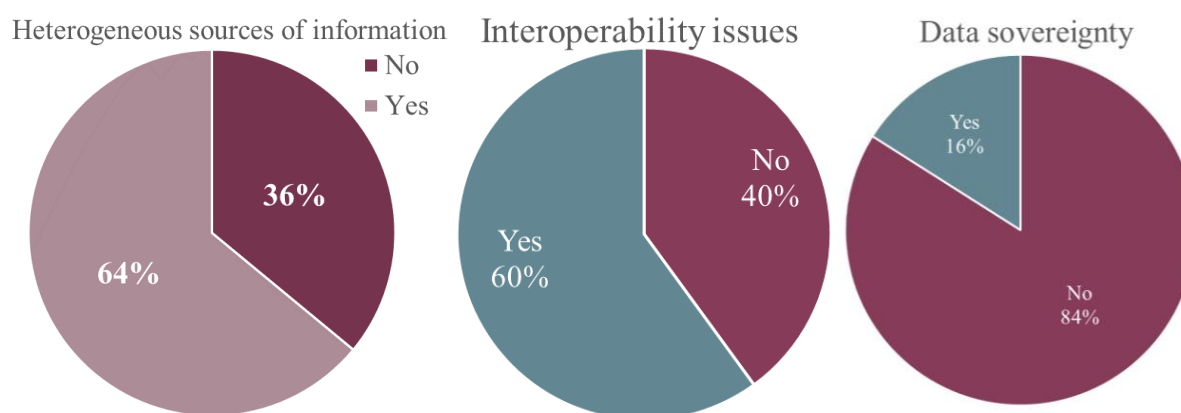


Figure 123. Data management analysis

The next group of questions were associated with the use of data for their inside business operations. According to the answers gathered in the three graphs of Figure 124, it was observed that the 64% of participants use the data gathered from their IoT or ICT systems in order to make operational decisions in a daily or weekly basis. Moreover, 76% of those participants that did not yet use the data extracted from their systems, had the feeling that their business operational processes could be improved if data analysis were performed.

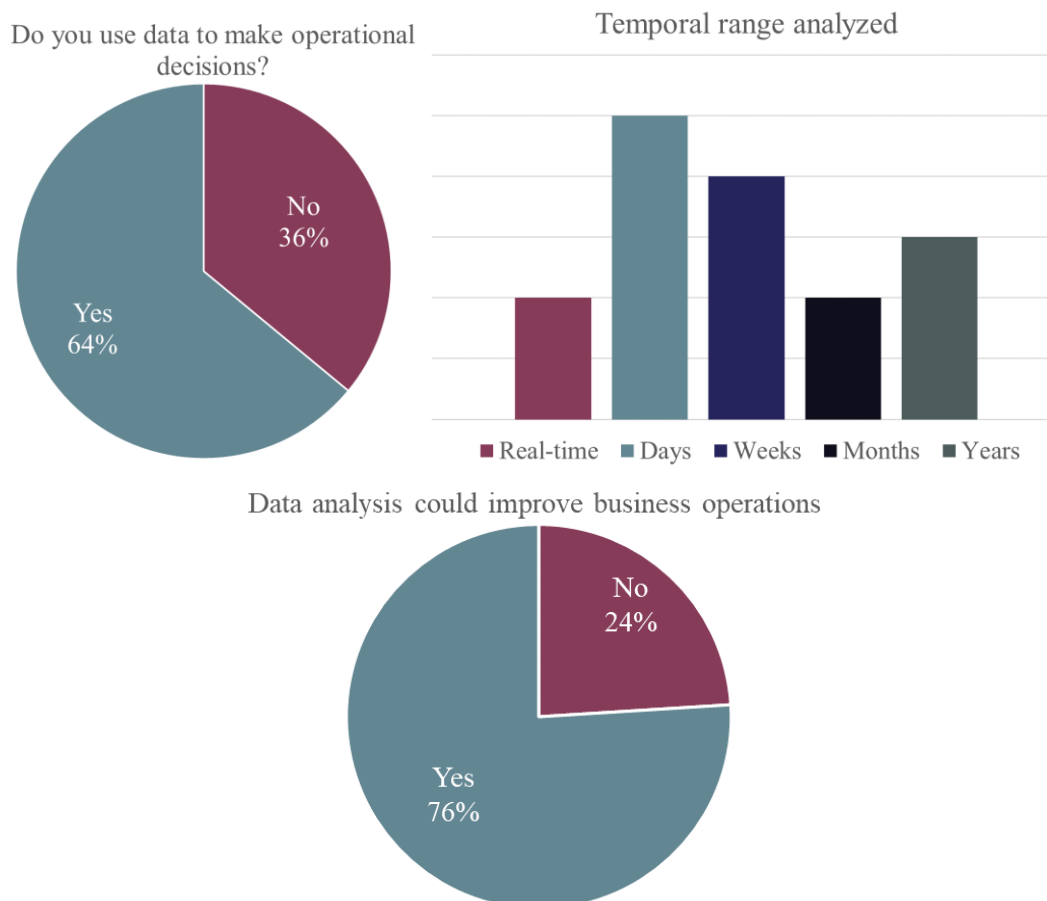


Figure 124. Business operations based on data analysis.

Two of the main features of ASSIST-IoT platform will be the enabling of self-\* and distributed intelligence, which would require to handle a vast amount of unstructured data from the big-data and AI world. After analysing the answers of the online survey, it was observed (see Figure 125), that almost the 50% of the participants are currently facing with this issue, and they had the impression that it is currently quite difficult to retrieve all the relevant data needed for the performance indicators. Probably because of this unexploited use of big-data services, they are not confident or aware of potential solving of hazardous or dangerous situations and operational issues based on real-time predictions.

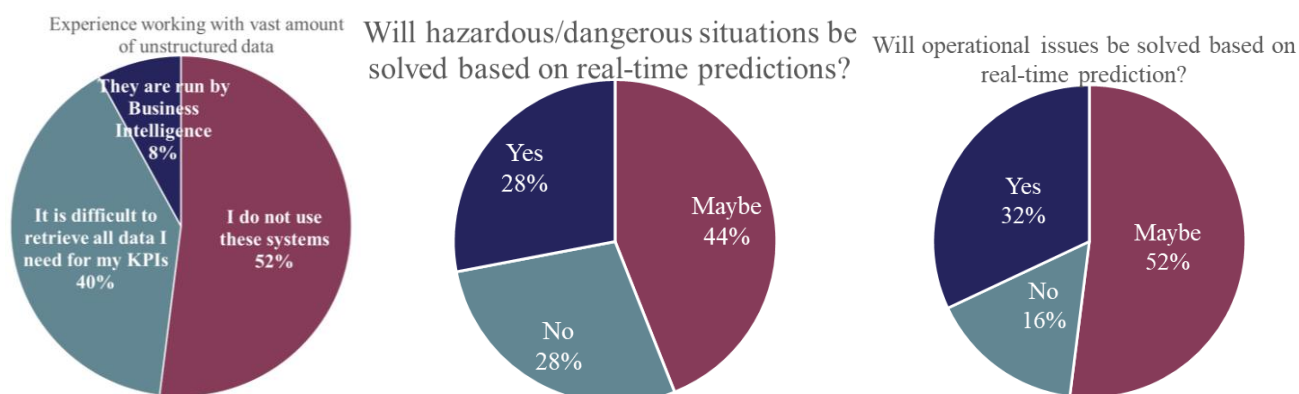


Figure 125. Unstructured data and real-time predictions.

Another pillar of ASSIST-IoT is the hyperconnectivity by making use of cloud and edge/fog continuum. This, would, accordingly, require deploying different NG-IoT services in the cloud. Despite the initial reluctance of sending owned data outside of their premises, it looks that the sector is starting to accept the benefits that cloud and virtualization entails, in terms of operational expenditure and scalability. As it can be observed in left pie graph of Figure 126, around 90% of the answers would accept the deployment of their services in the cloud, but

it should also be noticed that it would probably need around 1-3 years for their acceptance without all their business departments. From ASSIST-IoT perspective, this observation matches with the expected lifetime of the project, so that we could envision a potential success of the NG-IoT platform to be developed.

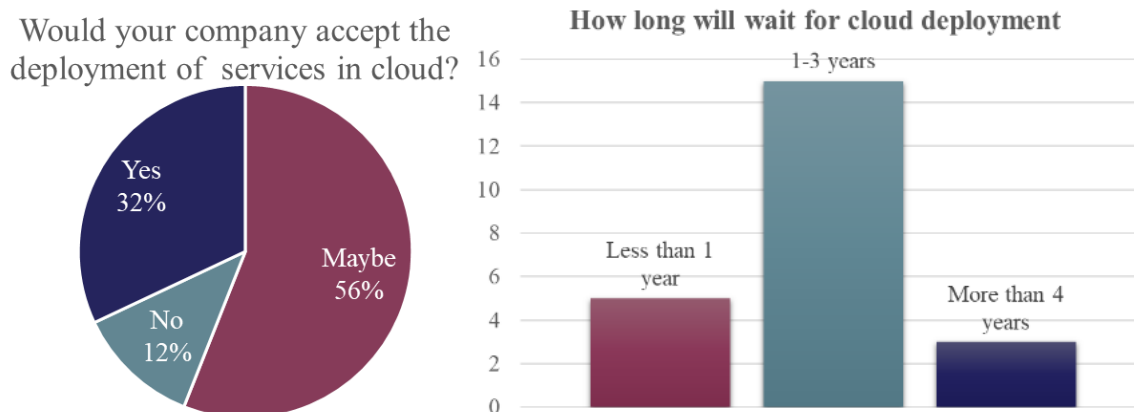


Figure 126. Interest on ICT cloud-based deployments

Last group of questions were related with limitations, needs, and interests on the deployment of new immersive experiences, which will require of extremely high data-rate and ultra-low (ideally zero) latencies. As it can be seen in Figure 127, initially the survey respondents considered in general (84%) that they are not suffering of high data rate bottlenecks in their current IoT architectures and devices. However, since it is considered that there may be zero-latency needs as well as traditional Human-to-Machine Interfaces may not be comfortable enough for the 44% of the respondents, if new immersive services as envisioned by ASSIST-IoT were deployed in a near future, the absence of data rate bottlenecks would be visible (as current IoT systems do not in general stress data rates rather than connection density, which would be the opposite of AR/VR services and applications).

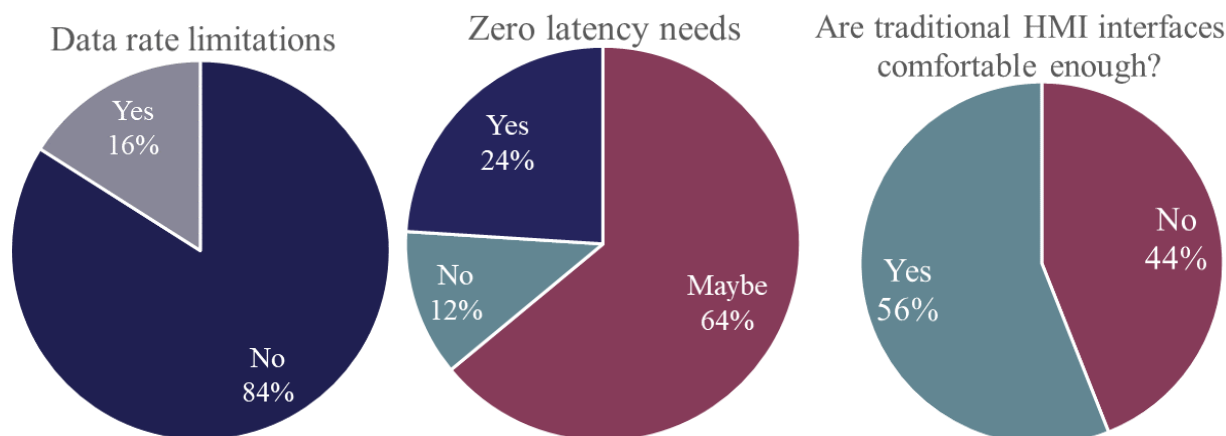


Figure 127. Data rate limitations, zero-latency, and HMI needs.

## 6 Conclusions

The state-of-the-art and market analysis contained in this report has targeted a large variety of technologies, vertical industries, and research initiatives.

On the one hand, the SotA sections cover different emerging technology sectors, including hyperconnectivity, edge/fog computing, interoperability, DLT and semantics, distributed intelligence, self-\*, human-to-machine interfaces, vertical applications of the tactile internet, and IoT cybersecurity, which will form the basis of Next Generation IoT architecture to be designed, developed, and implemented with ASSIST-IoT framework. Some of the main outcomes extracted from the in-depth study of these initiatives are presented next:

- Defining a single Reference Architecture as a blueprint for any potential ASSIST-IoT deployment will be a challenging task. For this reason, even without considering novel NGI enablers, many of them will coexist and their choice among which to instantiate will depend on project's verticals requirements, i.e., port automation, smart safety of workers, and cohesive vehicle monitoring diagnostics. Accordingly, and following NGIoT vision, the resulting technologies that have been identified as key enablers are: Edge Computing, 5G (including NFV features), AI and analytics, AR and Tactile Internet, and Distributed Ledgers.
- In the context of ASSIST-IoT, MEC will only be tackled in the Automotive pilot, when different cars (ECUs and other information included) will connect via 5G to an experimental base station. Therefore, the ASSIST-IoT reference architecture (T3.5) will consider the mechanisms and implementations used in MEC from a pure IoT point of view. There is no need to apply cloudlet schemas to solve ASSIST-IoT use-cases. Hence, initially, this approach will be discarded to be part of ASSIST-IoT. However, the mesh distribution and the overall concepts of data and computation offloading in cloudlets will be considered in T3.5 to be part of the reference architecture (RA) to be delivered out of the project.
- ASSIST-IoT will pay special attention to two types of data interoperability: syntactic interoperability and semantic interoperability. While the syntactic interoperability involves adopting a common data format and common data structure protocols, becoming a prerequisite to semantic interoperability and enables different software components to cooperate, semantic interoperability refers to the ability of computer systems to exchange meaningful data with unambiguous, shared meaning.
- As several IoT challenges are well-documented, including energy efficiency; real-time performance; interoperability; security and privacy, the research on the NG-IoT is ongoing as the need for tackling these challenges is evident. The idea of the semantics as a way to revolutionize the web seemed to profoundly change the sharing of scientific knowledge. In that sense, ASSIST-IoT will be constructed as an information space intended for human understanding, wherein the semantics would allow machines to handle structured data. Naturally, this idea is currently being applied in several IoT areas, where there is the apparent need that all the Things have to communicate with the rest of the world.
- From the distributed intelligence perspective, ASSIST-IoT will mainly focus on the field known as "*distributed problem solving*", in which the main idea is to e.g., assume that a computationally intensive task related to ML has to be undertaken. In this context, AI will involve training neural networks, but also nature inspired optimization, data clustering, etc. For performing such tasks on a single node, a substantial amount of time will be required, so that ASSIST-IoT will assume that multiple computing nodes are available, and the main concerns will be related to how the main task can be decomposed, and how the knowledge, originating from multiple sources can be combined to complete the original task. Furthermore, after the carefully SotA analysis, ASSIST-IoT partners have decided to address the following self-\* features: Self-learning, Self-diagnose, Self-adaptation, Self-organization, and Self-configuration.
- Since ASSIST-IoT involves three industrial sectors (maritime/logistics, construction, and automotive), the Industry 4.0 concept (based on cyber-physical systems, big data analytics and IoT) will be the common thread of the project's architecture and enablers, as there is already many enabling technologies that have not yet reached the required maturity, such as tactile human-centric applications embodied within the Augmented Reality end of the virtuality continuum.

On the other hand, the market analysis has provided some interesting outcomes that justify the future design of ASSIST-IoT solutions in the three pilots and subsequent scenarios of the project. The report is a contribution to the effort to roughly position the project in these markets and provide the necessary context within which the project outputs will operate after ending the project, so that it aims at providing the reader with all the gathered information to fully assess the magnitude and importance of it.

The following conclusions were drawn from the three different stakeholders approach carried out (i.e., workshop, peer-to-peer interviews, and anonymized online survey):

- There is clearly a demand in the market for the NG-IoT solutions that the project intends to develop.
- There are models and tools able to connect the physical world with the digital world. However, they do not use unified interfaces and reference architectures, which would limit the commercial success of NG-IoT solutions if there is not a common standardization framework.
- 5G, cloud/edge-based, and AI analytics are the top-three key innovations that a NG-IoT system should embrace. However, there are several security, safety and privacy concerns that should be guarantee before their operational deployment.
- Partners have now a clearer understanding of the market configuration as well as of the contents and expectations of stakeholders. By demonstrating the convergence of the foreseen solutions with stakeholder expectations, ASSIST-IoT outcomes will likely be successful in the market.



