Going to the Edge - Bringing Internet of Things and Artificial Intelligence Together

Michael Karner, Joachim Hillebrand, Manuela Klocker
Virtual Vehicle Research GmbH
Graz, Austria
michael.karner@v2c2.at

Ramiro Sámano-Robles
CISTER Research Centre
ISEP, Polytechnic Institute of Porto
Porto, Portugal
rasro@isep.ipp.pt

***Abstract*—Artificial Intelligence of Things (AIoT) is the natural evolution for both Artificial Intelligence (AI) and Internet of Things (IoT) because they are mutually beneficial. AI increases the value of the IoT through Machine Learning by transforming the data into useful information, while the IoT increases the value of AI through connectivity and data exchange. Therefore, InSecTT – Intelligent Secure Trustable Things, a pan-European effort with 52 key partners from 12 countries (EU and Turkey), provides intelligent, secure and trustworthy systems for industrial applications. This results in comprehensive cost-efficient solutions of intelligent, end-to-end secure, trustworthy connectivity and interoperability to bring the Internet of Things and Artificial Intelligence together. InSecTT aims at creating trust in AI-based intelligent systems and solutions as a major part of the AIoT. This paper provides an overview about the concept and ideas behind InSecTT and introduces the InSecTT Reference Architecture for infrastructure organization of AIoT use cases.**

***Index Terms*—internet of things, artificial intelligence, artificial intelligence of things, Reference Architecture**

I. Initial situation – Internet of Things and Artificial Intelligence

In recent years, technological development in consumer electronics and industrial applications has developed rapidly. More and smaller, networked devices are able to collect and process data anywhere. The Internet of Things (IoT) is a revolutionary change for many sectors like healthcare, building, automotive, railway, etc. Some developments are technologically amazing and frightening at the same time. Examples are fitness trackers, small devices that measure your movements and motions with help of integrated sensors. They can improve health by measuring your physical activities, measure your sleep quality etc. However, in 2018, the use of such fitness trackers has revealed secret locations of US military bases worldwide by publishing the regular jogging routes of soldiers on the Internet [1]. Information that would never have been stored a decade ago is now publicly available. The availability of those amounts of data also goes hand in hand with the development of Artificial Intelligence (AI) and Machine Learning (ML) algorithms to process them. With their use, faces of your friends can be recognized automatically in your online photo album or devices in the household can be simply controlled via voice recognition. The other side of the coin is the vulnerability of these devices in terms of security. Recent hacks of millions of webcams, printers, children's toys and even vacuum cleaners as well as Distributed Denial-of-service (DDoS) attacks reduce confidence in this technology. In addition, users are challenged to understand and trust their increasingly complex and smart devices, sometimes resulting in mistrust, usage hesitation and even rejection.

InSecTT (https://www.InSecTT.eu) has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876038. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Sweden, Spain, Italy, France, Portugal, Ireland, Finland, Slovenia, Poland, Netherlands, Turkey.
The document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.
The publication was written at Virtual Vehicle Research GmbH in Graz and partially funded within the COMET K2 Competence Centers for Excellent Technologies from the Austrian Federal Ministry for Climate Action (BMK), the Austrian Federal Ministry for Digital and Economic Affairs (BMDW), the Province of Styria (Dept. 12) and the Styrian Business Promotion Agency (SFG). The Austrian Research Promotion Agency (FFG) has been authorised for the programme management.

II. Going to the Edge – Bringing Internet of Things and Artificial Intelligence together

The developments described in Section I mostly cover processing of data in centralized Cloud locations and hence cannot be used for applications where milliseconds matter or for safety-critical applications. By moving AI to the Edge, i.e., processing data locally on a hardware device, real-time applications for self-driving cars, robots and many other areas in industry can be enabled. The push of AI towards the Edge can also be seen by recent announcements in consumer electronics. Google has reduced the size of the Cloud-based AI voice recognition model from 2 GB to only 80 MB, so that it can also be used on embedded devices and does not need an Internet connection [2].