# References

## NGIoT Architectures

- [NG-IoT-1] Ngiot Project, “D3.1. IoT research, innovation and deployment priorities in the EU,” 2020, Online: <https://www.ngiot.eu/wp-content/uploads/sites/26/2020/09/D3.1.pdf>
- [NG-IoT-2] M. W. Maier, D. Emery, and R. Hilliard, “Software architecture: Introducing IEEE standard 1471,” Computer (Long Beach, Calif.), vol. 34, no. 4, pp. 107–109, Apr. 2001.
- [NG-IoT-3] M. Weyrich and C. Ebert, “Reference architectures for the internet of things,” IEEE Softw., vol. 33, no. 1, pp. 112–116, Jan. 2016.
- [NG-IoT-4] IIC, “The Industrial Internet of Things Volume G1: Reference Architecture v1.9,” 2019, Online: <https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf>
- [NG-IoT-5] D. Jo and G. J. Kim, “IoT + AR: pervasive and augmented environments for ‘Digi-log’ shopping experience,” Human-centric Comput. Inf. Sci., vol. 9, no. 1, p. 1, Dec. 2019.
- [NG-IoT-6] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges,” IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1508–1532, Apr. 2019.
- [NG-IoT-7] O. Vermesan et al., “The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge,” in undefined, River Publishers Series in Communications, 2018, pp. 19–102.
- [NG-IoT-8] H. Muccini and M. T. Moghaddam, “IoT architectural styles: A systematic mapping study,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, vol. 11048 LNCS, pp. 68–85.
- [NG-IoT-9] F. Alshohoumi, M. Sarraf, A. AlHamadani, and D. Al-Abri, “Systematic review of existing IoT architectures security and privacy issues and concerns,” Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 7, pp. 232–251, 2019.
- [NG-IoT-10] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” J. Electr. Comput. Eng., vol. 2017, pp. 1–25, 2017.
- [NG-IoT-11] S. Pratap Singh, V. Kumar, A. Kumar Singh, and S. Singh, “A Survey on Internet of Things (IoT): Layer Specific vs. Domain Specific Architecture,” in Lecture Notes on Data Engineering and Communications Technologies, vol. 44, Springer, 2020, pp. 333–341.
- [NG-IoT-12] CREATE-IoT Project, “D6.2. Recommendations for commonalities and interoperability profiles of IoT platforms,” 2018, Online: [https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06\\_02\\_WP06\\_H2020\\_CREATE-IoT\\_Final.pdf](https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_02_WP06_H2020_CREATE-IoT_Final.pdf)
- [NG-IoT-13] M. Bauer and J. W. Walewski, “The IoT architectural reference model as enabler,” in Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model, Springer Berlin Heidelberg, 2013, pp. 17–25.
- [NG-IoT-14] D. T. Ross, “Structured Analysis (SA): A Language for Communicating Ideas,” IEEE Trans. Softw. Eng., vol. SE-3, no. 1, pp. 16–34, 1977.
- [NG-IoT-15] ISO/IEC/IEEE 42010, “ISO/IEC/IEEE 42010 - Systems and software engineering - Architecture description,” 2011, Online: <https://www.iso.org/standard/50508.html>
- [NG-IoT-16] N. Rozanski and E. Woods, Software Systems Architecture: Working With Stakeholders Using Viewpoints and Perspectives. Addison Wesley, 2011.
- [NG-IoT-17] IEEE, “IEEE 1471-2000 - IEEE Recommended Practice for Architectural Description for Software-Intensive Systems,” 2000, Online: <https://standards.ieee.org/standard/1471-2000.html>.

- [NG-IoT-18] IoT-A Project, “D1.5. Final architectural reference model for the IoT,” 2013, Online: [https://www.researchgate.net/publication/272814818\\_Internet\\_of\\_Things\\_-\\_Architecture\\_IoT-A\\_Deliverable\\_D15\\_-\\_Final\\_architectural\\_reference\\_model\\_for\\_the\\_IoT\\_v30](https://www.researchgate.net/publication/272814818_Internet_of_Things_-_Architecture_IoT-A_Deliverable_D15_-_Final_architectural_reference_model_for_the_IoT_v30)
- [NG-IoT-19] ITU-T, “TMN management functions, recommendation M.3400,” 1997, Online: <https://www.itu.int/rec/T-REC-M.3400-200002-I/es>
- [NG-IoT-20] CEN-CENELEC-ETSI Smart Grid Coordination Group, “CEN-CENELEC-ETSI Smart Grid Reference Architecture,” 2012, Online: [https://ec.europa.eu/energy/sites/ener/files/documents/xpert\\_group1\\_reference\\_architecture.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf)
- [NG-IoT-21] NIST, “NISTIR 7628 - Guidelines for smart grid cyber security,” Gaithersburg, MD, Aug. 2010, Online: <http://nvlpubs.nist.gov/nistpubs/ir/2010/NIST.IR.7628.pdf>
- [NG-IoT-22] VDI/VDE Society Measurement and Automatic Control (GMA), “Status Report Reference Architecture Model Industrie 4.0 (RAMI4.0),” 2015, Online: [https://www.zvei.org/fileadmin/user\\_upload/Presse\\_und\\_Medien/Publikationen/2016/januar/GMA\\_Status\\_Report\\_Reference\\_Architecture\\_Model\\_Industrie\\_4.0\\_RAMI\\_4.0\\_/GMA-Status-Report-RAMI-40-July-2015.pdf](https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/GMA_Status_Report_Reference_Architecture_Model_Industrie_4.0_RAMI_4.0_/GMA-Status-Report-RAMI-40-July-2015.pdf)
- [NG-IoT-23] CREATE-IoT Project, “D1.12. EU IoT value chain integration framework,” 2020, Online: [https://european-iot-pilots.eu/wp-content/uploads/2020/06/D01\\_12\\_WP01\\_H2020\\_CREATE-IoT\\_Final.pdf](https://european-iot-pilots.eu/wp-content/uploads/2020/06/D01_12_WP01_H2020_CREATE-IoT_Final.pdf)
- [NG-IoT-24] OpenFog Consortium, “OpenFog Reference Architecture for Fog Computing,” 2017, Online: [http://site.ieee.org/denver-com/files/2017/06/OpenFog\\_Reference\\_Architecture\\_2\\_09\\_17-FINAL-1.pdf](http://site.ieee.org/denver-com/files/2017/06/OpenFog_Reference_Architecture_2_09_17-FINAL-1.pdf)
- [NG-IoT-25] A. Willner and V. Gowtham, “Towards a Reference Architecture Model for Industrial Edge Computing,” Comput. Sci., 2020.
- [NG-IoT-26] SerIoT Project, “D2.1. SerIoT Architecture & Specifications,” 2018, Online: <https://seriot-project.eu/deliverables/>
- [NG-IoT-27] S. K. Singh, S. Rathore, and J. H. Park, “BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence,” Futur. Gener. Comput. Syst., vol. 110, pp. 721–743, Sep. 2020.
- [NG-IoT-28] H. HaddadPajouh, R. Khayami, A. Dehghantanha, K. K. R. Choo, and R. M. Parizi, “AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of things,” Neural Comput. Appl., vol. 32, no. 20, pp. 16119–16133, Oct. 2020.
- [NG-IoT-29] H. Rahimi, A. Zibaenejad, and A. A. Safavi, “A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies,” in 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018, 2019, pp. 81–88.
- [NG-IoT-30] FAR-EDGE Project, “D2.4. FAR-EDGE Architecture and Components Specification,” 2017.
- [NG-IoT-31] MANTIS Project, “D2.9. Reference architecture and design specification final version,” 2018, Online: [http://www.mantis-project.eu/wp-content/uploads/2018/07/D2.9\\_Reference\\_Architecture\\_and\\_Design\\_Specification\\_Final\\_.pdf](http://www.mantis-project.eu/wp-content/uploads/2018/07/D2.9_Reference_Architecture_and_Design_Specification_Final_.pdf)
- [NG-IoT-32] ISO, “ISO 13374-1:2003 - Condition monitoring and diagnostics of machines - Data processing, communication and presentation,” 2003, Online: <https://www.iso.org/standard/21832.html>
- [NG-IoT-33] SynchroniCity Project, “D2.1. Reference Architecture for IoT Enabled Smart Cities,” 2019, Online: [https://synchronicity-iot.eu/wp-content/uploads/2018/05/synchronicity\\_d2\\_1\\_reference\\_architecture\\_for\\_iiot\\_enabled\\_smart\\_cities.pdf](https://synchronicity-iot.eu/wp-content/uploads/2018/05/synchronicity_d2_1_reference_architecture_for_iiot_enabled_smart_cities.pdf)
- [NG-IoT-34] QUALITY Project, “D2.11. Reference Architecture and Blueprints,” 2019, Online: [https://qu4lity.ems-innovalia.org/nfs/programme\\_5/call\\_3/call\\_preparation/QU4LITY\\_D2.11\\_v1.0.pdf](https://qu4lity.ems-innovalia.org/nfs/programme_5/call_3/call_preparation/QU4LITY_D2.11_v1.0.pdf)
- [NG-IoT-35] ESPRESSO Project, “D4.2. Definition of Smart City Reference Architecture,” 2016, Online: <http://espresso.espresso-project.eu/wp-content/uploads/2017/03/D4-17579.2-Smart-City-reference-architecture-report.pdf>

- [NG-IoT-36] DEMETER Project, “D3.1. DEMETER Reference Architecture (Release 1),” 2020, Online: [https://h2020-demeter.eu/wp-content/uploads/2020/10/D3.1-DEMETER-reference-architecture\\_v1.0.pdf](https://h2020-demeter.eu/wp-content/uploads/2020/10/D3.1-DEMETER-reference-architecture_v1.0.pdf)
- [NG-IoT-37] IDSA, “Reference Architecture Model for the Industrial Data Space,” 2017, Online: [https://www.internationaldataspaces.org/wp-content/uploads/dlm\\_uploads/2019/05/Industrial-Data-Space-Reference-Architecture-Model-2017.pdf](https://www.internationaldataspaces.org/wp-content/uploads/dlm_uploads/2019/05/Industrial-Data-Space-Reference-Architecture-Model-2017.pdf)
- [NG-IoT-38] OPEN DEI Project, “D2.1. Reference Architecture for Cross-Domain Digital Transformation V1,” 2020, Online: [https://www.opendei.eu/wp-content/uploads/2020/10/D2.1-REF-ARCH-FOR-CROSS-DOMAIN-DT-V1\\_UPDATED.pdf](https://www.opendei.eu/wp-content/uploads/2020/10/D2.1-REF-ARCH-FOR-CROSS-DOMAIN-DT-V1_UPDATED.pdf)
- [NG-IoT-39] BIG IoT Project, “D2.4. High-level Architecture Specification,” 2017, Online: [http://big-iot.eu/wp-content/uploads/2016/04/BIG-IoT\\_D2.4.b-High\\_Level\\_Architecture\\_Specification\\_V1.0.pdf](http://big-iot.eu/wp-content/uploads/2016/04/BIG-IoT_D2.4.b-High_Level_Architecture_Specification_V1.0.pdf)
- [NG-IoT-40] AIOTI WG03-IoT Standardisation, “High Level Architecture (HLA) Release 4.0,” 2018, Online: <https://aioti.eu/wp-content/uploads/2018/06/AIOTI-HLA-R4.0.7.1-Final.pdf>
- [NG-IoT-41] ONEM2M Technical Specification, “Functional Architecture,” 2019, Online: [https://www.onem2m.org/images/files/deliverables/Release3/TS-0001-Functional\\_Architecture-V3\\_15\\_1.pdf](https://www.onem2m.org/images/files/deliverables/Release3/TS-0001-Functional_Architecture-V3_15_1.pdf)
- [NG-IoT-42] ECC and AII, “Edge Computing Reference Architecture 2.0,” 2017, Online: <http://en.eccconsortium.net/Uploads/file/20180328/1522232376480704.pdf>
- [NG-IoT-43] ITU-T, “Y.2060: Overview of the Internet of things,” 2012, Online: <https://www.itu.int/rec/T-REC-Y.2060-201206-I>
- [NG-IoT-44] ISO/IEC, “ISO/IEC 30141:2018 - Internet of Things (IoT) - Reference Architecture,” 2018, Online: <https://www.iso.org/standard/65695.html>
- [NG-IoT-45] BDVA, “European Big Data Value Strategic Research and Innovation Agenda,” 2017, Online: [https://bdva.eu/sites/default/files/BdVA\\_SRIA\\_v4\\_Ed1.1.pdf](https://bdva.eu/sites/default/files/BdVA_SRIA_v4_Ed1.1.pdf)
- [NG-IoT-46] ISO/IEC, “ISO/IEC 20547-3:2020 - Information technology - Big data reference architecture,” 2020, Online: <https://www.iso.org/standard/71277.html>
- [NG-IoT-47] ETSI, “TS 102 690 Machine-to-Machine communications (M2M); Functional architecture Technical Specification,” 2013, Online: [https://www.etsi.org/deliver/etsi\\_ts/102600\\_102699/102690/01.02.01\\_60/ts\\_102690v010201p.pdf](https://www.etsi.org/deliver/etsi_ts/102600_102699/102690/01.02.01_60/ts_102690v010201p.pdf)
- [NG-IoT-48] CISCO, “The Internet of Things Reference Model,” 2014, Online: [http://cdn.ietf.com/resources/71/IoT\\_Reference\\_Model\\_White\\_Paper\\_June\\_4\\_2014.pdf](http://cdn.ietf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf)
- [NG-IoT-49] Intel, “The Intel IoT Platform - Architecture Specification,” 2015, Online: [http://d885pvm0z6oe.cloudfront.net/hubs/intel\\_80616/assets/downloads/general/Architecture\\_Specification\\_Of\\_An\\_IOT\\_Platform.pdf](http://d885pvm0z6oe.cloudfront.net/hubs/intel_80616/assets/downloads/general/Architecture_Specification_Of_An_IOT_Platform.pdf)
- [NG-IoT-50] Intel and SAP, “IoT Joint Reference Architecture from Intel and SAP,” 2018, Online: <https://www.intel.com/content/dam/www/public/us/en/documents/reference-architectures/sap-iot-reference-architecture.pdf>
- [NG-IoT-51] WSO2, “A Reference Architecture for the Internet of Things,” 2015, Online: <https://wso2.com/whitepapers/a-reference-architecture-for-the-internet-of-things/>
- [NG-IoT-52] Microsoft, “Azure IoT Reference Architecture 2.1 release,” 2018, Online: [https://download.microsoft.com/download/A/4/D/A4DAD253-BC21-41D3-B9D9-87D2AE6F0719/Microsoft\\_Azure\\_IoT\\_Reference\\_Architecture.pdf](https://download.microsoft.com/download/A/4/D/A4DAD253-BC21-41D3-B9D9-87D2AE6F0719/Microsoft_Azure_IoT_Reference_Architecture.pdf)

## Hyperconnectivity

- [HYP-1] A. Quan-Haase and B. Wellman, “Local Virtuality in an Organization: Implications for Community of Practice,” in *Communities and Technologies* 2005, Dordrecht: Springer Netherlands, 2005, pp. 215–238.

- [HYP-2] B. A. A. Nunes, M. Mendonca, X. N. Nguyen, K. Obraczka, and T. Turletti, “A survey of software-defined networking: Past, present, and future of programmable networks,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.
- [HYP-3] A. T. Campbell, I. Katzela, K. Miki, and J. Vicente, “Open signaling for ATM, internet and mobile networks (OPENSIG’98),” *Comput. Commun. Rev.*, vol. 29, no. 1, pp. 97–107, 1999.
- [HYP-4] D. L. Tennenhouse, J. M. Smith, W. D. Sincoskie, D. J. Wetherall, and G. J. Minden, “A survey of active network research,” *IEEE Commun. Mag.*, vol. 35, no. 1, pp. 80–86, 1997.
- [HYP-5] O.N.F., “Software-defined networking: The new norm for networks,” in *ONF White Paper*, 2012, vol. 2, pp. 2–6.
- [HYP-6] F. Hu, Q. Hao, and K. Bao, “A survey on software-defined network and OpenFlow: From concept to implementation,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014.
- [HYP-7] M. S. Bonfim, K. L. Dias, and S. F. L. Fernandes, “Integrated NFV/SDN architectures: A systematic literature review,” *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–39, Feb. 2019.
- [HYP-8] N. McKeown et al., “OpenFlow,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008.
- [HYP-9] R. Masoudi and A. Ghaffari, “Software defined networks: A survey,” *J. Netw. Comput. Appl.*, vol. 67, pp. 1–25, May 2016.
- [HYP-10] A. Rodriguez-Natal et al., “LISP: A southbound SDN protocol?,” *IEEE Commun. Mag.*, vol. 53, no. 7, pp. 201–207, Jul. 2015.
- [HYP-11] P. Vijay Tijare and D. Vasudevan, “IJESRT INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY THE NORTHBOUND APIs OF SOFTWARE DEFINED NETWORKS,” © *Int. J. Eng. Sci. Res. Technol.*, vol. 501, 2016.
- [HYP-12] F. Bannour, S. Souihi, and A. Mellouk, “Distributed SDN Control: Survey, Taxonomy, and Challenges,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 333–354, 2018.
- [HYP-13] F. Wang, H. Wang, B. Lei, and W. Ma, “A research on high-performance SDN controller,” in *Proceedings - 2014 International Conference on Cloud Computing and Big Data, CCBBD 2014*, 2014, pp. 168–174.
- [HYP-14] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, “Software defined networking: State of the art and research challenges,” *Comput. Networks*, vol. 72, pp. 74–98, Oct. 2014.
- [HYP-15] J. Gil Herrera and J. F. Botero, “Resource Allocation in NFV: A Comprehensive Survey,” *IEEE Trans. Netw. Serv. Manag.*, vol. 13, no. 3, pp. 518–532, Sep. 2016.
- [HYP-16] F. Van Lingen et al., “The Unavoidable Convergence of NFV, 5G, and Fog: A Model-Driven Approach to Bridge Cloud and Edge,” *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 28–35, 2017.
- [HYP-17] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, “Network function virtualization: Challenges and opportunities for innovations,” *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.
- [HYP-18] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, “A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements,” *IEEE Access*, vol. 5, pp. 1872–1899, 2017.
- [HYP-19] S. K. Tayyaba, M. A. Shah, O. A. Khan, and A. W. Ahmed, “Software defined network (SDN) based internet of things (IoT): A road ahead,” in *ACM International Conference Proceeding Series*, 2017, vol. Part F1305.
- [HYP-20] S. Namal, I. Ahmad, S. Saud, M. Jokinen, and A. Gurtov, “Implementation of OpenFlow based cognitive radio network architecture: SDN&R,” *Wirel. Networks*, vol. 22, no. 2, pp. 663–677, Jun. 2016.
- [HYP-21] G. Sun, G. Liu, and Y. Wang, “SDN architecture for cognitive radio networks,” in *2014 1st International Workshop on Cognitive Cellular Systems, CCS 2014*, 2014.



- [HYP-22] M. Alenezi, K. Almustafa, and K. A. Meerja, “Cloud based SDN and NFV architectures for IoT infrastructure,” *Egypt. Informatics J.*, vol. 20, no. 1, pp. 1–10, Mar. 2019.
- [HYP-23] Y. Xu, Y. Yan, Z. Dai, and X. Wang, “A management model for SDN-based data center networks,” in *Proceedings - IEEE INFOCOM*, 2014, pp. 113–114.
- [HYP-24] R. K. Rangan, “Trends in SD-WAN and SDN,” *CSI Trans. ICT*, vol. 8, no. 1, pp. 21–27, Mar. 2020.
- [HYP-25] S. K. Routray, M. K. Jha, A. Javali, L. Sharma, S. Sarkar, and T. Ninikrishna, “Software defined networking for optical networks,” in *2016 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics, DISCOVER 2016 - Proceedings*, 2016, pp. 133–137.
- [HYP-26] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, “Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 267–277, Feb. 2019.
- [HYP-27] N. Foster et al., “Languages for software-defined networks,” *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 128–134, Feb. 2013.
- [HYP-28] L. Zhu, M. M. Karim, K. Sharif, F. Li, X. Du, and M. Guizani, “SDN Controllers: Benchmarking & Performance Evaluation,” 2019.
- [HYP-29] Y. Zhang, X. Gong, Y. Hu, W. Wang, and X. Que, “SDNMP: Enabling SDN management using traditional NMS,” in *2015 IEEE International Conference on Communication Workshop, ICCW 2015*, 2015, pp. 357–362.
- [HYP-30] S. Huang, J. Griffioen, and K. L. Calvert, “Network Hypervisors: Enhancing SDN Infrastructure,” *Comput. Commun.*, vol. 46, pp. 87–96, Jun. 2014.
- [HYP-31] G. Sherwood, Rob and Gibb, Glen and Yap, Kok-Kiong and Appenzeller, Guido and Casado, Martin and McKeown, Nick and Parulkar, “FlowVisor: A Network Virtualization Layer,” 2009.
- [HYP-32] A. A. Gebremariam, M. Usman, and M. Qaraqe, “Applications of Artificial Intelligence and Machine Learning in the Area of SDN and NFV: A Survey,” in *16th International Multi-Conference on Systems, Signals and Devices, SSD 2019*, 2019, pp. 545–549.
- [HYP-33] M. Latah and L. Toker, “Artificial intelligence enabled software-defined networking: A comprehensive overview,” *IET Networks*, vol. 8, no. 2, pp. 79–99, Mar. 2019.
- [HYP-34] X. Guibao, M. Yubo, and L. Jialiang, “Inclusion of Artificial Intelligence in Communication Networks and Services,” *ITU J. ICT Discov. Spec. Issue*, no. 1, pp. 1–6, 2017.
- [HYP-35] A. Mestres et al., “Knowledge-defined networking,” *Comput. Commun. Rev.*, vol. 47, no. 3, pp. 1–10, Sep. 2017.
- [HYP-36] N. Abdolmaleki, M. Ahmadi, H. T. Malazi, and S. Milardo, “Fuzzy topology discovery protocol for SDN-based wireless sensor networks,” *Simul. Model. Pract. Theory*, vol. 79, pp. 54–68, 2017.
- [HYP-37] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas, and Y. Wang, “A comprehensive survey of interface protocols for software defined networks,” *J. Netw. Comput. Appl.*, vol. 156, p. 102563, 2020.
- [HYP-38] M. Bansal, J. Mehlman, S. Katti, and P. Levis, *OpenRadio: A Programmable Wireless Dataplane*. 2012.
- [HYP-39] L. Bonati, M. Polese, S. D’Oro, S. Basagni, and T. Melodia, “Open, Programmable, and Virtualized 5G Networks: State-of-the-Art and the Road Ahead,” *Comput. Networks*, vol. 182, p. 107516, 2020.
- [HYP-40] S. K. Singh, R. Singh, and B. Kumbhani, “The Evolution of Radio Access Network Towards Open-RAN: Challenges and Opportunities,” in *2020 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2020 - Proceedings*, 2020, pp. 1–6.
- [HYP-41] H. H. Cho, C. F. Lai, T. K. Shih, and H. C. Chao, “Integration of SDR and SDN for 5G,” *IEEE Access*, vol. 2, pp. 1196–1204, 2014.
- [HYP-42] I. F. Akyildiz, P. Wang, and S. C. Lin, “SoftAir: A software defined networking architecture for 5G wireless systems,” *Comput. Networks*, vol. 85, pp. 1–18, Jul. 2015.



- [HYP-43] L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, “SDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for WIREless Sensor networks,” in Proceedings - IEEE INFOCOM, 2015, vol. 26, pp. 513–521.
- [HYP-44] A. C. Anadiotis, L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, “SD-WISE: A Software-Defined WIREless SENSor network,” Comput. Networks, vol. 159, pp. 84–95, 2019.
- [HYP-45] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao, “Towards programmable enterprise WLANS with Odin,” in HotSDN’12 - Proceedings of the 1st ACM International Workshop on Hot Topics in Software Defined Networks, 2012, pp. 115–120.
- [HYP-46] S. Jain et al., “B4: Experience with a globally-deployed software defined WAN,” in SIGCOMM 2013 - Proceedings of the ACM SIGCOMM 2013 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, 2013, pp. 3–14.
- [HYP-47] C.-Y. Hong, S. Kandula, R. Mahajan, M. Zhang, V. Gill, and M. Nanduri, “Achieving High Utilization with Software-Driven WAN,” ACM SIGCOMM, 2013, Online: <https://www.microsoft.com/en-us/research/publication/achieving-high-utilization-with-software-driven-wan/>
- [HYP-48] C. A. B. Macapuna, C. E. Rothenberg, and M. F. Magalhães, “In-packet bloom filter based data center networking with distributed OpenFlow controllers,” in 2010 IEEE Globecom Workshops, GC’10, 2010, pp. 584–588.
- [HYP-49] V. Mann, A. Vishnoi, K. Kannan, and S. Kalyanaraman, “CrossRoads: Seamless VM mobility across data centers through software defined networking,” in Proceedings of the 2012 IEEE Network Operations and Management Symposium, NOMS 2012, 2012, pp. 88–96.
- [HYP-50] B. Boughzala, R. Ben Ali, M. Lemay, Y. Lemieux, and O. Cherkaoui, “OpenFlow supporting inter-domain virtual machine migration,” in 8th IEEE and IFIP International Conference on Wireless and Optical Communications Networks, WOCN2011, 2011.

## Edge/fog computing

- [EDGE-1] Kiryong Ha et al., “The Impact of Mobile Multimedia Applications on Data Center Consolidation,” in 2013 IEEE International Conference on Cloud Engineering (IC2E), 2013.
- [EDGE-2] “Latency is Critical for IoT Applications in 5G Perspective,” [https://www.vodafone-chair.org/media/publications/philipp-schulz/Latency Critical IoT Applications in 5G Perspective on the Design of Radio Interface and Network Architecture.pdf](https://www.vodafone-chair.org/media/publications/philipp-schulz/Latency%20Critical%20IoT%20Applications%20in%205G%20Perspective%20on%20the%20Design%20of%20Radio%20Interface%20and%20Network%20Architecture.pdf)
- [EDGE-3] C. C. Byers, “Architectural Imperatives for Fog Computing: Use Cases, Requirements, and Architectural Techniques for Fog-Enabled IoT Networks,” IEEE Communications Magazine, vol. 55, no. 8, Aug. 2017.
- [EDGE-4] “Webpages are getting larger every year,” <https://www.pingdom.com/blog/webpages-are-getting-larger-every-year-and-heres-why-it-matters>
- [EDGE-5] <https://medium.com/faun/10-disadvantages-risks-of-cloud-computing-35111de75611>, “10 Disadvantages and Risks of Cloud Computing,” 12-Dec-2020.
- [EDGE-6] “5 Trends Driving 2020’s Gartner Hype Cycle,” <https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020>
- [EDGE-7] “Everything to know about AI,” <https://www.zdnet.com/article/what-is-ai-everything-you-need-to-know-about-artificial-intelligence>
- [EDGE-8] “Fog computing and its role in the Internet of Things,” <https://readwrite.com/2020/10/30/fog-computing-and-its-role-in-the-internet-of-things>
- [EDGE-9] “IDC forecasts 79ZB of data generated by devices in 2025,” <https://futureiot.tech/idc-forecasts-connected-iot-devices-to-generate-79-4zb-of-data-in-2025>

- [EDGE-10] C. Avasalcai, I. Murturi, and S. Dustdar, “Edge and Fog: A Survey, Use Cases, and Future Challenges,” in *Fog Computing*, Wiley, 2020.
- [EDGE-11] “Edge Computing Advantages (Whitepaper) by IIC,” [https://www.iiconsortium.org/pdf/IIC\\_Edge\\_Computing\\_Advantages\\_White\\_Paper\\_2019-10-24.pdf](https://www.iiconsortium.org/pdf/IIC_Edge_Computing_Advantages_White_Paper_2019-10-24.pdf)
- [EDGE-12] S. A. Mostafavi, A. Dawlatnazar, and F. Paydar, “Edge Computing for IoT: Challenges and Solutions,” *Journal of Communications Technology, Electronics and Computer Science*, ISSN 2457-905X, no. 26, 2019.
- [EDGE-13] M. Satyanarayanan et al., “Edge Analytics in the Internet of Things,” *IEEE Pervasive Computing*, vol. 14, no. 2, Apr. 2015.
- [EDGE-14] “LightKone Project - Deliverable D3.1 - Initial Runtime Edge Computing,” [https://wordix.inesctec.pt/wp-lightkone/wp-content/uploads/2019/04/D3.1\\_InitialRuntimeEdgeComputingSystem.pdf](https://wordix.inesctec.pt/wp-lightkone/wp-content/uploads/2019/04/D3.1_InitialRuntimeEdgeComputingSystem.pdf)
- [EDGE-15] “Fog Google - GitHub,” <https://github.com/fog/fog-google>
- [EDGE-16] “AWS vs Cisco Fog Computing and Cloud,” <https://etherealmind.com/aws-iot-vs-cisco-fog-computing-cloud-vs-network-iot>
- [EDGE-17] “Intel, Ericsson and Toyota team up on Automotive Edge Computing,” <https://www.sdxcentral.com/articles/news/intel-ericsson-and-toyota-team-up-on-automotive-edge-computing/2017/08>
- [EDGE-18] “European Commission ICT programme 2018-2020,” [https://cordis.europa.eu/programme/id/H2020\\_ICT-12-2018-2020/es](https://cordis.europa.eu/programme/id/H2020_ICT-12-2018-2020/es)
- [EDGE-19] “Topic ICT-51-2020 call from EC’s H2020 programme,” [https://cordis.europa.eu/programme/id/H2020\\_ICT-51-2020](https://cordis.europa.eu/programme/id/H2020_ICT-51-2020)
- [EDGE-20] “Industrial Internet Consortium (IIC) website,” <https://www.iiconsortium.org>
- [EDGE-21] “Open Edge Computing (OEC) association website,” <https://www.openedgecomputing.org>
- [EDGE-22] ETSI, “Multi-Access Edge Computing (MEC) association website,” <https://www.etsi.org/technologies/multi-access-edge-computing>
- [EDGE-23] “3 Industries with Edge Computing cases,” <https://www.infopulse.com/blog/3-industries-with-edge-computing-use-cases>
- [EDGE-24] “Next steps in the architecture and design of Edge Computing,” <https://www.openstack.org/use-cases/edge-computing/edge-computing-next-steps-in-architecture-design-and-testing>
- [EDGE-25] C. Avasalcai, I. Murturi, and S. Dustdar, “Edge and Fog: A Survey, Use Cases, and Future Challenges,” in *Fog Computing*, Wiley, 2020.
- [EDGE-26] K. Dolui and S. K. Datta, “Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing,” in *2017 Global Internet of Things Summit (GloTS)*, 2017.
- [EDGE-27] ETSI, “NFV Technology Reference,” <https://www.etsi.org/technologies/nfv>
- [EDGE-28] “MQTT official website,” <https://mqtt.org/>
- [EDGE-29] C. C. Byers, “Architectural Imperatives for Fog Computing: Use Cases, Requirements, and Architectural Techniques for Fog-Enabled IoT Networks,” *IEEE Communications Magazine*, vol. 55, no. 8, Aug. 2017.
- [EDGE-30] K. Dolui and S. K. Datta, “Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing,” in *2017 Global Internet of Things Summit (GloTS)*, 2017.
- [EDGE-31] “Beyond fog, edge and cloud computing,” <https://www.e-zigurat.com/innovation-school/blog/beyond-cloud-fog-edge-computing>
- [EDGE-32] R. K. Barik et al., “Mist Data: Leveraging Mist Computing for Secure and Scalable Architecture

for Smart and Connected Health,” *Procedia Computer Science*, vol. 125, 2018.

[EDGE-33] “Arduino Official Website,” <https://www.arduino.cc>

[EDGE-34] Y. Wang, “Definition and Categorization of Dew Computing,” *Open Journal of Cloud Computing (OJCC)*, vol. 3, no. 1, 2016.

[EDGE-35] M. Gusev, “A dew computing solution for IoT streaming devices,” in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2017.

[EDGE-36] M. Gushev, “Dew Computing Architecture for Cyber-Physical Systems and IoT,” *Internet of Things*, vol. 11, Sep. 2020.

[EDGE-37] ETSI, “MEC deployment in 4G and 5G,” [https://www.etsi.org/images/files/ETSIWhitePapers/etsi\\_wp24\\_MEC\\_deployment\\_in\\_4G\\_5G\\_FINAL.pdf](https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf)

[EDGE-38] ETSI, “MEC in 5G,” [https://www.etsi.org/images/files/ETSIWhitePapers/etsi\\_wp28\\_mec\\_in\\_5G\\_FINAL.pdf](https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf)

[EDGE-39] “5G Market Status Report by January 2020,” <https://gsacom.com/paper/5g-market-status-snapshot-january-2020/>

[EDGE-40] M. T. Beck, M. Werner, S. Feld, and T. Schimper, “Mobile Edge Computing: A Taxonomy,” in *AFIN 2014 : The Sixth International Conference on Advances in Future Internet*, 2020.

[EDGE-41] K. Habak, M. Ammar, K. A. Harras, and E. Zegura, “Femto Clouds: Leveraging Mobile Devices to Provide Cloud Service at the Edge,” in *2015 IEEE 8th International Conference on Cloud Computing*, 2015.

[EDGE-42] S. Abdelwahab, B. Hamdaoui, M. Guizani, and T. Znati, “Replisom: Disciplined Tiny Memory Replication for Massive IoT Devices in LTE Edge Cloud,” *IEEE Internet of Things Journal*, vol. 3, no. 3, Jun. 2016.

[EDGE-43] G. Orsini, D. Bade, and W. Lamersdorf, “CloudAware: A Context-Adaptive Middleware for Mobile Edge and Cloud Computing Applications,” in *2016 IEEE 1st International Workshops on Foundations and Applications of Self\* Systems (FAS\*W)*, 2016.

[EDGE-44] IEEE, “CORD - Central Office Re-Architected as a Datacentre,” <https://sdn.ieee.org/newsletter/november-2015/cord-central-office-re-architected-as-a-datacenter>

[EDGE-45] Telefonica, “OnLife Networks Learnings from CORD,” <https://opennetworking.org/wp-content/uploads/2018/12/OnLife-Networks-Learnings-from-CORD-.pdf>

[EDGE-46] ETSI, “ETSI Forge website,” <https://forge.etsi.org/>

[EDGE-47] M. Satyanarayanan, Z. Chen, K. Ha, W. Hu, W. Richter, and P. Pillai, “Cloudlets: at the Leading Edge of Mobile-Cloud Convergence,” in *Proceedings of the 6th International Conference on Mobile Computing, Applications and Services*, 2014.

[EDGE-48] D. Fernández-Cerero, J. Y. Fernández-Rodríguez, J. A. Álvarez-García, L. M. Soria-Morillo, and A. Fernández-Montes, “Single-Board-Computer Clusters for Cloudlet Computing in Internet of Things,” *Sensors*, vol. 19, no. 13, Jul. 2019.

[EDGE-49] H. Elazhary, “Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions,” *Journal of Network and Computer Applications*, vol. 128, Feb. 2019.

[EDGE-50] G. A. Lewis, S. Echeverría, S. Simanta, B. Bradshaw, and J. Root, “Cloudlet-based cyber-foraging for mobile systems in resource-constrained edge environments,” in *Companion Proceedings of the 36th International Conference on Software Engineering*, 2014.

[EDGE-51] M. Satyanarayanan, G. Lewis, E. Morris, S. Simanta, J. Boleng, and K. Ha, “The Role of Cloudlets in Hostile Environments,” *IEEE Pervasive Computing*, vol. 12, no. 4, Oct. 2013.

[EDGE-52] “From Cloud to Cloudlets,” <https://semiengineering.com/from-cloud-to-cloudlets>

[EDGE-53] “Carnegie Mellon University (CMU) official website,” <https://www.cmu.edu>

- [EDGE-54] “Open Edge Computing reference,” <https://www.openedgecomputing.org/>
- [EDGE-55] K. Ha, Z. Chen, W. Hu, W. Richter, P. Pillai, and M. Satyanarayanan, “Towards wearable cognitive assistance,” in Proceedings of the 12th annual international conference on Mobile systems, applications, and services, 2014.
- [EDGE-56] M. Satyanarayanan et al., “An open ecosystem for mobile-cloud convergence,” IEEE Communications Magazine, vol. 53, no. 3, Mar. 2015.
- [EDGE-57] “Internet of Things Agenda: A case of the edge,” <https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Computing-at-the-edge-A-case-of-cloudlets-to-enable-a-smart-edge>
- [EDGE-58] M. Satyanarayanan, V. Bahl, R. Caceres, and N. Davies, “The Case for VM-based Cloudlets in Mobile Computing,” IEEE Pervasive Computing, 2011.
- [EDGE-59] K. A. Khan, Q. Wang, C. Luo, X. Wang, and C. Grecos, “Impact of different cloud deployments on real-time video applications for mobile video cloud users,” 2015.
- [EDGE-60] “Computing at the Edge: A case of cloudlets to enable a smart edge,” <https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Computing-at-the-edge-A-case-of-cloudlets-to-enable-a-smart-edge>
- [EDGE-61] Y. Shi, S. Abhilash, and K. Hwang, “Cloudlet Mesh for Securing Mobile Clouds from Intrusions and Network Attacks,” in 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2015.
- [EDGE-62] E. Cuervo et al., “MAUI,” in Proceedings of the 8th international conference on Mobile systems, applications, and services - MobiSys '10, 2010.
- [EDGE-63] B.-G. Chun, S. Ihm, P. Maniatis, M. Naik, and A. Patti, “CloneCloud,” in Proceedings of the sixth conference on Computer systems - EuroSys '11, 2011.
- [EDGE-64] E. Koukoudidis, D. Lymberopoulos, K. Strauss, J. Liu, and D. Burger, “Pocket cloudlets,” ACM SIGPLAN Notices, vol. 46, no. 3, Mar. 2011.
- [EDGE-65] S. Kosta, A. Aucinas, Pan Hui, R. Mortier, and Xinwen Zhang, “ThinkAir: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading,” in 2012 Proceedings IEEE INFOCOM, 2012.
- [EDGE-66] W. Qing, H. Zheng, W. Ming, and L. Haifeng, “CACTSE: Cloudlet aided cooperative terminals service environment for mobile proximity content delivery,” China Communications, vol. 10, no. 6, Jun. 2013.
- [EDGE-67] D. McCarthy et al., “Personal Cloudlets: Implementing a User-centric Datastore with Privacy Aware Access Control for Cloud-Based Data Platforms,” in 2015 IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity, 2015.
- [EDGE-68] M. Satyanarayanan et al., “Edge Analytics in the Internet of Things,” IEEE Pervasive Computing, vol. 14, no. 2, Apr. 2015.
- [EDGE-69] “VirtualBox official website,” <https://www.virtualbox.org>
- [EDGE-70] “OpenStack official website,” <https://www.openstack.org>
- [EDGE-71] CMU, “Elijah - Cloudlet Computing node,” <http://elijah.cs.cmu.edu>
- [EDGE-72] CMU, “Gabriel - Cloudlet Computing platform,” <https://pypi.org/project/elijah-gabriel>
- [EDGE-73] H. Flores, V. Kostakos, S. Tarkoma, P. Hui, and Y. Li, “Evidence-Aware Mobile Cloud Architectures,” 2018.
- [EDGE-74] OpenStack, “Meghdwar - A Cloudlet Application,” <https://wiki.openstack.org/wiki/Meghdwar>
- [EDGE-75] E. A. S. Mendoza, A. F. da Conceicao, A. H. M. Aliaga, and D. Vieira, “Pytos: A Framework for Mobile Computation Offloading in Python,” in 2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), 2015.