The technological race to bringing AI to the Edge can also be seen by very recent developments of hardware manufacturers. In October 2018, Google released Edge TPU [3], a custom processor to run the specific TensorFlow Lite models on Edge devices. Many other, mostly US companies like Gyrfalcon, Mythic and Syntiant are also developing custom silicon for the Edge.

The InSecTT partners believe that Artificial Intelligence of Things (AIoT) is the natural evolution for both AI and IoT because they are mutually beneficial. AI increases the value

978-1-6654-2703-6/21/$31.00 ©2021 IEEE
DOI 10.1109/DSD53832.2021.00052

of the IoT through Machine Learning by transforming the data into useful information knowledge, while the IoT increases the value of AI through connectivity and data exchange:
AI + IoT = AIoT.

III. Building on a Sound Basis

The InSecTT project [6] is built on the basis of the predecessor projects DEWI [4] and SCOTT [5]. They, among others, reuse and extend the well-established DEWI Bubble concept and the related, ISO 29182-compliant [8] multi-domain High-Level Architecture. Within the DEWI project key solutions for wireless seamless connectivity and interoperability in smart cities and infrastructures were developed. DEWI was started in March 2014 as part of the ARTEMIS Joint Undertaking and ended in April 2017. The DEWI Bubble concept, the defined DEWI High-Level Architecture, as well as the DEWI technology items have been used as starting point for systems development within SCOTT and can be seen as the continuation of DEWI technology solutions. Complementary to DEWI, the SCOTT project put additional focus on the following aspects:

- Extending and connecting Bubbles and integrating distributed Bubbles into the Cloud.
- Extending the High-Level Architecture concerning security, trustability and Cloud integration.
- The development of safe and secure solutions for wireless distributed systems: implementing a layer where multiple Bubbles need to cooperate in deterministic (real-time) and secure way to establish systems in distributed locations.
- Elaboration of new approaches for secure distributed Cloud integration - extending DEWI High-Level Architecture.
- Developing secure and trustable applications coming from new domains such as Health and Home (besides commercial/public buildings).

SCOTT was started in May 2017 as part of the ECSEL Joint Undertaking and ended in June 2020. InSecTT now goes a significant step further and brings Internet of Things and Artificial Intelligence together.

IV. Overall Objectives of InSecTT – Competitiveness for strong European Industry

The overall objectives of InSecTT are to develop solutions for (1) Intelligent, (2) Secure, (3) Trustable (4) Things applied in (5) industrial solutions for European industry throughout the whole Supply Chain (6). More precisely:

1) Providing intelligent processing of data applications and communication characteristics locally at the Edge to enable real-time and safety-critical industrial applications.
2) Developing industrial-grade secure, safe and reliable solutions that can cope with cyberattacks and difficult network conditions.
3) Providing measures to increase trust for user acceptance, make AI/ML explainable and give the user control over AI functionality.

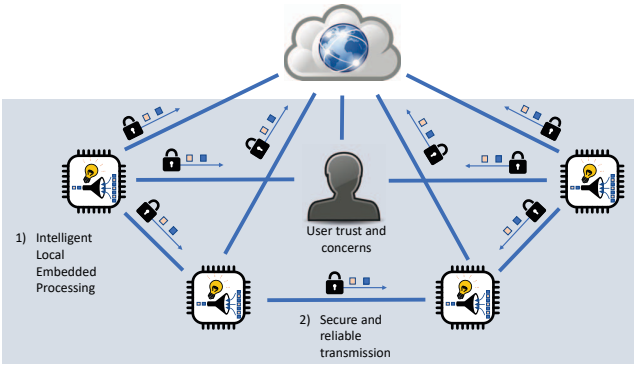

Fig. 1. InSecTT - Distributed intelligent processing

4) Developing solutions for the Internet of Things, i.e., mostly wireless devices with energy- and processing-constraints, in heterogeneous and also hostile/harsh environments.
5) Providing re-usable solutions across industrial domains.
6) Methodological approach with the Integral Supply Chain, from academic, to system designers and integrators, to component providers, applications and services developers & providers and end users.