- [EDGE-76] “Amazon AWS Lambda,” <https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>
- [EDGE-77] “OpenNebula website,” <https://opennebula.io>
- [EDGE-78] “OneEdge H2020 Project website,” <https://oneedge.io>
- [EDGE-79] Akamai, “Cloudlets performance,” <https://www.akamai.com/es/es/products/performance/cloudlets>
- [EDGE-80] D. Fernández-Cerero, J. Y. Fernández-Rodríguez, J. A. Álvarez-García, L. M. Soria-Morillo, and A. Fernández-Montes, “Single-Board-Computer Clusters for Cloudlet Computing in Internet of Things,” *Sensors*, vol. 19, no. 13, Jul. 2019.
- [EDGE-81] “Xiaomi MiWifi website,” <http://www.mi.com/miwifi>
- [EDGE-82] Z. Pang, L. Sun, Z. Wang, E. Tian, and S. Yang, “A Survey of Cloudlet Based Mobile Computing,” in *2015 International Conference on Cloud Computing and Big Data (CCBD)*, 2015.
- [EDGE-83] L. Tong, Y. Li, and W. Gao, “A hierarchical edge cloud architecture for mobile computing,” in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, 2016.
- [EDGE-84] T. Verbelen, P. Simoens, F. de Turck, and B. Dhoedt, “Cloudlets,” in *Proceedings of the third ACM workshop on Mobile cloud computing and services - MCS '12*, 2012.
- [EDGE-85] Z. Wang, F. Gao, and X. Jin, “Optimal deployment of cloudlets based on cost and latency in Internet of Things networks,” *Wireless Networks*, vol. 26, no. 8, Nov. 2020.
- [EDGE-86] Z. Xu, W. Liang, W. Xu, M. Jia, and S. Guo, “Efficient Algorithms for Capacitated Cloudlet Placements,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 10, Oct. 2016.
- [EDGE-87] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role on the internet of things,” in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing - MCC '12*, 2012.
- [EDGE-88] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. Goren, and C. Mahmoudi, “Fog computing conceptual model,” Gaithersburg, MD, Mar. 2018.
- [EDGE-89] C. Avasalcai, I. Murturi, and S. Dustdar, “Edge and Fog: A Survey, Use Cases, and Future Challenges,” in *Fog Computing*, Wiley, 2020.
- [EDGE-90] “Raspberry Pi official website,” <https://www.raspberrypi.org>
- [EDGE-91] A. B. Manju and S. Sumathy, “Efficient Load Balancing Algorithm for Task Preprocessing in Fog Computing Environment,” 2019.
- [EDGE-92] C.-C. Lin and J.-W. Yang, “Cost-Efficient Deployment of Fog Computing Systems at Logistics Centers in Industry 4.0,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, Oct. 2018.
- [EDGE-93] F. Bonomi, “Connected Vehicles, the Internet of Things, and Fog Computing,” in *The Eighth ACM International Workshop on Vehicular Inter-NETworking (VANET 2011)*, 2011.
- [EDGE-94] E. Marín-Tordera, X. Masip-Bruin, J. García-Almiñana, A. Jukan, G.-J. Ren, and J. Zhu, “Do we all really know what a fog node is? Current trends towards an open definition,” *Computer Communications*, vol. 109, Sep. 2017.
- [EDGE-95] “Docker official website,” <https://www.docker.com>
- [EDGE-96] W. Steiner and S. Poledna, “Fog computing as enabler for the Industrial Internet of Things,” *e & i Elektrotechnik und Informationstechnik*, vol. 133, no. 7, Nov. 2016.
- [EDGE-97] R. K. Naha, S. Garg, and A. Chan, “Fog-computing architecture: survey and challenges,” in *Big Data-Enabled Internet of Things*, Institution of Engineering and Technology, 2019.
- [EDGE-98] P. Habibi, M. Farhoudi, S. Kazemian, S. Khorsandi, and A. Leon-Garcia, “Fog Computing: A Comprehensive Architectural Survey,” *IEEE Access*, vol. 8, 2020.
- [EDGE-99] A. V. Dastjerdi, H. Gupta, and R. N. Calheiros, “Fog Computing: Principles, Architectures, and Applications,” in *Internet of Things: Principles and Paradigms*.



- [EDGE-100] P. Habibi, S. Baharlooei, M. Farhoudi, S. Kazemian, and S. Khorsandi, “Virtualized SDN-Based End-to-End Reference Architecture for Fog Networking,” in 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2018.
- [EDGE-101] K. Velasquez et al., “Service Orchestration in Fog Environments,” in 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), 2017.
- [EDGE-102] OpenFog Consortium, “OpenFog Reference Architecture for Fog Computing,” [http://site.ieee.org/denver-com/files/2017/06/OpenFog\\_Reference\\_Architecture\\_2\\_09\\_17-FINAL-1.pdf](http://site.ieee.org/denver-com/files/2017/06/OpenFog_Reference_Architecture_2_09_17-FINAL-1.pdf).
- [EDGE-103] “OpenFog Consortium by OPC,” <https://opcfoundation.org/markets-collaboration/openfog/>
- [EDGE-104] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. Goren, and C. Mahmoudi, “Fog computing conceptual model,” Gaithersburg, MD, Mar. 2018.
- [EDGE-105] “Cisco IOX Datasheet,” <https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/iox/datasheet-c78-736767.html>
- [EDGE-106] S. Banerjee, P. Liu, A. Patro, and D. Willis, “ParaDrop,” in Fog for 5G and IoT, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2017.
- [EDGE-107] “Paradrop reference website,” <https://paradrop.org/about>
- [EDGE-108] LFEdege, “LFEdege initiative,” <https://www.lfedge.org/projects/edgexfoundry/>
- [EDGE-109] LFEdege, “EdgeXFoundry official website,” <https://www.edgexfoundry.org/>
- [EDGE-110] “FogLamp-FlEdge code reference,” <https://github.com/foglamp/FogLAMP>
- [EDGE-111] FBK, “Fondazione Bruno Kessler official website,” <https://www.fbk.eu/en/>
- [EDGE-112] Eclipse, “fog05 code reference,” <https://fog05.io/>
- [EDGE-113] “INTER-IoT Project H2020 official website,” <https://inter-iot.eu/>.
- [EDGE-114] A. Yousefpour et al., “All one needs to know about fog computing and related edge computing paradigms: A complete survey,” Journal of Systems Architecture, vol. 98, Sep. 2019.
- [EDGE-115] M. Abderrahim, M. Ouzzif, K. Guilloard, J. Francois, and A. Lebre, “A Holistic Monitoring Service for Fog/Edge Infrastructures: a Foresight Study,” in The IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud 2017), 2017, pp. 337–344.
- [EDGE-116] Opennetworking, “Switch OpenFlow,” <https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf>
- [EDGE-117] C. Mouradian and D. Naboulsi, “A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges,” Distributed, Parallel, and Cluster Computing, 2017.
- [EDGE-118] “Custom Resources extension - Kubernetes,” <https://kubernetes.io/docs/concepts/extend-kubernetes/api-extension/custom-resources>
- [EDGE-119] “StarlingX official website,” <https://www.starlingx.io/software>
- [EDGE-120] “KubeEdge,” <https://kubernetes.io/blog/2019/03/19/kubeedge-k8s-based-edge-intro/>
- [EDGE-121] “KubeFed code reference,” <https://github.com/kubernetes-sigs/kubefed>
- [EDGE-122] OpenStack, “Edge Computing use-cases by OpenStack,” <https://www.openstack.org/use-cases/edge-computing>
- [EDGE-123] Open Edge Computing, “Living Edge Lab by CMU and OEC,” <https://www.openedgecomputing.org/living-edge-lab>
- [EDGE-124] Apache, “OpenWhisk reference description,” <http://openwhisk.apache.org>
- [EDGE-125] “Prometheus DB official reference website,” <https://prometheus.io>
- [EDGE-126] Y. Shi, S. Abhilash, and K. Hwang, “Cloudlet Mesh for Securing Mobile Clouds from Intrusions

and Network Attacks,” in 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2015.

[EDGE-127] T. Yu, X. Wang, and A. Shami, “A Novel Fog Computing Enabled Temporal Data Reduction Scheme in IoT Systems,” in GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017.

## Interoperability

[INT-1] J. ho Park, M. M. Salim, J. H. Jo, J. C. S. Sicato, S. Rathore, and J. H. Park, “CIoT-Net: a scalable cognitive IoT based smart city network architecture,” Human-centric Comput. Inf. Sci., vol. 9, no. 1, p. 29, Dec. 2019.

[INT-2] P. Wegner, “Interoperability,” ACM Comput. Surv., vol. 28, no. 1, pp. 285–287, Mar. 1996.

[INT-3] “Business dictionary.”, Online: <http://www.businessdictionary.com/definition/interoperability.html>

[INT-4] OmniSci, “What is Interoperability? Definition and FAQs.”, Online: <https://www.omnisci.com/technical-glossary/interoperability>

[INT-5] ITU-T, “Y.2060: Overview of the Internet of things,” 2012, Online: <https://www.itu.int/rec/T-REC-Y.2060-201206-I>

[INT-6] O. Vermesan, Advancing IoT Platforms Interoperability. 2018.

[INT-7] M. Ganzha, M. Paprzycki, W. Pawłowski, P. Szmeja, and K. Wasielewska, “Towards semantic interoperability between internet of things platforms,” Internet of Things, vol. 0, no. 9783319612997, pp. 103–127, 2018.

[INT-8] P. Annicchino, A. Brékiné, F. M. Facca, A. Heijnen, and F. M. Castro, “Next Generation Internet of Things Deliverable number D3.1 Deliverable title IoT research, innovation and deployment priorities in the EU White Paper WP number WP3 Lead beneficiary MARTEL Deliverable type Report Dissemination level PU Delivery due month M18 Actual submission month M22,” 2018, Online: <https://www.ngiot.eu/wp-content/uploads/sites/26/2020/09/D3.1.pdf>

[INT-9] “CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT Strategy and coordination plan for IoT interoperability and standard approaches,” Online: [https://european-iot-pilots.eu/wp-content/uploads/2017/10/D06\\_01\\_WP06\\_H2020\\_CREATE-IoT\\_Final.pdf](https://european-iot-pilots.eu/wp-content/uploads/2017/10/D06_01_WP06_H2020_CREATE-IoT_Final.pdf)

[INT-10] M. Noura, M. Atiquzzaman, and M. Gaedke, “Interoperability in Internet of Things: Taxonomies and Open Challenges,” Mob. Networks Appl., vol. 24, no. 3, pp. 796–809, Jun. 2019.

[INT-11] W. Wang, A. Tolk, and W. Wang, “The levels of conceptual interoperability model: applying systems engineering principles to M&S,” 2009.

[INT-12] European Commission, “European Interoperability Framework for Pan-European eGovernment Services.”, p. 79, 2008.

[INT-13] Hans van der Veer (Alcatel-Lucent) and Anthony Wiles (ETSI Secretariat), “Achieving Technical Interoperability-the ETSI Approach,” 2008.

[INT-14] D. D. GROW - Internal Market, “COMMITTEE AND THE COMMITTEE OF THE REGIONS ICT Standardisation Priorities for the Digital Single Market,” Online: <http://is.jrc.ec.europa.eu/pages/ISG/EURIPIDIS/EURIPIDIS.index.html>.

## DLT and semantics

[DLT-1] Feki, M. A., Kawsar, F., Boussard, M., & Trappeniers, L. (2013). The internet of things: the next technological revolution. Computer, 46(2), 24-25.

[DLT-2] Nižetić, S., Djilali, N., Papadopoulos, A., & Rodrigues, J. J. (2019). Smart technologies for promotion of energy efficiency, utilization of sustainable resources and waste management. Journal of cleaner production, 231, 565-591.

- [DLT-3] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8-27.
- [DLT-4] Nikoukar, A., Raza, S., Poole, A., Güneş, M., & Dezfouli, B. (2018). Low-power wireless for the Internet of Things: Standards and applications. *IEEE Access*, 6, 67893-67926.
- [DLT-5] Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, 14(11), 4724-4734.
- [DLT-6] Berners-Lee, T., & Hendler, J. (2001). Publishing on the semantic web. *Nature*, 410(6832), 1023-1024.
- [DLT-7] Ruta, M., Scioscia, F., Ieva, S., Capurso, G., Loseto, G., Gramegna, F., & Di Sciascio, E. (2017). Semantic-enhanced blockchain technology for smart cities and communities. In 3rd Italian conference on ICT.
- [DLT-8] Abou-Nassar, E. M., Ilyasu, A. M., El-Kafrawy, P. M., Song, O. Y., Bashir, A. K., & Abd El-Latif, A. A. (2020). DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE Access*, 8, 111223-111238.
- [DLT-9] Patel, P., Ali, M. I., & Sheth, A. (2018). From raw data to smart manufacturing: AI and semantic web of things for industry 4.0. *IEEE Intelligent Systems*, 33(4), 79-86.
- [DLT-10] Al Ridhawi, I., Aloqaily, M., Boukerche, A., & Jaraweh, Y. (2020, June). A blockchain-based decentralized composition solution for iot services. In 2020 IEEE international conference on communications (ICC) (pp. 1-6).
- [DLT-11] Naim, B. A., & Klas, W. (2019, October). Knowledge Graph-Enhanced Blockchains by Integrating a Graph-Data Service-Layer. In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 420-427). IEEE.
- [DLT-12] Markovic, M., Edwards, P., & Jacobs, N. (2019, October). Recording Provenance of Food Delivery Using IoT, Semantics and Business Blockchain Networks. In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 116-118). IEEE.

## Distributed Intelligence

- [DI-1] Constantin-Valentin Pal, Florin Leon, Marcin Paprzycki, Maria Ganzha, “A Review of Platforms for the Development of Agent Systems”, <https://arxiv.org/abs/2007.08961>
- [DI-2] Claudio Savaglio, et. al., “Agent-based Internet of Things: State-of-the-art and research challenges”, *Future Generation Computer Systems*, 2020, Volume 102, Pages 1038-1053
- [DI-3] [https://www.researchgate.net/publication/35750879\\_Efficient\\_and\\_Accurate\\_Parallel\\_Genetic\\_Algorithms](https://www.researchgate.net/publication/35750879_Efficient_and_Accurate_Parallel_Genetic_Algorithms)
- [DI-4] F.J. Provost, D. N. Hennessey, “Distributed Machine Learning: Scaling up with Coarse-grained Parallelism”, *ISMB-94 Proceedings of AAAI*, 1994
- [DI-5] Chan, P., & Stolfo, S. (1993a). “Meta-Learning for Multistrategy and Parallel Learning”, in *Proceedings of the Second International Workshop on Multistrategy Learning*
- [DI-6] Cook, D., & Holder, L. (1990). Accelerated Learning the Connection Machine. In *Proceedings of the Second IEEE Symposium on Parallel and Distributed Processing*, p. 448-454.
- [DI-7] Philip A Bernstein and Eric Newcomer. 2009. *Principles of transaction processing*. Morgan Kaufmann.
- [DI-8] Ioan Raicu, Ian Foster, Alex Szalay, and Gabriela Turcu. 2006. “Astroportal: A science gateway for large-scale astronomy data analysis”. In *TeraGrid Conference*. 12–15
- [DL-9] J. Verbraeken, et. al., A Survey on Distributed Machine Learning, 2019, <https://arxiv.org/ftp/arxiv/papers/1912/1912.09789.pdf>
- [DI-10] Qinbin Li, et. al., “A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection”, <https://arxiv.org/abs/1907.09693>
- [DI-11] K. Bonawitz et al.. *Towards Federated Learning at Scale: System Design*, SysML 2019