The issues of ethics and public trust in deployed AI systems are now receiving significant international interest. The European Commission (EC) has recently released ethics guidelines for trustworthy AI [7]. Trustworthy AI has three components: it should be lawful, it should be ethical, and it should be robust. In InSecTT, we focus on robustness and ethics, ensuring our developed systems are resilient, secure and reliable, while prioritising the principles of explainability and privacy.

Figure 1 gives an overview of the focus of InSecTT. Local intelligent processing makes it possible to reduce the data required for transmission. Although most of work will be done on local level, communication with a Cloud is not excluded and will be needed in the right balance in some use cases. User trust and concern considerations will be incorporated throughout the design, development, and evaluation processes to ensure trustworthiness and acceptance.

Today, the development of IoT devices is already so complex that human errors inevitably occur in the conventional development process during their development. This is often exploited by resourceful hackers to compromise security and consequently leads to a loss of consumer trust. By using AI, a completely new approach is taken. The burden of finding solutions to complex problems will be transferred from the programmer to their program. InSecTT is therefore utilizing AI for two core tasks (see Figure 1):

1) AI-supported Embedded Processing for industrial tasks: this does not only include the typical speech and image recognition tasks that AI is used for today, but also specific smaller control and monitoring tasks needed in

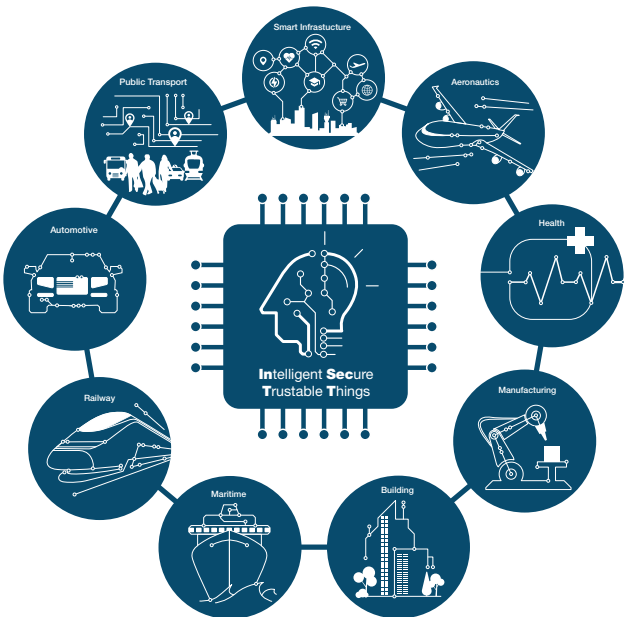

Fig. 2. InSecTT - Providing re-usable solutions across domains

industry and multiple instances of the most traditional ones (audio and video) cross-correlated with other monitoring techniques.

2) AI enhanced wireless transmission (e.g., beam-forming, propagation, prediction, interference reduction, energy saving, opportunistic transmission, improved direction of arrival estimations, improved human safety operation, etc.) for improving reliability as well as security (e.g., intrusion detection and response) in heterogeneous and even hostile environments (e.g., crowded urban areas, under water and metallic environment).

InSecTT aims to provide cross-domain solutions for 9 industrial domains: Health, Smart Infrastructure, Urban Public Transport, Aeronautics, Automotive, Railway, Manufacturing, Maritime, and Building (see Figure 2). The cross-domain aspect is not only realised by bringing in components to different domains, but also by interconnecting the domains in a truly cross-domain communication. This can be seen e.g., in use cases on airports or ports, where information from buildings, vehicles and planes needs to be exchanged with each other.

V. The InSecTT Reference Architecture

A. Overview

The InSecTT Reference Architecture (RA) is the set of guidelines for infrastructure organization of IoT use cases targeting industrial-grade connectivity, security, dependability, interoperability and trustworthiness with the help of AI. It provides the high-level view of building blocks, interfaces, vulnerabilities, security solutions, protocols, and in general the detailed information/control flow of InSecTT use cases in different industrial domains (aeronautics, automotive, railway,