- [DI-12] <https://medium.com/@ODSC/what-is-federated-learning-99c7fc9bc4f5>
- [DI-13] B. Yuan, S. Ge, W. Xing “A Federated Learning Framework for Healthcare IoT devices”, 2020
- [DI-14] Jianmin Chen, Rajat Monga, Samy Bengio, Rafal Jozefowicz Revisiting distributed synchronous SGD, in ICLR Workshop\_Track, 2016
- [DI-15] Brendan McMahan et al. *Communication-Efficient Learning of Deep Networks from Decentralized Data*, 2017
- [DI-16] Jakub Konecny et al. *Federated learning: strategies for improving communication efficiency*
- [DI-17] Jakub Konecny, Peter Richtarik *Randomized distributed mean estimation: Accuracy vs communication*, 2018
- [DI-18] Jia Qian, Xenofon Fafoutis, Lars Kai Hansen, Towards Federated Learning: Robustness to Extremely Unbalanced Data for Edge Computing
- [DI-19] Otkrist Gupta, Ramesh Raskar Distributed learning of deep neural network over multiple agents, Journal of Network and Computer Applications, 2018
- [DI-20] Xinwei Zhang et al. A Federated Learning Framework with Optimal Rates and Adaptivity to Non-IID Data, 2020
- [DI-21] Semih Yagli, Alex Dytso, H. Vincent Poor Information-Theoretic Bounds on the Generalization Error and Privacy Leakage in Federated Learning, 2020
- [DI-22] Ce Ju, et.al. *Federated Transfer Learning for EEG Signal Classification*, 2020
- [DI-23] Geun Hyeong Lee et al. Reliability and Performance Assessment of Federated Learning on Clinical Benchmark Data, 2020
- [DI-24] Hyesung Kim et al. Blockchain On-Device Federated Learning, 2019
- [DI-25] Gan Sun et al. *Data Poisoning Attacks on Federated Machine Learning*, 2020
- [DI-26] Renuga Kanagavelu et al. Two-Phase Multi-Party Computation Enabled Privacy-Preserving Federated Learning, 2020
- [DI-27] A. Hard et al. *Training Keyword Spotting Models on Non-IID Data with Federated Learning*, 2020
- [DI-28] Thomas Hiessl et al. *Industrial Federated Learning – Requirements and System Design*, 2020
- [DI-29] Chenyou Fan, Ping Liu *Federated Generative Adversarial Learning*, 2020
- [DI-30] Qinbin Li , Zeyi Wen, Zhaomin Wu, Sixu Hu, Naibo Wang, Bingsheng He, A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection, <https://arxiv.org/abs/1907.09693>

## Self-\*

- [SELF-1] J.O. Kephart and D. M. Chess. “The Vision of Autonomic Computing.”, 2003, Online: <http://lia.disi.unibo.it/courses/2007-2008/SMA-LS/papers/9/kephart2003a.pdf>
- [SELF-2] An Architectural Blueprint for Autonomic Computing. IBM, eds. , IBM (2005). Online: <https://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf>
- [SELF-3] S. Poslad. Autonomous systems and Artificial Life, In: Ubiquitous Computing Smart Devices, Smart Environments and Smart Interaction. 2009
- [SELF-4] M. R. Nami and K. Bertels, "A Survey of Autonomic Computing Systems," *Third International Conference on Autonomic and Autonomous Systems (ICAS'07)*, Athens, 2007, pp. 26-26, doi: 10.1109/CONIELECOMP.2007.48.
- [SELF-5] <https://www.bbvaopenmind.com/en/technology/digital-world/what-is-autonomic-computing/>

- [SELF-6] McCann JA, Huebscher MC, 2004, Evaluation issues in autonomic computing, Berlin, 3rd international conference on grid and cooperative computing (GCC 2004), Wuhan, Peoples Republic of China, Publisher: Springer-Verlag, Pages: 597-608
- [SELF-7] Thomas R.W., Friend D.H., DaSilva L.A., MacKenzie A.B. (2007) Cognitive Networks. In: Arslan H. (eds) Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems. Springer, Dordrecht. [https://doi.org/10.1007/978-1-4020-5542-3\\_2](https://doi.org/10.1007/978-1-4020-5542-3_2)
- [SELF-8] D. M. Alias and Ragesh G. K, "Cognitive Radio networks: A survey," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1981-1986, doi: 10.1109/WiSPNET.2016.7566489.
- [SELF-9] Wooldridge, Michael (2002). An Introduction to MultiAgent Systems. John Wiley & Sons. p. 366. ISBN 978-0-471-49691-5.
- [SELF-10] C. Savaglio, and G. Fortino, "Autonomic and Cognitive Architectures for the Internet of Things," in Proceedings of the 8th Internet and distributed Computing Systems (IDCS) Int'l Conf., Windsor (UK), 2015, pp. 39-47
- [SELF-11] Manzalini, A., Zambonelli, F.: Towards autonomic and situation-aware communication services: the cascadas vision. In: Distributed Intelligent Systems: Collective Intelligence and Its Applications, 2006. IEEE Workshop on, IEEE 383–388
- [SELF-12] Strassner, J., N. Agoulmine and E. Lehtihet. "FOCALE: A Novel Autonomic Networking Architecture." (2006).
- [SELF-13] Clayman, S., Galis, A.: Inox: A managed service platform for inter-connected smart objects. In: Proc. of the Workshop on IoT and Service Platforms, ACM (2011)
- [SELF-14] Vlacheas, P., Giaffreda, R., et al.: Enabling smart cities through a cognitive management framework for the internet of things. Communications Magazine, IEEE 51(6) (2013) Device Application Loose Coupling
- [SELF-15] C. Savaglio, G. Fortino, and M. Zhou. Towards Interoperable, Cognitive and Autonomic IoT Systems: an Agent-based Approach, 2016.
- [SELF-16] Q.M. Ashraf and M. H. Habaebi. Autonomic schemes for threat mitigation in Internet of Things. Journal of Network and Computer Applications, <https://iotone.ir/shop/public/upload/article/5b8e2de47cf73.pdf>
- [SELF-17] P. R. Lewis, A. Chandra, S. Parsons, E. Robinson, K. Glette, R. Bahsoon, J. Torresen, and X. Yao. A Survey of Self-Awareness and Its Application in Computing Systems. In 2011 Fifth IEEE Conference on Self-Adaptive and Self-Organizing Systems
- [SELF-18] H. Schmeck, C. Muller-Schloer, E. Çakar, M. Mnif, " and U. Richter. Adaptivity and Self-organization in Organic Computing Systems. ACM Trans. Auton. Adapt. Syst., 5(3):10:1–10:32, Sept. 2010.
- [SELF-19] Müller-Schloer, C., Schmeck, H., and Ungerer, T. (eds) (2011). Organic Computing – A Paradigm Shift for Complex Systems. Autonomic Systems. Basel, CH: Birkhäuser Verlag.
- [SELF-20] Tomforde, S., Rudolph, S., Bellman, K., and Würtz, R. (2016). "An organic computing perspective on self-improving system interweaving at runtime," in Proceedings of the 13th IEEE International Conference on Autonomic Computing (ICAC) (Würzburg: IEEE Press), 276–284.
- [SELF-21] Kounev S. et al. (2017) The Notion of Self-aware Computing. In: Kounev S., Kephart J., Milenkoski A., Zhu X. (eds) Self-Aware Computing Systems. Springer, Cham. [https://doi.org/10.1007/978-3-319-47474-8\\_1](https://doi.org/10.1007/978-3-319-47474-8_1)
- [SELF-22] Giese H., Vogel T., Diaconescu A., Götz S., Kounev S. (2017) Architectural Concepts for Self-aware Computing Systems. In: Kounev S., Kephart J., Milenkoski A., Zhu X. (eds) Self-Aware Computing Systems. Springer, Cham. [https://doi.org/10.1007/978-3-319-47474-8\\_5](https://doi.org/10.1007/978-3-319-47474-8_5)



- [SELF-23] Giese H., Vogel T., Diaconescu A., Götz S., Kounev S. (2017) Architectural Concepts for Self-aware Computing Systems. In: Kounev S., Kephart J., Milenkoski A., Zhu X. (eds) Self-Aware Computing Systems. Springer, Cham. [https://doi.org/10.1007/978-3-319-47474-8\\_5](https://doi.org/10.1007/978-3-319-47474-8_5)
- [SELF-24] Jeff Kramer and Jeff Magee. Self-Managed Systems: an Architectural Challenge. In FOSE '07: 2007 Future of Software Engineering, pages 259–268. IEEE, 2007.
- [SELF-25] Laird, John E. (2012). The Soar Cognitive Architecture. MIT Press. ISBN 978-0262122962
- [SELF-26] N.M. Villegas, G. Tamura, H.A. Müller, Chapter 2 - Architecting Software Systems for Runtime Self-Adaptation: Concepts, Models, and Challenges, Editor(s): Ivan Mistrik, Nour Ali, Rick Kazman, John Grundy, Bradley Schmerl,
- [SELF-27] Villegas N.M., Tamura G., Müller H.A., Duchien L., Casallas R. (2013) DYNAMICO: A Reference Model for Governing Control Objectives and Context Relevance in Self-Adaptive Software Systems. In: de Lemos R., Giese H., Müller H.A., Shaw M. (eds) Software Engineering for Self-Adaptive Systems II. Lecture Notes in Computer Science, vol 7475. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-642-35813-5\\_11](https://doi.org/10.1007/978-3-642-35813-5_11)
- [SELF-28] <http://www.ascens-ist.eu/deeco.html>
- [SELF-29] I. Gerostathopoulos, T. Bures, Hnetyinka P., and J. Pacovsky. Using Component Ensembles for Modeling Autonomic Component Collaboration in Smart Farming. Software Engineering for Adaptive and Self-Managing Systems (SEAMS), 2020.
- [SELF-30] M. Kit, I. Gerostathopoulos, T. Bures, and Hnetyinka P. An Architecture Framework for Experimentations with Self-Adaptive Cyber-physical Systems. Software Engineering for Adaptive and Self-Managing Systems (SEAMS), 2015.
- [SELF-31] I. Rodonaia, A. Merabiani, and V. Rodonaia. Application of Autonomic Component Ensembles Methods and Cloud Computing to MDVRPWTM Problem. Journal of Technical Science Technologies, 2017.
- [SELF-32] Aßmann U., Götz S., Jézéquel JM., Morin B., Trapp M. (2014) A Reference Architecture and Roadmap for Models@run.time Systems. In: Bencomo N., France R., Cheng B.H.C., Aßmann U. (eds) Models@run.time. Lecture Notes in Computer Science, vol 8378. Springer, Cham.
- [SELF-33] Giese H. et al. (2017) State of the Art in Architectures for Self-aware Computing Systems. In: Kounev S., Kephart J., Milenkoski A., Zhu X. (eds) Self-Aware Computing Systems. Springer, Cham.
- [SELF-34] Nikil Dutt, Axel Jantsch, and Santanu Sarma. 2016. Toward Smart Embedded Systems: A Self-aware System-on-Chip (SoC) Perspective. ACM Trans. Embed. Comput. Syst. 15, 2, Article 22 (May 2016), 27 pages
- [SELF-35] Sarma, Santanu, et al. "CyberPhysical-System-On-Chip (CPSoC): Sensoractuator rich self-aware computational platform." University of California Irvine, Tech. Rep. CECS-TR-13-06 (2013).
- [SELF-36] S. Sarma, T. Muck, L. A. D. Bathen, N. Dutt and A. Nicolau, "SmartBalance: A sensing-driven linux load balancer for energy efficiency of heterogeneous MPSoCs," 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 2015, pp. 1-6
- [SELF-37] Abeywickrama, D.B., Bicocchi, N., Mamei, M. et al. The SOTA approach to engineering collective adaptive systems. Int J Softw Tools Technol Transfer 22, 399–415 (2020).
- [SELF-38] H. Muccini, M. Sharaf, and D. Weyns. Self-Adaptation for Cyber-Physical Systems: A Systematic Literature Review. 2016.
- [SELF-39] Athreya, A.P. & DeBruhl, Bruce & Tague, Patrick. (2013). Designing for Self-Configuration and Self-Adaptation in the Internet of Things. 585-592.
- [SELF-40] Alwyn Burger, Christopher Cichiwskyj, Stephan Schmeißer, Gregor Schiele. The Elastic Internet of Things - A platform for self-integrating and self-adaptive IoT-systems with support for embedded adaptive hardware. Future Generation Computer Systems, Volume 113, Pages 607-619.
- [SELF-41] <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.696.1092&rep=rep1&type=pdf>

- [SELF-42] P. R. Lewis, M. Platzner, B. Rinner, J. Torresen, and X. Yao, Eds., *Self-aware Computing Systems: An Engineering Approach*. Springer, 2016.
- [SELF-43] S. Kounev, P. Lewis, K. Bellman, N. Bencomo, J. Camara, A. Diaconescu, L. Esterle, K. Geihs, H. Giese, S. Gotz, P. Inverardi, J. Kephart, and A. Zisman, "The " notion of self-aware computing," in *Self-Aware Computing Systems*, S. Kounev, J. O. Kephart, A. Milenkoski, and X. Zhu, Eds., 2017, pp. 3–16.
- [SELF-44] M. Mostl, J. Schlatow, R. Ernst, H. Hoffmann, " A. Merchant, and A. Shraer, "Self-aware systems for the internet-of-things," in *Proc. Int. Conf. on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, Oct 2016, pp. 1–9
- [SELF-45] Esterle, Lukas and B. Rinner. "An Architecture for Self -Aware IOT Applications." 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2018): 6588-6592.
- [SELF-46] Kounev S. et al. (2017) The Notion of Self-aware Computing. In: Kounev S., Kephart J., Milenkoski A., Zhu X. (eds) *Self-Aware Computing Systems*. Springer, Cham.
- [SELF-47] M. R. Nami and K. Bertels, "A Survey of Autonomic Computing Systems," *Third International Conference on Autonomic and Autonomous Systems (ICAS'07)*, Athens, 2007, pp. 26-26, doi: 10.1109/CONIELECOMP.2007.48.
- [SELF-48] McCann JA, Huebscher MC, 2004, Evaluation issues in autonomic computing, Berlin, 3rd international conference on grid and cooperative computing (GCC 2004), Wuhan, Peoples Republic of China, Publisher: Springer-Verlag, Pages: 597-608
- [SELF-49] Anant Agarwal, Jason Miller, Jonathan Eastep, David Wentzlaff, and Harshad Kasture. *Self-aware computing*. Technical Report AFRL-RI-RS-TR-2009-161, MIT, 2009.
- [SELF-50] Lewis P. et al. (2017) Towards a Framework for the Levels and Aspects of Self-aware Computing Systems. In: Kounev S., Kephart J., Milenkoski A., Zhu X. (eds) *Self-Aware Computing Systems*. Springer, Cham.
- [SELF-51] Herbst N. et al. (2017) Metrics and Benchmarks for Self-aware Computing Systems. In: Kounev S., Kephart J., Milenkoski A., Zhu X. (eds) *Self-Aware Computing Systems*. Springer, Cham.
- [SELF-52] L. Esterle and B. Rinner, "An Architecture for Self -Aware IOT Applications," 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, 2018, pp. 6588-6592
- [SELF-53] P. R. Lewis, M. Platzner, B. Rinner, J. Torresen, and X. Yao, Eds., *Self-aware Computing Systems: An Engineering Approach*. Springer, 2016.
- [SELF-54] L. Esterle and B. Rinner, "An Architecture for Self -Aware IOT Applications," 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, 2018, pp. 6588-6592
- [SELF-55] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Secure Comput.*
- [SELF-56] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique and E. Bartocci, "A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems," in *IEEE Access*, vol. 7, pp. 13260-13283, 2019
- [SELF-57] F. P. Preparata, G. Metze and R. T. Chien, "On the Connection Assignment Problem of Diagnosable Systems," in *IEEE Transactions on Electronic Computers*, vol. EC-16, no. 6, pp. 848-854, Dec. 1967
- [SELF-58] Pasquale Antonante, David I. Spivak, Luca Carlone: *Monitoring and Diagnosability of Perception Systems*. CoRR abs/2005.11816 (2020).
- [SELF-59] Tahir, M., Ashraf, Q. M., & Dabbagh, M. (2019, August). Towards Enabling Autonomic Computing in IoT Ecosystem. In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 646-651). IEEE.

- [SELF-60] Ashraf, Q. M., & Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, 49, 112-127.
- [SELF-61] Msadek, N., Soua, R., Ladid, L., & Engel, T. (2018, November). Advancing the Security of Trustworthy Self-IoT. In *2018 International Conference on Smart Communications and Networking (SmartNets)* (pp. 1-7). IEEE.
- [SELF-62] Ge, M., Hong, J. B., Guttman, W., & Kim, D. S. (2017). A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications*, 83, 12-27.
- [SELF-63] Zeng, T., Yang, X., Wan, Y., Mao, Y., & Liu, Z. (2020). Vehicle Transport Security System Based on the Self-Security Intelligence of Radioactive Material. *Science and Technology of Nuclear Installations*, 2020.
- [SELF-64] Zeng, Tiejun and yang, Xiaohua and Wan, Yaping and Liu, Zhenghai and Mao, Yu, *Swarm Self-Security Intelligence System of Radioactive Materials* (December 18, 2019).
- [SELF-65] Zambonelli, F.. “Towards a General Software Engineering Methodology for the Internet of Things.”
- [SELF-66] Fortino G., Re B., Viroli M., Zambonelli F. (2019) Fluidware: An Approach Towards Adaptive and Scalable Programming of the IoT. In: Boreale M., Corradini F., Loreti M., Pugliese R. (eds) *Models, Languages, and Tools for Concurrent and Distributed Programming*. Lecture Notes in Computer Science, vol 11665. Springer, Cham
- [SELF-67] <https://cordis.europa.eu/project/id/027807>
- [SELF-68] <https://cordis.europa.eu/project/id/034567>
- [SELF-69] <https://reflect.pst.ifi.lmu.de/>
- [SELF-70] <https://www.safeadapt.eu/>
- [SELF-71] <http://www.wearhealth.com>
- [SELF-72] <http://pledger-project.eu>
- [SELF-73] <https://www.ibm.com/developerworks/autonomic/books/fpu0mst.htm>

## Human-machine interfaces for collaboration

- [HMI-1] G. Aceto, V. Persico, A. Pescapé, and S. Member, “A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges,” *IEEE Commun. Surv. TUTORIALS*, vol. 21, no. 4, pp. 3467–3501, 2019.
- [HMI-2] V. Alcácer and V. Cruz-Machado, “Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems,” *Eng. Sci. Technol. an Int. J.*, vol. 22, no. 3, pp. 899–919, 2019.
- [HMI-3] L. Da Xu, E. L. Xu, and L. Li, “Industry 4.0: State of the art and future trends,” *Int. J. Prod. Res.*, vol. 56, no. 8, pp. 2941–2962, 2018.
- [HMI-4] A. Ilic and E. Fleisch, “Augmented Reality and the Internet of Things,” Zurich, Switzerland, 2016, Online: <https://www.semanticscholar.org/paper/Augmented-Reality-and-the-Internet-of-Things-Ilic-Fleisch/70ad920303626cc779e5c04cec42e79a497e236c>
- [HMI-5] J. Nuamah and Y. Seong, “Human machine interface on the Internet of Things (IoT),” in *12th System of Systems Engineering Conference, SoSE 2017*, 2017.
- [HMI-6] F. Karray, M. Alemzadeh, J. Abou Saleh, and M. N. Arab, “Human-computer interaction: Overview on state of the art,” *Int. J. Smart Sens. Intell. Syst.*, vol. 1, no. 1, 2008.
- [HMI-7] P. Milgram and F. Kishino, “A Taxonomy of Mixed Reality Visual Displays,” *IEICE Trans. Inf. Syst.*, vol. E77-D, no. 12, pp. 1–15, 1994.

- [HMI-8] E. Oztemel and S. Gursev, “Literature review of Industry 4.0 and related technologies,” *J. Intell. Manuf.*, vol. 31, no. 1, pp. 127–182, 2020.
- [HMI-9] O. Cakmakci and J. Rolland, “Head-worn displays: a review,” *J. Disp. Technol.*, vol. 2, no. 3, pp. 199–216, 2006.
- [HMI-10] F. Zhou, H. B.-L. Dun, and M. Billinghurst, “Trends in augmented reality tracking, interaction and display: A review of ten years of ISMAR,” in *Proceedings - 7th IEEE International Symposium on Mixed and Augmented Reality 2008, ISMAR 2008*, 2008, pp. 193–202.
- [HMI-11] R. Pierdicca, E. Frontoni, R. Pollini, M. Trani, and L. Verdini, “The Use of Augmented Reality Glasses for the Application in Industry 4.0,” in *Augmented Reality, Virtual Reality, and Computer Graphics*, 2017, pp. 389–401.
- [HMI-12] R. Palmarini, J. A. Erkoyuncu, R. Roy, and H. Torabmostaedi, “A systematic review of augmented reality applications in maintenance,” *Robot. Comput. Integr. Manuf.*, vol. 49, no. March 2017, pp. 215–228, 2018.
- [HMI-13] B. J. Dixon, M. J. Daly, H. Chan, A. D. Vescan, I. J. Witterick, and J. C. Irish, “Surgeons blinded by enhanced navigation: the effect of augmented reality on attention,” *Surg. Endosc.*, vol. 27, no. 2, pp. 454–461, 2013.
- [HMI-14] B. J. Dixon, M. J. Daly, H. H. L. Chan, A. Vescan, I. J. Witterick, and J. C. Irish, “Inattentive Blindness Increased with Augmented Reality Surgical Navigation,” *Am. J. Rhinol. Allergy*, vol. 28, no. 5, pp. 433–437, 2014.
- [HMI-15] C. Koch, M. Neges, M. König, and M. Abramovici, “Natural markers for augmented reality-based indoor navigation and facility maintenance,” *Autom. Constr.*, vol. 48, pp. 18–30, 2014.
- [HMI-16] D. K. Baroroh, C. Chu, and L. Wang, “Systematic literature review on augmented reality in smart manufacturing: Collaboration between human and computational intelligence,” *J. Manuf. Syst.*, 2020.
- [HMI-17] P. Fraga-Lamas, T. M. Fernández-Caramés, Ó. Blanco-Novoa, and M. A. Vilar-Montesinos, “A Review on Industrial Augmented Reality Systems for the Industry 4.0 Shipyard,” *IEEE Access*, vol. 6, pp. 13358–13375, 2018.
- [HMI-18] X. Wang, S. K. Ong, and A. Y. C. Nee, “A comprehensive survey of augmented reality assembly research,” *Adv. Manuf.*, vol. 4, no. 1, pp. 1–22, 2016.
- [HMI-19] greenTEG, “CORE.”, Online: <https://www.greenteg.com/core-body-temperature/>
- [HMI-20] Fitbit Inc., “Fitbit.”, Online: <https://www.fitbit.com/global/us/technology/health-metrics>
- [HMI-21] La Roche-Posay, “MySkinTrack UV.”, Online: <https://www.laroche-posay.us/my-skin-track-uv>
- [HMI-22] SHADE, “Shade UV.”, Online: <https://store.wearshade.com/>
- [HMI-23] Y.-S. Kim et al., “All-in-One, Wireless, Stretchable Hybrid Electronics for Smart, Connected, and Ambulatory Physiological Monitoring,” *Adv. Sci.*, vol. 6, no. 17, p. 1900939, 2019.
- [HMI-24] J. Erkoyuncu and S. Khan, “Olfactory-based augmented reality support for industrial maintenance,” *IEEE Access*, vol. 8, pp. 30306–30321, 2020.
- [HMI-25] Microsoft, “Mixed Reality Toolkit.”, Online: <https://microsoft.github.io/MixedRealityToolkit-Unity/README.html>
- [HMI-26] Epic Games Inc., “Unreal Engine.”, Online: <https://www.unrealengine.com/en-US/vr>
- [HMI-27] Apple Inc., “ARKit.”, Online: <https://developer.apple.com/augmented-reality/>
- [HMI-28] Google, “ARCore.”, Online: <https://developers.google.com/ar/discover/>
- [HMI-29] PTC, “Vuforia.”, Online: <https://developer.vuforia.com/>
- [HMI-30] Microsoft, “HoloLens 2.”, Online: <https://www.microsoft.com/en-us/hololens/hardware>
- [HMI-31] Facebook Technologies LLC, “Oculus.”, Online: <https://www.oculus.com/rift/>



- [HMI-32] Seiko Epson Corp., “MOVERIO.”, Online: <https://moverio.epson.com/>
- [HMI-33] Vuzix Corporation, “Vuzix.”, Online: <https://www.vuzix.eu/>
- [HMI-34] Magic Leap Inc., “Magic Leap.”, Online: <https://www.magicleap.com/en-us/magic-leap-1>
- [HMI-35] Iristick, “Iristick.”, Online: <https://iristick.com/products/iristick-z1-premium>
- [HMI-36] REALITY, “Revolutionary projector platform for virtual and augmented reality eyewear,” H2020, 2017., Online: <https://cordis.europa.eu/project/id/756043>
- [HMI-37] VIMS, “Virtual IoT Maintenance System,” H2020, 2019., Online: <https://cordis.europa.eu/project/id/878757>
- [HMI-38] VISCOPIC, “An accessible and versatile Augmented Reality content creation tool for SMEs and large companies,” H2020, 2019., Online: <https://cordis.europa.eu/project/id/878239>
- [HMI-39] AIM, “Augmented Reality Assisted System for Utilities Infrastructure Management,” H2020, 2018., Online: <https://cordis.europa.eu/project/id/807591>
- [HMI-40] LARA, “LBS Augmented Reality Assistive System for Utilities Infrastructure Management through Galileo and EGNOS,” H2020, 2015., Online: <https://cordis.europa.eu/project/id/641460>
- [HMI-41] ImmerSAFE, “Immersive Visual Technologies for Safety-critical Applications,” H2020, 2018., Online: <https://cordis.europa.eu/project/id/764951>
- [HMI-42] ARIESS, “Augmented Reality and Indoor Navigation for Enhanced ASSEMBLY,” H2020, 2017., Online: <https://cordis.europa.eu/project/id/755490>.

## Vertical applications for tactile internet

- [TI-1] N. Promwongsa et al., “A Comprehensive Survey of the Tactile Internet: State-of-the-art and Research Directions,” IEEE Commun. Surv. Tutorials, pp. 1–1, 2020.
- [TI-2] ITU-T, “Tactile Internet.”, Online: <https://www.itu.int/en/ITU-T/techwatch/Pages/tactile-internet.aspx>
- [TI-3] M. Maier, M. Chowdhury, B. P. Rimal, and D. P. Van, “The tactile internet: vision, recent progress, and open challenges,” IEEE Commun. Mag., vol. 54, no. 5, pp. 138–145, May 2016.
- [TI-4] G. P. Fettweis, “The tactile internet: Applications and challenges,” IEEE Veh. Technol. Mag., vol. 9, no. 1, pp. 64–70, Mar. 2014.
- [TI-5] O. Holland et al., “The IEEE 1918.1 ‘tactile Internet’ standards working group and its standards,” Proc. IEEE, vol. 107, no. 2, pp. 256–279, Feb. 2019.
- [TI-6] “IPv6-based Tactile Internet,” Online: [https://portal.etsi.org/webapp/workProgram/Report\\_WorkItem.asp?wki\\_id=47202](https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=47202)
- [TI-7] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis, “5G-Enabled Tactile Internet,” IEEE J. Sel. Areas Commun., vol. 34, no. 3, pp. 460–473, Mar. 2016.
- [TI-8] D. Szabó, A. Gulyás, F. H. P. Fitzek, and D. E. Lucani, “Towards the tactile Internet: Decreasing communication latency with network coding and Software Defined Networking,” in Proceedings of 21st European Wireless Conference, European Wireless 2015, 2015, pp. 1–6.
- [TI-9] A. Aijaz, M. Dohler, A. Hamid Aghvami, V. Friderikos, and M. Frodigh, “Realizing the Tactile Internet: Haptic Communications over Next Generation 5G Cellular Networks,” IEEE Wirel. Commun., vol. 24, no. 2, pp. 82–89, 2017.
- [TI-10] Z. S. Bojkovic, B. M. Bakmaz, and M. R. Bakmaz, “Vision and enabling technologies of tactile internet realization,” in 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications, TELSIKS 2017 - Proceeding, 2017, vol. 2017-Octob, pp. 113–118.



- [TI-11] A. A. Ateya, A. Muthanna, I. Gudkova, A. Abuarqoub, A. Vybornova, and A. Koucheryavy, "Development of intelligent core network for tactile internet and future smart systems," *J. Sens. Actuator Networks*, vol. 7, no. 1, p. 1, 2018.
- [TI-12] J. Prados-Garzon, O. Adamuz-Hinojosa, P. Ameigeiras, J. J. Ramos-Munoz, P. Andres-Maldonado, and J. M. Lopez-Soler, "Handover implementation in a 5G SDN-based mobile network architecture," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2016, vol. 0.
- [TI-13] A. A. Ateya, A. Vybornova, A. Muthanna, A. Koucheryavy, and I. Gudkova, "Intelligent core network for tactile internet system," in *ACM International Conference Proceeding Series*, 2017, vol. Part F1305.
- [TI-14] H. S. Varsha and K. P. Shashikala, "The tactile Internet," in *IEEE International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2017 - Proceedings*, 2017, pp. 419–422.
- [TI-15] D. Van Den Berg et al., "Challenges in haptic communications over the tactile internet," *IEEE Access*, vol. 5, pp. 23502–23518, 2017.
- [TI-16] S. Aggarwal and N. Kumar, "Fog Computing for 5G-Enabled Tactile Internet: Research Issues, Challenges, and Future Research Directions," *Mob. Networks Appl.*, Nov. 2019.
- [TI-17] K. C. Joshi, S. Niknam, R. V. Prasad, and B. Natarajan, "Analyzing the Tradeoffs in Using Millimeter Wave Directional Links for High Data-Rate Tactile Internet Applications," *IEEE Trans. Ind. Informatics*, vol. 16, no. 3, pp. 1924–1932, Mar. 2020.
- [TI-18] M. T. Vega, T. Mehmli, J. Van Der Hooft, T. Wauters, and F. De Turck, "Enabling Virtual Reality for the Tactile Internet: Hurdles and Opportunities," in *14th International Conference on Network and Service Management, CNSM 2018 and Workshops, 1st International Workshop on High-Precision Networks Operations and Control, HiPNet 2018 and 1st Workshop on Segment Routing and Service Function Chaining, SR+SFC 2*, 2018, pp. 378–383.
- [TI-19] K. Antonakoglou, X. Xu, E. Steinbach, T. Mahmoodi, and M. Dohler, "Toward haptic communications over the 5g tactile internet," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3034–3039, 2018.
- [TI-20] E. Steinbach et al., "Haptic codecs for the tactile internet," *Proc. IEEE*, vol. 107, no. 2, pp. 447–470, Feb. 2019.
- [TI-21] S. Haddadin, L. Johannsmeier, and F. Diaz Ledezma, "Tactile robots as a central embodiment of the tactile internet," *Proc. IEEE*, vol. 107, no. 2, pp. 471–487, Feb. 2019.
- [TI-22] A. Aijaz and M. Sooriyabandara, "The tactile internet for industries: A review," *Proc. IEEE*, vol. 107, no. 2, pp. 414–435, Feb. 2019.
- [TI-23] M. Chowdhury and M. Maier, "Collaborative Computing for Advanced Tactile Internet Human-to-Robot (H2R) Communications in Integrated FiWi Multirobot Infrastructures," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2142–2158, 2017.
- [TI-24] E. Wong, M. P. I. Dias, and L. Ruan, "Predictive Resource Allocation for Tactile Internet Capable Passive Optical LANs," *J. Light. Technol.*, vol. 35, no. 13, pp. 2629–2641, Jul. 2017.
- [TI-25] O. Khatib et al., "Ocean one: A robotic avatar for oceanic discovery," *IEEE Robot. Autom. Mag.*, vol. 23, no. 4, pp. 20–29, 2016.
- [TI-26] M. Wrzesien et al., "Treating small animal phobias using a projective-augmented reality system: A single-case study," *Comput. Human Behav.*, vol. 49, pp. 343–353, 2015.
- [TI-27] C. Grasso and G. Schembra, "Design of a UAV-Based Videosurveillance System with Tactile Internet Constraints in a 5G Ecosystem," in *2018 4th IEEE Conference on Network Softwarization and Workshops, NetSoft 2018*, 2018, pp. 132–140.
- [TI-28] M. S. Elbamby, C. Perfecto, M. Bennis, and K. Doppler, "Toward Low-Latency and Ultra-Reliable Virtual Reality," *IEEE Netw.*, vol. 32, no. 2, pp. 78–84, Mar. 2018.
- [TI-29] S. Tanwar, S. Tyagi, I. Budhiraja, and N. Kumar, "Tactile Internet for Autonomous Vehicles: Latency and Reliability Analysis," *IEEE Wirel. Commun.*, vol. 26, no. 4, pp. 66–72, 2019.

- [TI-30] H. Cao, S. Gangakhedkar, A. R. Ali, M. Gharba, and J. Eichinger, “A 5G V2X testbed for cooperative automated driving,” in IEEE Vehicular Networking Conference, VNC, 2016, vol. 0.
- [TI-31] X. Wei, Q. Duan, and L. Zhou, “A QoE-Driven Tactile Internet Architecture for Smart City,” IEEE Netw., vol. 34, no. 1, pp. 130–136, 2020.
- [TI-32] M. F. Zhani and H. ElBakoury, “FlexNGIA: A Flexible Internet Architecture for the Next-Generation Tactile Internet,” J. Netw. Syst. Manag., vol. 28, no. 4, pp. 751–795, Mar. 2020.

## IoT Security and software development using DevSecOps on IoT ecosystems

- [IoTDSO-1] ENISA Security Measures. Good practices for IoT and Smart Infrastructures Too <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT>
- [IoTDSO-2] DevOps definition, and differences from CD/CI <https://www.itproportal.com/features/stop-messing-up-with-cicd-vs-devops-and-learn-the-difference-finally/>
- [IoTDSO-3] A. Brown, M. Sthanke, N. Kersten, et al. “State of DevOps Report.” Puppet, 2020, <https://puppet.com/resources/report/2020-state-of-devops-report>
- [IoTDSO-4] Rakesh Kumar, Rinkaj Goyal, July 2020 “Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud ADOC”

## State of the Art in Port Automation

- [PA-1] P. Beaumont, “Cybersecurity Risks and Automated Maritime Container Terminals in the Age of 4IR,” in Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution, IGI Global, 2018, pp. 497–516.
- [PA-2] K. Rintanen and A. Thomas, “Container terminal automation,” 2016.
- [PA-3] I. de la Peña Zarzuelo, M. J. Freire Soeane, and B. López Bermúdez, “Industry 4.0 in the port and maritime industry: A literature review,” J. Ind. Inf. Integr., vol. 20, p. 100173, 2020.
- [PA-4] A. M. Martín-Soberón, A. Monfort, R. Sapiña, N. Monterde, and D. Caldach, “Automation in Port Container Terminals,” Procedia - Soc. Behav. Sci., vol. 160, no. Cit, pp. 195–204, 2014.
- [PA-5] N. Zrnić, Z. Petković, and S. Bošnjak, “Automation of ship-to-shore container cranes: A review of state-of-the-art,” FME Trans., vol. 33, no. 3, pp. 111–121, 2005.
- [PA-6] C. Mi, Z. Zhang, Y. Huang, and Y. Shen, “A fast automated vision system for container corner casting recognition,” J. Mar. Sci. Technol., vol. 24, no. 1, pp. 54–60, 2016.
- [PA-7] Y. Yang, M. Zhong, H. Yao, F. Yu, X. Fu, and O. Postolache, “Internet of things for smart ports: Technologies and challenges,” IEEE Instrum. Meas. Mag., vol. 21, no. 1, pp. 34–43, 2018.
- [PA-8] S. Pihkala and C. Malesci, “Wirelessly connecting RTGs for remote and automated operations,” 2020.
- [PA-9] R. Kompany, “5G and MEC can significantly improve smart port operations,” 2019, Online: <https://www.analysismason.com/Research/Content/Comments/5g-mec-ports-rma18/>
- [PA-10] M. Etienne, S. Khan, and M. Eakambaram, “Modern ships and ports,” 2020.
- [PA-11] L. Heillig, E. Lalla-Ruiz, “Machine Learning in Container Terminals”, Port Technology Information (PTI), Edition 83, May 2019.
- [PA-12] M. Anwar, “Digitalization in Container Terminal Logistics: A Literature Review,” in 27th Annual Conference of International Association of Maritime Economists (IAME):, 2019, pp. 1–25.
- [PA-13] M. Francisconi, “An explorative study on blockchain technology in application to port logistics,” TU Delft, 2017.