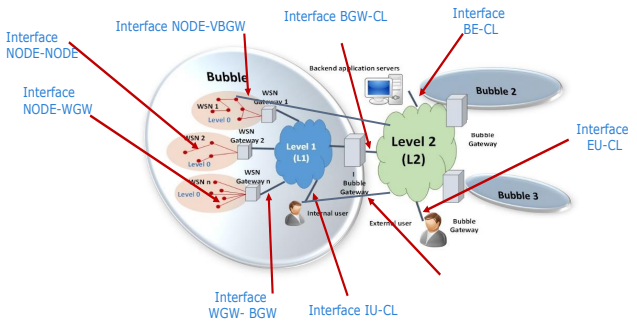

Fig. 3. Entity model

building, healthcare, maritime, etc). This provides us with a tool to analyse reusability, standardization, certification and verification issues across domains.

The InSecTT RA hosts a set of best practices collected across three EU projects: DEWI [4], SCOTT [5] and InSecTT [6]. The DEWI RA focused on dependability, using IoT protocols as a method to provide interoperability using the concept of DEWI Bubble as the encapsulation of legacy infrastructure. The DEWI RA was built on top of the ISO SNRA (Sensor Network Reference Architecture) [8]. The SCOTT project saw the extension towards a full IoT architecture with high level aspects such as Edge/Fog processing, security, privacy, safety and trustworthiness combining multiple standard architectures. The InSecTT RA re-takes the DEWI/SCOTT frameworks and the Bubble to investigate the impact of AI on IoT architectures.

The core of the DEWI / SCOTT/ InSecTT solution is the Bubble (see Fig. 3). An InSecTT Bubble is a logical entity composed by a group of nodes, gateways (GWs), internal users and existing (legacy or new) industrial infrastructure. The main property of a Bubble is that it provides a single point of access to the information of the entities in the intra-Bubble space. The InSecTT Bubble is therefore useful to encapsulate multiple industrial protocol standards into a consolidated IoT technology format improving and enforcing inter-operability, dependability and cross-domain development. The Bubble recommendations allow for the dependable integration of wireless/wireline industrial infrastructure using a three-layered intra-Bubble hierarchy that facilitates intra-domain adaptation and protocol translation, and a new trustworthiness-by-design philosophy. InSecTT foresees a landscape of communicating Bubbles implemented in different industrial use cases that can be called the Internet of Bubbles (IoB). Each Bubble can decide, if convenient, to allow transparent access to the nodes inside the Bubble or provide only consolidated, aggregated or processed information. The InSecTT RA follows the multiple perspective or view approach used by modern IoT systems matching the needs of multiple stakeholders and multi-level quality of service end user applications. Fig. 4 shows the perspectives of the InSecTT RA. We will describe the two central views of the architecture.