- [PA-14] TradeLens Collaboration, “TradeLens,” GTD Solution Inc. and IBM, 2020, Online: <https://www.tradelens.com/>
- [PA-15] IBM, “Digitizing Global Trade with Maersk and IBM,” 2018., Online: <https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/>
- [PA-16] M. Oude Weernink, W. Van Den Engh, M. Francisconi, and F. Thorborg, “The Blockchain Potential for Port Logistics,” Erasmus Univ. Delft Univ. Technol., no. 2 January 2018, p. 16, 2017.
- [PA-17] N. Ndraha, H.-I. Hsiao, J. Vljajic, M.-F. Yang, and H.-T. V. Lin, “Time-temperature abuse in the food cold chain: Review of issues, challenges, and recommendations,” Food Control, vol. 89, pp. 12–21, 2018.
- [PA-18] iTerminals 4.0, “Application of Industry 4.0 Technologies towards Digital Port Container Terminals,” 2018., Online: <https://iterminalsproject.eu/>
- [PA-19] Horizon 2020, “Capacity with a pOsitive enviRonmEntal and societAL footprInt: portS in the future era,” 2018., Online: <https://cordis.europa.eu/project/id/768994>
- [PA-20] Horizon 2020, “Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain,” 2019. , Online: <https://cordis.europa.eu/project/id/833389>
- [PA-21] Horizon 2020, “Port IoT for Environmental Leverage,” 2018. , Online: <https://cordis.europa.eu/project/id/769355>
- [PA-22] MarineInsight, “Rolls-Royce Offers Ship Navigators A Bird’s-Eye View With Intelligent Awareness Game-Changer,” 2018m Online: <https://www.marineinsight.com/shipping-news/rolls-royce-offers-ship-navigators-a-birds-eye-view-with-intelligent-awareness-game-changer/>
- [PA-23] I. Parolas, “ETA prediction for containerships at the Port of Rotterdam using Machine Learning Techniques,” TU Delft, 2016.
- [PA-24] R. O’Dwyer, “AI-based marine traffic control tested in Singapore,” 2019, Online: <https://smartmaritimene트워크.com/2019/04/03/ai-based-marine-traffic-control-tested-in-singapore/>
- [PA-25] R. Cardone, “The 5G Port of the Future,” 2020. , Online: <https://www.ericsson.com/en/blog/2020/7/the-5g-port-of-the-future>
- [PA-26] Huawei, “Working with China Telecom Huawei will Build the MEC Network of Ningbo Zhenhai Smart Refinery,” 2017.
- [PA-27] “Port Call Optimization,” International Taksforce., Online: <https://portcalloptimization.org/>
- [PA-28] “Terminal Industry Committee 4.0.”, Online: <https://tic40.org/>
- [PA-29] “Digital Container Shipping Association.”, Online: <https://dcsa.org/>

## State of the Art in Smart Safety of Workers

- [SSW-1] A. Sawhney, M. Riley, and J. Irizarry, Construction 4.0, 1st Editio. 2020.
- [SSW-2] H. Li, M. Lu, S. Hsu, M. Gray, and T. Huang, “Proactive behavior-based safety management for construction safety improvement,” Saf. Sci., vol. 75, pp. 107–117, 2015.
- [SSW-3] W. Fang, P. E. D. Love, H. Luo, and L. Ding, “Computer vision for behaviour-based safety in construction: A review and future directions,” Adv. Eng. Informatics, vol. 43, no. November 2019, p. 100980, 2020.
- [SSW-4] D. Cooper, “Implementing The Behaviour-Based Approach: A Practical Guide,” Heal. Saf. Pract., vol. 12, no. 11, pp. 18–23, 1994.
- [SSW-5] A. R. Duff, I. T. Robertson, R. A. Phillips, and M. D. Cooper, “Improving safety by the modification of behaviour,” Constr. Manag. Econ., vol. 12, no. 1, pp. 67–78, 1994.

- [SSW-6] D. Podgórski, K. Majchrzycka, A. Dąbrowska, G. Gralewicz, and M. Okrasa, “Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies,” *Int. J. Occup. Saf. Ergon.*, vol. 23, no. 1, 2017.
- [SSW-7] D. Podgórski, “Enhancing OSH management processes through the use of smart personal protective equipment, wearables and Internet of Things technologies,” in *New Opportunities and Challenges in Occupational Safety and Health Management*, D. Podgórski, Ed. CRC Press Taylor & Francis Group, 2020, pp. 125–164.
- [SSW-8] R. Kanan, O. Elhassan, and R. Bensalem, “An IoT-based autonomous system for workers’ safety in construction sites with real-time alarming, monitoring, and positioning strategies,” *Autom. Constr.*, vol. 88, no. January, pp. 73–86, 2018.
- [SSW-9] T. D. Akinosho et al., “Deep learning in the construction industry: A review of present status and future innovations,” *J. Build. Eng.*, vol. 32, p. 101827, Nov. 2020.
- [SSW-10] R. Y. Ma Li, “Smart construction safety in road repairing works,” in *Procedia Computer Science*, 2017, vol. 111, pp. 301–307.
- [SSW-11] S. Tang, D. R. Shelden, C. M. Eastman, P. Pishdad-Bozorgi, and X. Gao, “A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends,” *Automation in Construction*, vol. 101. Elsevier B.V., pp. 127–139, May-2019.
- [SSW-12] J. Teizer, T. Cheng, and Y. Fang, “Location tracking and data visualization technology to advance construction ironworkers’ education and training in safety and productivity,” *Autom. Constr.*, vol. 35, pp. 53–68, Nov. 2013.
- [SSW-13] H. Li, M. Lu, G. Chan, and M. Skitmore, “Proactive training system for safe and efficient precast installation,” *Autom. Constr.*, vol. 49, no. PA, pp. 163–174, Jan. 2015.
- [SSW-14] C. S. Park, D. Y. Lee, O. S. Kwon, and X. Wang, “A framework for proactive construction defect management using BIM, augmented reality and ontology-based data collection template,” *Autom. Constr.*, vol. 33, pp. 61–71, 2013.
- [SSW-15] X. Li, W. Yi, H. L. Chi, X. Wang, and A. P. C. Chan, “A critical review of virtual and augmented reality (VR/AR) applications in construction safety,” *Autom. Constr.*, vol. 86, no. July 2016, pp. 150–162, 2018.
- [SSW-16] J. Ahn and R. Han, “Human-centric Computing and Information Sciences,” 2012.
- [SSW-17] C. Catal, A. Akbulut, · Berkay Tunali, · Erol Ulug, and · Eren Ozturk, “Evaluation of augmented reality technology for the design of an evacuation training game,” *Virtual Real.*, vol. 24, pp. 359–368, 2020.
- [SSW-18] U. Ruppel and K. Schatz, “Designing a BIM-based serious game for fire safety evacuation simulations | Elsevier Enhanced Reader,” *Adv. Eng. Informatics*, vol. 25, no. 2011, pp. 600–611, 2011.
- [SSW-19] L. Zhang, Y. Wang, H. Shi, and L. Zhang, “Modeling and analyzing 3D complex building interiors for effective evacuation simulations | Elsevier Enhanced Reader,” *Fire Saf. J.*, vol. 53, no. 2012, pp. 1–12, 2012.
- [SSW-20] X. Wang, M. Truijens, L. Hou, Y. Wang, and Y. Zhou, “Integrating Augmented Reality with Building Information Modeling: Onsite construction process controlling for liquefied natural gas industry,” *Autom. Constr.*, vol. 40, pp. 96–105, Apr. 2014.
- [SSW-21] M. Kobes, I. Helsloot, B. de Vries, and J. G. Post, “Building safety and human behaviour in fire A literature review | Elsevier Enhanced Reader,” *Fire Saf. J.*, vol. 45, no. 2010, pp. 1–11, 2010.
- [SSW-22] M. Kinateder et al., “Social influence on route choice in a virtual reality tunnel fire,” *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 26, no. PART A, pp. 116–125, Sep. 2014.
- [SSW-23] K. Andrée, D. Nilsson, and J. Eriksson, “Evacuation experiments in a virtual reality high-rise building: exit choice and waiting time for evacuation elevators,” *Fire Mater.*, vol. 40, no. 4, pp. 554–567, Jun. 2016.



- [SSW-24] S. C. Swanström Wyke, K. Meyer Andersen, M. Hardahl, M. Mejlholm Harlyk, E. Risbøl Vils, and K. Svidt, “Virtual reality use for evaluation and improvement of building emergency signage,” in *Proceedings of the 2019 European Conference on Computing in Construction*, 2019, vol. 1, pp. 452–460.
- [SSW-25] Q.-J. Peng, X.-M. Kang, and T.-T. Zhao, “Effective Virtual Reality Based Building Navigation Using Dynamic Loading and Path Optimization,” *Int. J. Autom. Comput.*, vol. 6, no. 4, pp. 335–343, 2009.
- [SSW-26] IEEE, “P2048.4 - Standard for Virtual Reality and Augmented Reality: Person Identity,” 2019. .
- [SSW-27] A. Aryal, A. Ghahramani, and B. Becerik-Gerber, “Monitoring fatigue in construction workers using physiological measurements,” *Autom. Constr.*, vol. 82, pp. 154–165, Oct. 2017.
- [SSW-28] R. Edirisinghe and N. Blismas, “A prototype of smart clothing for construction work health and safety,” in *Proceedings of the CIB W099 International Health and Safety Conference: Benefitting Workers and Society through Inherently Safe (r) Construction*, 2015, no. September 2015, pp. 1–11.
- [SSW-29] N. Hashiguchi et al., “Practical Judgment of Workload Based on Physical Activity, Work Conditions, and Worker’s Age in Construction Site,” *Sensors*, vol. 20, no. 13, p. 3786, Jul. 2020.
- [SSW-30] D. Calvetti, P. Mêda, M. C. Gonçalves, and H. Sousa, “Worker 4.0: The future of sensed construction sites,” *Buildings*, vol. 10, no. 10, pp. 1–22, 2020.
- [SSW-31] J. H. Kim, B. W. Jo, J. H. Jo, and D. K. Kim, “Development of an IoT-based construction worker physiological data monitoring platform at high temperatures,” *Sensors (Switzerland)*, vol. 20, no. 19, pp. 1–17, 2020.
- [SSW-32] H. Jebelli, S. Hwang, and S. H. Lee, “EEG-based workers’ stress recognition at construction sites,” *Autom. Constr.*, vol. 93, pp. 315–324, Sep. 2018.
- [SSW-33] J. D. Runkle, C. Cui, C. Fuhrmann, S. Stevens, J. Del Pinal, and M. M. Sugg, “Evaluation of wearable sensors for physiologic monitoring of individually experienced temperatures in outdoor workers in southeastern U.S.,” *Environ. Int.*, vol. 129, pp. 229–238, Aug. 2019.
- [SSW-34] U. C. Gatti, S. Schneider, and G. C. Migliaccio, “Physiological condition monitoring of construction workers,” *Autom. Constr.*, vol. 44, pp. 227–233, 2014.
- [SSW-35] W. Lee, K. Y. Lin, E. Seto, and G. C. Migliaccio, “Wearable sensors for monitoring on-duty and off-duty worker physiological status and activities in construction,” *Autom. Constr.*, vol. 83, no. May, pp. 341–353, 2017.
- [SSW-36] K. M. Mehata, S. K. Shankar, N. Karthikeyan, K. Nandhinee, and P. R. Hedwig, “IoT Based Safety and Health Monitoring for Construction Workers,” in *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*, 2019, pp. 1–7.
- [SSW-37] K. Miura, K. Takagi, and K. Ikematsu, “Evaluation of two cooling devices for construction workers by a thermal manikin,” *Fash. Text.*, vol. 4, no. 23, pp. 1–12, 2017.
- [SSW-38] W. Yi, Y. Zhao, and A. P. C. Chan, “Evaluation of the ventilation unit for personal cooling system (PCS),” *Int. J. Ind. Ergon.*, vol. 58, pp. 62–68, Mar. 2017.
- [SSW-39] K. Yang, C. R. Ahn, M. C. Vuran, and S. S. Aria, “Semi-supervised near-miss fall detection for ironworkers with a wearable inertial measurement unit,” *Autom. Constr.*, vol. 68, pp. 194–202, 2016.
- [SSW-40] U Lindemann, A. Hock, M. Stuber, W. Keck, and C. Becker, “Evaluation of a fall detector based on accelerometers: a pilot study.”
- [SSW-41] A. K. Bourke and G. M. Lyons, “A threshold-based fall-detection algorithm using a bi-axial gyroscope sensor,” *Med. Eng. Phys.*, vol. 30, no. 1, pp. 84–90, Jan. 2008.
- [SSW-42] Q. Li, J. A. Stankovic, M. A. Hanson, A. T. Barth, J. Lach, and G. Zhou, “Accurate, fast fall detection using gyroscopes and accelerometer-derived posture information,” *Proc. - 2009 6th Int. Work. Wearable Implant. Body Sens. Networks, BSN 2009*, pp. 138–143, 2009.
- [SSW-43] S.-Y. Hwang, M. Ryu, Y.-S. Yang, and N. Lee, “Fall Detection with Three-Axis Accelerometer and Magnetometer in a Smartphone,” 2012.



- [SSW-44] M. Tolkiehn, L. Atallah, B. Lo, and G. Yang, “Direction sensitive fall detection using a triaxial accelerometer and a barometric pressure sensor,” in 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2011, pp. 369–372.
- [SSW-45] S. Cagnoni, G. Matrella, M. Mordonini, F. Sassi, and L. Ascari, “Sensor Fusion-Oriented Fall Detection for Assistive Technologies Applications,” in 2009 Ninth International Conference on Intelligent Systems Design and Applications, 2009, pp. 673–678.
- [SSW-46] J. Dai, X. Bai, Z. Yang, Z. Shen, and D. Xuan, “Mobile phone-based pervasive fall detection.”
- [SSW-47] ASSECURO, “Aplikacja FRIEND - alarm upadku NT001,” 2020. .
- [SSW-48] S. Dong, H. Li, and Q. Yin, “Building information modeling in combination with real time location systems and sensors for safety performance enhancement,” *Saf. Sci.*, vol. 102, no. November 2017, pp. 226–237, 2018.
- [SSW-49] P. Dollár, C. Wojek, B. Schiele, and P. Perona, “Pedestrian detection: An evaluation of the state of the art,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 4, pp. 743–761, 2012.
- [SSW-50] N. Schneider and D. M. Gavrilu, “Pedestrian Path Prediction with Recursive Bayesian Filters: A Comparative Study,” in *Pattern Recognition*, 2013, pp. 174–183.
- [SSW-51] S. Köhler, M. Goldhammer, S. Bauer, K. Doll, U. Brunsmann, and K. Dietmayer, “Early detection of the Pedestrian’s intention to cross the street,” in 2012 15th International IEEE Conference on Intelligent Transportation Systems, 2012, pp. 1759–1764.
- [SSW-52] J. W. Park, X. Yang, Y. K. Cho, and J. Seo, “Improving dynamic proximity sensing and processing for smart work-zone safety,” *Autom. Constr.*, vol. 84, no. August, pp. 111–120, 2017.
- [SSW-53] B. Choi, S. Hwang, and S. H. Lee, “What drives construction workers’ acceptance of wearable technologies in the workplace?: Indoor localization and wearable health devices for occupational safety and health,” *Autom. Constr.*, vol. 84, no. July 2016, pp. 31–41, 2017.
- [SSW-54] “Helmets, Sensors, and More: A Review - Practical Neurology.” .
- [SSW-55] U. S. Patent, “Helmet impact detection and prevention mechanism to minimize head concussion,” Jan. 2015.
- [SSW-56] “This new bike helmet can automatically call for help if you crash | Popular Science.” .
- [SSW-57] “Football helmet sensors monitor impact of collisions, tackles | FierceElectronics.” .
- [SSW-58] A. Kelm et al., “Mobile passive Radio Frequency Identification (RFID) portal for automated and rapid control of Personal Protective Equipment (PPE) on construction sites,” *Autom. Constr.*, vol. 36, pp. 38–52, 2013.
- [SSW-59] G. Gralewicz, “System automatycznej identyfikacji i zarządzania środkami ochrony indywidualnej w zakładzie pracy,” 2014.

## State of the Art in Cohesive Vehicle Monitoring Diagnostics

- [CVMD-1] F. Payri, J. M. Luján, C. Guardiola, and B. Pla, “A challenging future for the IC engine: new technologies and the control role,” *Oil Gas Sci. Technol. d’IFP Energies Nouv.*, vol. 70, no. 1, pp. 15–30, 2015.
- [CVMD-2] B. Bánhelyi and T. Szabó, “Data mining and analysis for data from vehicles based on the OBDII standard,” *CEUR Workshop Proc.*, vol. 2650, pp. 30–37, 2020.
- [CVMD-3] N. Goyal, V. Goel, M. Anand, and S. Garg, “Smart Vehicle : Online Prognosis for Vehicle Health Monitoring,” *J. Innov. Comput. Sci. Eng.*, vol. 9, no. 2, 2020.
- [CVMD-4] S. K. Andrews and V. N. Rajavarman, “Designing an iot enabled vehicular diagnostics system using automotive sensors and actuators integrated with onboard video camera,” *Int. J. Appl. Eng. Res.*, vol. 12, no. 19, pp. 8273–8277, 2017.

- [CVMD-5] V. Kirthika and A. K. Vecraraghavatr, “Design and development of flexible on-board diagnostics and mobile communication for internet of vehicles,” in 2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP), 2018, pp. 1–6.
- [CVMD-6] G. Signoretti et al., “Performance Evaluation of an evolving data compression algorithm embedded into an OBD-II edge device,” in 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, 2020, pp. 696–701.
- [CVMD-7] H. Schweppe, A. Zimmermann, and D. Grilly, “Flexible in-vehicle stream processing with distributed automotive control units for engineering and diagnosis,” in 2008 International Symposium on Industrial Embedded Systems, 2008, pp. 74–81.
- [CVMD-8] J. Oncken and B. Chen, “Real-Time Model Predictive Powertrain Control for a Connected Plug-In Hybrid Electric Vehicle,” IEEE Trans. Veh. Technol., vol. 69, no. 8, pp. 8420–8432, 2020.
- [CVMD-9] Y. Xun, J. Liu, J. Ning, and H. Zhang, “An experimental study towards the in-vehicle network of intelligent and connected vehicles,” in 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1–6.
- [CVMD-10] L. Atzori, A. Floris, R. Girau, M. Nitti, and G. Pau, “Towards the implementation of the Social Internet of Vehicles,” Comput. Networks, vol. 147, pp. 132–145, 2018.
- [CVMD-11] J. Kim, H. Hwangbo, and S. Kim, “An empirical study on real-time data analytics for connected cars: Sensor-based applications for smart cars,” Int. J. Distrib. Sens. Networks, vol. 14, no. 1, p. 1550147718755290, 2018.
- [CVMD-12] H. Wen, Q. A. Chen, and Z. Lin, “Plug-N-Pwned: Comprehensive vulnerability analysis of OBD-II dongles as a new over-the-air attack surface in automotive IoT,” Proc. 29th USENIX Secur. Symp., pp. 949–965, 2020.
- [CVMD-13] S. Halder, A. Ghosal, and M. Conti, “Secure over-the-air software updates in connected vehicles: A survey,” Comput. Networks, vol. 178, p. 107343, 2020.
- [CVMD-14] R. E. Vinodhini and K. Bavithiraja, S.V.M.G. Vimalkumar, “A detailed survey on research challenges in vehicular IoT,” J. Adv. Res. Dyn. Control Syst., vol. 11, no. 4, pp. 872–881, 2019.
- [CVMD-15] B. Martens and F. Mueller-Langer, “Access to Digital Car Data and Competition in Aftersales Services,” Seville, Spain, 2018.
- [CVMD-16] W. Kerber and D. Gill, “Access to data in connected cars and the recent reform of the motor vehicle type approval regulation,” J. Intellect. Prop. Inf. Technol. E-Commerce Law, vol. 10, no. 2, pp. 244–255, 2019.
- [CVMD-17] M. Pham and K. Xiong, “A survey on security attacks and defense techniques for Connected and Autonomous Vehicles,” arXiv, pp. 1–24, 2020.
- [CVMD-18] M. Steger et al., “An efficient and secure automotive wireless software update framework,” IEEE Trans. Ind. Informatics, vol. 14, no. 5, pp. 2181–2193, 2017.
- [CVMD-19] P. Subke, M. Moshref, and J. Erber, “In-Vehicle Diagnostic System for Prognostics and OTA Updates of Automated/Autonomous Vehicles,” SAE Int. J. Adv. Curr. Pract. Mobil., vol. 2, no. 2020-01–1373, pp. 2963–2968, 2020.
- [CVMD-20] International Organization for Standardization, “ISO 20077-1:2017 Road Vehicles — Extended vehicle (ExVe) methodology — Part 1: General information,” 2017.
- [CVMD-21] HERE, “Driving the automotive industry forward with location intelligence.” , Online: <https://www.here.com/solutions/automotive>
- [CVMD-22] Otonomo, “Connected Car Data for Predictive Maintenance.” , Online: <https://otonomo.io/use-cases/predictive-maintenance-car-data/>
- [CVMD-23] D. R. Varnhagen, “Electronic Horizon: A Map as a Sensor and Predictive Control,” in SAE Technical Paper, 2017.

- [CVMD-24] AutoMat, “Automotive Big Data Marketplace for Innovative Cross-sectorial Vehicle Data Services,” H2020, 2015. , Online: <https://cordis.europa.eu/project/id/644657>
- [CVMD-25] C. Guardiola, B. Pla, V. Pandey, and R. Burke, “On the potential of traffic light information availability for reducing fuel consumption and NOx emissions of a diesel light-duty vehicle,” *Proc. Inst. Mech. Eng. Part D J. Automob. Eng.*, vol. 234, no. 4, pp. 981–991, 2020.
- [CVMD-26] C. S. Nelson, “Particulate matter sensor.” Google Patents, 2012.
- [CVMD-27] J. Mora, F. Willems, X. Seykens, and C. Guardiola, “An OBD strategy to estimate SCR ageing and detect urea injection faults,” *IFAC-PapersOnLine*, vol. 51, no. 31, pp. 369–376, 2018.
- [CVMD-28] S. Leonhardt, N. Muller, and R. Isermann, “Methods for engine supervision and control based on cylinder pressure information,” *IEEE/ASME Trans. mechatronics*, vol. 4, no. 3, pp. 235–245, 1999.
- [CVMD-29] J. M. Desantes, J. Galindo, C. Guardiola, and V. Dolz, “Air mass flow estimation in turbocharged diesel engines from in-cylinder pressure measurement,” *Exp. Therm. Fluid Sci.*, vol. 34, no. 1, pp. 37–47, 2010.
- [CVMD-30] C. Guardiola, B. Pla, P. Bares, and A. Stefanopoulou, “Cylinder charge composition observation based on in-cylinder pressure measurement,” *Measurement*, vol. 131, pp. 559–568, 2019.
- [CVMD-31] Continental (Division Chassis & Safety), “Fuel Quality Sensor helps to protect the Engine and the Environment,” 2011. , Online: <https://www.electronicsspecifier.com/industries/automotive/fuel-quality-sensor-helps-to-protect-the-engine-and-the-environment>
- [CVMD-32] D. M. Vanzullen, G. Mouaici, F. Bernard, and I. Mckenzie, “Fuel sensor.” Google Patents, 2007.
- [CVMD-33] P. Fernandes, E. Macedo, B. Bahmankhah, R. F. Tomas, J. M. Bandeira, and M. C. Coelho, “Are internally observable vehicle data good predictors of vehicle emissions?,” *Transp. Res. Part D Transp. Environ.*, vol. 77, pp. 252–270, 2019.
- [CVMD-34] T. Tsokov and D. Petrova-Antonova, “Monitoring and Control of Vehicles’ Carbon Emissions,” in *International Conference on Software Technologies*, 2017, pp. 229–243.
- [CVMD-35] C. Guardiola, B. Pla, P. Bares, and J. C. P. Jones, “Integration of intermittent measurement from in-cylinder pressure resonance in a multi-sensor mass flow estimator,” *Mech. Syst. Signal Process.*, vol. 131, pp. 152–165, 2019.
- [CVMD-36] T. Kim and S. Park, “Compare of Vehicle Management over the Air and On-Board Diagnostics,” in *2019 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, 2019, pp. 1–2.
- [CVMD-37] J. Han et al., “GS1 Connected Car: An Integrated Vehicle Information Platform and Its Ecosystem for Connected Car Services based on GS1 Standards,” in *2018 IEEE Intelligent Vehicles Symposium (IV)*, 2018, pp. 367–374.
- [CVMD-38] J. E. Siegel, Y. Sun, and S. Sarma, “Automotive diagnostics as a service: An artificially intelligent mobile application for tire condition assessment,” in *International Conference on AI and Mobile Services*, 2018, pp. 172–184.
- [CVMD-39] A. Azman et al., “An integrated vehicle servicing and breakdown assistance system,” *Int. J. Eng. Technol.*, vol. 7, no. 4.40, pp. 42–47, 2018.
- [CVMD-40] S. Körper, R. Herberth, F. Gauterin, and O. Bringmann, “Harmonizing Heterogeneous Diagnostic Data of a Vehicle Fleet for Data-Driven Analytics,” in *2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE)*, 2019, pp. 1–6.
- [CVMD-41] L. Nkenyereye and J.-W. Jang, “A study of big data solution using hadoop to process connected vehicle’s diagnostics data,” in *Information Science and Applications*, Springer, 2015, pp. 697–704.
- [CVMD-42] D. Kwon, S. Park, and J.-T. Ryu, “A study on big data thinking of the internet of things-based smart-connected car in conjunction with controller area network bus and 4g-long term evolution,” *Symmetry (Basel)*, vol. 9, no. 8, p. 152, 2017.

- [CVMD-43] M. Johanson, S. Belenki, J. Jalminger, M. Fant, and M. Gjertz, “Big automotive data: Leveraging large volumes of data for knowledge-driven product development,” in 2014 IEEE international conference on big data (Big Data), 2014, pp. 736–741.
- [CVMD-44] A. Chin, P. Wolf, and J. Tian, “A Cloud IoT Edge Framework for Efficient Data-Driven Automotive Diagnostics,” in 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 2019, pp. 1–5.
- [CVMD-45] T. P. Carvalho, F. A. A. M. N. Soares, R. Vita, R. da P. Francisco, J. P. Basto, and S. G. S. Alcalá, “A systematic literature review of machine learning methods applied to predictive maintenance,” *Comput. Ind. Eng.*, vol. 137, no. September, 2019.
- [CVMD-46] M. Ren, X. Wang, G. Xiao, M. Chen, and L. Fu, “Fast Defect Inspection Based on Data-Driven Photometric Stereo,” *IEEE Trans. Instrum. Meas.*, vol. 68, no. 4, pp. 1148–1156, 2019.
- [CVMD-47] K. K. Kieselbach, M. Nöthen, and H. Heuer, “Development of a visual inspection system and the corresponding algorithm for the detection and subsequent classification of paint defects on car bodies in the automotive industry,” *J. Coatings Technol. Res.*, vol. 16, no. 4, pp. 1033–1042, 2019.
- [CVMD-48] Q. Zhou, R. Chen, B. Huang, C. Liu, J. Yu, and X. Yu, “An automatic surface defect inspection system for automobiles using machine vision methods,” *Sensors*, vol. 19, no. 3, p. 644, 2019.
- [CVMD-49] J. Molina, J. E. Solanes, L. Arnal, and J. Tornero, “On the detection of defects on specular car body surfaces,” *Robot. Comput. Integr. Manuf.*, vol. 48, pp. 263–278, 2017.
- [CVMD-50] F. Chang, M. Liu, M. Dong, and Y. Duan, “A mobile vision inspection system for tiny defect detection on smooth car-body surfaces based on deep ensemble learning,” *Meas. Sci. Technol.*, vol. 30, no. 12, 2019.
- [CVMD-51] A. Muñoz, X. Mahiques, J. E. Solanes, A. Martí, L. Gracia, and J. Tornero, “Mixed reality-based user interface for quality control inspection of car body surfaces,” *J. Manuf. Syst.*, vol. 53, pp. 75–92, 2019.
- [CVMD-52] J. Zhang et al., “An improved MobileNet-SSD algorithm for automatic defect detection on vehicle body paint,” *Multimed. Tools Appl.*, vol. 79, pp. 23367–23385, 2020.
- [CVMD-53] J. Xu, J. Zhang, K. Zhang, T. Liu, D. Wang, and X. Wang, “An APF-ACO algorithm for automatic defect detection on vehicle paint,” *Multimed. Tools Appl.*, vol. 79, no. 35, pp. 25315–25333, 2020.
- [CVMD-54] I. Jovančević, S. Larnier, J.-J. Orteu, and T. Sentenac, “Automated exterior inspection of an aircraft with a pan-tilt-zoom camera mounted on a mobile robot,” *J. Electron. Imaging*, vol. 24, no. 6, p. 61110, 2015.
- [CVMD-55] M. H. Priya and S. K. Vasudevan, “An innovative application for car engine disparity check—A novel attempt,” in 2017 International Conference on Signal Processing and Communication (ICSPC), 2017, pp. 175–180.
- [CVMD-56] S. H. Park, A. Tjolleng, J. Chang, M. Cha, J. Park, and K. Jung, “Detecting and Localizing Dents on Vehicle Bodies Using Region-Based Convolutional Neural Network,” *Appl. Sci.*, vol. 10, no. 4, p. 1250, 2020.
- [CVMD-57] W. A. R. Harshani and K. Vidanage, “Image processing based severity and cost prediction of damages in the vehicle body: A computational intelligence approach,” in 2017 National Information Technology Conference (NITC), 2017, pp. 18–21.

## Market analysis

- [MA-1] Internet of Things (IoT) Market Size, Share & COVID-19 Impact Analysis 2020-2027, Fortune Business Insights, July 2020.
- [MA-2] P. Azzoni, “*From Internet of Things to System of Systems*”, Artemis Industry Association, April 2020.
- [MA-3] R. Rishi, R. Saluja, “Future of IoT”, FICCI & Ernst & Young Analysis <http://ficci.in/spdocument/23092/Future-of-IoT.pdf>



- [MA-4] Edge Computing Market Size, Share & Trends Analysis Report Forecasts, 2020 – 2027, Grand View Research, March 2020.
- [MA-5] Edge Computing Market by Component, Application, Organization Size, and Industry Vertical: Global Opportunity Analysis and Industry Forecast, 2018–2025, Allied Market Research, May 2019.
- [MA-6] J.M. Chabas, C. Gnanasambandam, S. Gupte, M. Mahdavian, “New demand, new markets: what edge computing means for hardware companies”, McKinsey & Company, November 2018.
- [MA-7] LPWAN: The fastest growing IoT communication technology, IoTnow, November 2018.
- [MA-8] 5G Technology Market by Offering, Connectivity, Application, and End User: Global Opportunity Analysis and Industry Forecast, 2020–2026, Allied Market Research, June 2019.
- [MA-9] 5G infrastructure market - growth, trends, COVID-19 impact, and Forecasts (2021 - 2026), Mordor Intelligence, 2020.
- [MA-10] 5G Infrastructure Market by Communication Infrastructure, Core Network, Network Architecture, Operational Frequency, End User & Geography - Global Forecast to 2027, October 2019.
- [MA-11] 5G for business: a 2030 market compass, Ericsson, October 2019.
- [MA-12] Industrial Connectivity Market Report 2019-2024, IoT Analytics, August 2019 <https://iot-analytics.com/product/industrial-connectivity-market-report-2019-2024/>
- [MA-13] Forecast: The Business Value of Artificial Intelligence Worldwide 2017-2025, Gartner, March 2018 <http://tashfeen.pbworks.com/f/Forecasting%20Business%20value%20of%20AI%20-2025.pdf>
- [MA-14] Industrial AI Market Report 2020-2025, IoT Analytics, December 2019 <https://iot-analytics.com/product/industrial-ai-market-report-2020-2025/>
- [MA-15] Artificial Intelligence (AI) Market by Technology, and Industry vertical – Global opportunity Analysis and Industry Forecast 2018-2025, Allied Market Research, July 2018.
- [MA-16] Blockchain Market by Component, Provider, Type, Organization Size, Application Area, and Region - Global Forecast to 2025, Markets and Markets, May 2020.
- [MA-17] Blockchain Distributed Ledger Market by Type and End User – Global opportunity Analysis and Industry Forecast 2017-2023, Allied Market Research, March 2017.
- [MA-18] Blockchain Technology Market Size, Share, & Trends Analysis Report By Type, By Component, By Application, By Enterprise Size, By End-user, By Region, And Segment Forecasts, 2019 – 2025, Grand View Research, July 2019.
- [MA-19] Digital Transformation Index 2020, Dell Technologies, 2020 <https://www.delltechnologies.com/en-us/perspectives/digital-transformation-index.htm#overlay=/en-us/collaterals/unauth/briefs-handouts/solutions/dt-index-2020-executive-summary.pdf>
- [MA-20] K. L. Lueth, “40+ Emerging IoT Technologies you should have on your radar”, IoT Analytics, September 2019 <https://iot-analytics.com/40-emerging-iot-technologies-you-should-have-on-your-radar/>
- [MA-21] Global Artificial Intelligence Industry whitepaper, Deloitte, 2019 <https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-ai-report-en-190927.pdf>
- [MA-22] J.H. Moeller, “IoT patent landscape reference report”, Moeller Ventures LLC, September 2019 <https://www.moellerventures.com/mv-files/mv-reports/IoTPatentLandscapeReport-MoellerVentures-201909.pdf>
- [MA-23] J. Murnane, “Ports and shipping: The need for solutions that cross lines”, McKinsey & Co, May 2017 <https://www.mckinsey.com/industries/travel-logistics-and-transport-infrastructure/our-insights/ports-and-shipping-the-need-for-solutions-that-cross-lines>
- [MA-24] E. Lopez, “Ocean carrier reliability rebounds after record lows in early 2018”, SupplyChainDive, July 2018 <https://www.supplychaindive.com/news/ocean-carrier-reliability-May-2018-upswing/527711/>



- [MA-25] M. Wackett, “Global fleet capacity to bulge as more containerships are delivered in 2018”, The Load Star, January 2018 <https://theloadstar.com/global-fleet-capacity-bulge-containerships-delivered-2018/>
- [MA-26] O. Merk, T. T. Dang, “Efficiency of World Ports in Container and Bulk Cargo (oil, coal, ores and grain)”, OECD Regional Development Working Papers, September 2019.
- [MA-27] F. Chu, S. Gailus, L. Liu, L. Ni, “The future of automated ports”, McKinsey & Co, December 2018, <https://www.mckinsey.com/industries/travel-logistics-and-transport-infrastructure/our-insights/the-future-of-automated-ports>
- [MA-28] Top 50 world container ports, World Shipping Council, 2018 <https://www.worldshipping.org/about-the-industry/global-trade/top-50-world-container-ports>
- [MA-29] N. Davidson, “Retrofit Terminal Automation”, Port Technology Information, Edition 77, Spring 2018.
- [MA-30] Accidents at work statistics, Eurostat statistics, 2018 [https://ec.europa.eu/eurostat/statistics-explained/index.php/Accidents\\_at\\_work\\_statistics](https://ec.europa.eu/eurostat/statistics-explained/index.php/Accidents_at_work_statistics)
- [MA-31] The economics of occupational safety and health – the value of OSH to society, EU-OSHA, 2017, <https://visualisation.osha.europa.eu/osh-costs#!/>
- [MA-32] R. Agarwal, S. Chandrasekaran, M. Sridhar, “Imagining construction’s digital future”, McKinsey & Co, June 2016.
- [MA-33] V Franco, F Posada Sánchez, J German, P Mock “Real-world exhaust emissions from modern diesel cars. A meta-analysis of PEMS emissions data from EU (Euro 6) and US (Tier 2 Bin 5/ULEV II) diesel passenger cars. Part 1” The International Council on Clean Transportation. White Paper, 2014
- [MA-34] D. Bogdan, R. Bogdan and M. Popa, "Delta flashing of an ECU in the automotive industry," 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, 2016, pp. 503-508.
- [MA-35] J. Martinez, C. Dennison, Z. Lian, “Sequence Based Classification for Predictive Maintenance”, 2017.
- [MA-36] C. Ress, A. Etemad, D. Kuck, J. Requejo, “Electronic Horizon - Providing Digital Map Data for ADAS Applications”, in Proceedings of the 2nd International Workshop on Intelligent Vehicle Control Systems, pages 40-49, 2008.
- [MA-37] EC. Digital Transformation Monitor. “The race for automotive data”, 2017.
- [MA-38] Gao et al., “Disruptive trends that will transform the auto industry”, McKinsey & Co, January 2016.
- [MA-39] Fleet Management Market by Solution, Service, Deployment Type, Fleet Type, and Region - Global Forecast to 2025, MarketsandMarkets, June 2020.
- [MA-40] European Data Protection Supervisor. TechDispatch #3: Connected Cars, December 2019
- [MA-41] "Regulation (EC) No 715/2007". The European Parliament and the Council of the Europ. Union. 2007-06-20. pp. 5–9.
- [MA-42] The European Commission and EU consumer authorities publish final assessment of dialogue with Volkswagen [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_18\\_4549](https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4549)