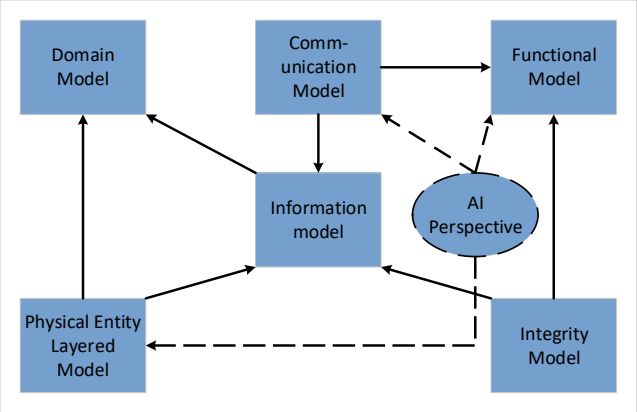

Fig. 4. Architecture perspectives

B. Entity model

The main perspective of the InSecTT RA is the layered physical entity model. In addition to the definition of each entity in an IoT network, the InSecTT RA provides a layered hierarchy which has been specifically designed for the integration of new and legacy wireless and wireline industrial infrastructure in a dependable and secure manner. The proposed three-layers reflect the interaction between the flexible wireless or Level 0 (L0) world, with the existing and potentially critical wireline industrial infrastructure (denoted Level 1 or L1), and Level 2 (L2) that acts as the encapsulation of the previous two layers in the form of a Bubble using a physical or virtual InSecTT Bubble GW (BGW) providing external services that can be invoked by other applications or other Bubbles based on multiple trustworthiness metrics. The BGW is therefore the main entity controlling access to the information of the internal nodes of the Bubble. Other GW entities can be defined inside the Bubble to deal with decentralized processing and dependability control between L0 and L1. The three-layer architecture allows designers to distribute complexity in different layers and different types of gateways, providing encapsulation of legacy technology in modern IoT protocols for interoperability and secure information transport. Level 0 (L0) is the wireles technology used inside the Bubble for one or more WSNs. Level 1 (L1) is the infrastructure inside the InSecTT Bubble to connect several WSNs to the corresponding BGW. This can be for example, the internal bus of a vehicle. Level 2 (L2) is the infrastructure providing a common external access to the Bubble (request-response).

The Bubble helps designers to enforce different trustworthiness metrics inside the Bubble. By explicitly isolating critical infrastructure and providing specific mechanisms (secured) that external entities are allowed to access or request, security is improved and therefore external attacks can be controlled or reduced. In addition, the concept of the Bubble has been found compatible with modern technologies such as Block Chain, Edge/Fog computing, and now AI. The Bubble is well suited for distributed AI in the three levels of the architecture. The virtual Bubble GW is adapted to include direct Cloud links or hybrid combinations of short range with long range direct Cloud links inside the Bubble. This means that the BGW can be completely virtualized in the Cloud or Edge infrastructure of a service provider. This is also compatible with futuristic implementations of 5G/6G systems with network slicing. The layered approach of the InSecTT Bubble is shown in Fig. 3 with the different types of interfaces between entities.

The InSecTT RA hosts a set of entities with different roles and functionalities. The main entities and the hardware interfaces enabled between them are shown in Fig. 3. The main entities are the Bubble nodes, the different types of Bubble Gateways, the different types of users of Bubble services and the external entities to the Bubble. The Bubble GW has a dominant role in being the enabler of the Bubble services and controls all access to the information inside the Bubble. We highlight the possibility of the Virtual Bubble GW (VBGW) to deal with those use cases where direct Cloud links can be used by nodes inside the Bubble. The virtual and physical BGW can coexist, but always should be integrated to mimic a single entity for security reasons. This also leads to the concept of hybrid user which is particularly suited for modern terminals with multiple radio interfaces and flexible mobility that can roam in and out the Bubble providing different levels of connectivity between nodes and external entities or with the virtual Bubble GW. We highlight the use of multiple gateways per level of the hierarchy to preserve the quality of service, delay, security, and offer encapsulation of underlying industrial technologies. Unlike other standard architectures, the InSecTT RA provides with specific procedures to support this detailed industrial connectivity and dependability issues between wireless and internal industrial wireline protocols. This is particularly useful, for example, in automotive use cases where wireless sensor readings are relayed to the internal network of the car, or also on board an aircraft where sensor nodes using the new wireless avionics technologies relay information to the internal critical aeronautics network. The node and entities of InSecTT are allowed to use multiple interfaces creating new challenges in routing, security, authentication and privacy that can be addressed by the InSecTT building blocks. The RA also has specific procedures for service and object virtualization which are important in applications such as digital twins and for security enhanced remote control.

C. Functional model

The proposed functional model in Fig. 5 is a combination of the ISO IOT/SNRA [8] [9], the ITU [11], IEEE [10] and the AIOTI functional models [12]. The layers are implemented by the physical entities of the RA. Each of the layers of the functional model can communicate with other layers using software interfaces. Each SW interface is potentially a standard data format or protocol and it can be subject to vulnerabilities. The InSecTT RA provides security mechanisms for each layer, in addition to the conventional security network layer included in the service and virtualization layer. It also includes a security management vertical layer that coordinates all security

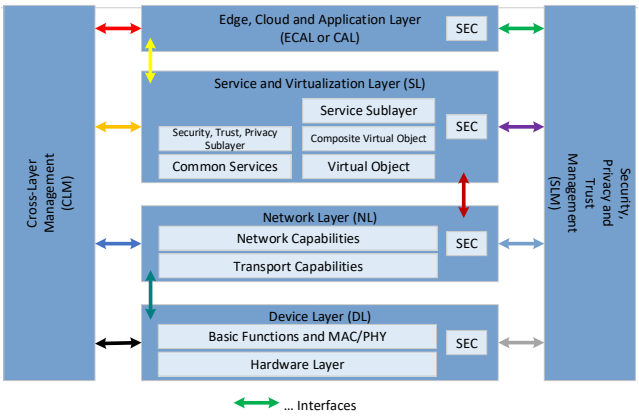

Fig. 5. Functional model

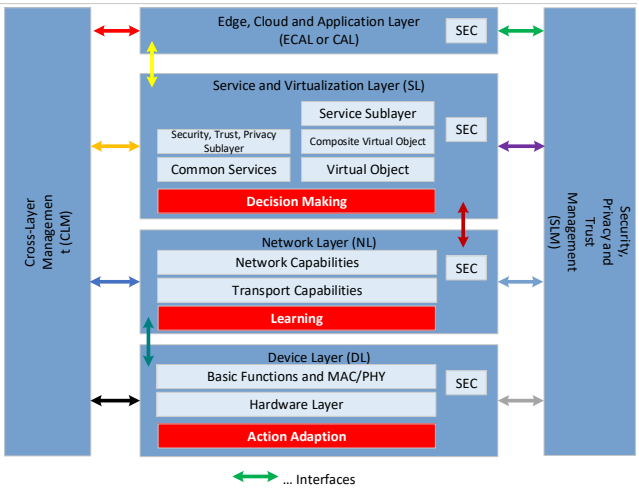

Fig. 6. Example of AI sublayers in the functional model

and trustworthiness solutions across different layers. The four horizontal layers are: Device Layer (DL), Network Layer (NL), Service Layer (SL), and the Cloud and Application Layers (CAL). The DL includes functions near the hardware, such as energy harvesting, sensor-related and basic MAC-PHY functionalities. The NL maps information into the cyberspace of L2 level. The SL encapsulates the lower layers presenting them as services, including virtualized services. This layer includes a security layer that runs on top of the conventional networking OSI layer. Finally, the CAL layer invokes the services of the SL as applications.

The InSecTT functional model includes specific service virtualization features and cross-layer management. In addition, it includes a detailed functional model decomposition with multiple trustworthiness metrics evaluation models to investigate how these different metrics evolve across layers and entities of the RA. This has led to L2 adaptation based on trustworthiness indicators and online certificates between Bubbles. Our vision is that communicating Bubbles in the cyberspace will be able to exchange trustworthiness metrics, indicators or information with online certification entities or anchors and this exchanged information can be used to adapt security, communication, semantics and other features in the interaction between Bubbles and other entities. InSecTT aims to use AI to improve several of these inter-Bubble interactions.

VI. Impact of AI

The last decade has witnessed an exponential increase in applications of AI for a variety of aspects of IoT applications. These aspects range from the lower layer transmission improvements, to upper layer applications and mainly intelligent services. However, the impact on the IoT architectures is rarely addressed consistently in the literature. One example is the work in [13], where the authors study the use of specific AI functionalities across different layers and entities of an IoT architecture enabled with Blockchain technology. The authors provide an analysis of the types of functionalities addressed by AI algorithms in different layers. The use of AI in Edge computing architectures is presented in [14]. This work focuses more on the entity and logical model views of Edge processing architecture and the impact of AI. Other works offer a semantical decomposition of AI algorithms and their specific processes in IoT architectures or applications. The authors in [15] propose the use of specific sub-functionalities generic to different AI algorithms such as feature extraction, learning, knowlEdge storage, decision making and automation control. This type of decomposition seems the most attractive to include specific AI processes in future AIoT architectures.

The work in InSecTT proposes an advance in the state of the art on how AI tools have an impact on IoT Reference Architectures. More specifically the work will be initially intended to decide whether the AI impact is high enough to include specific sublayers or views or other types of tools in the official InSecTT RA. The next step will be to modify the official architecture and align the existing use cases and the InSecTT universe of AI algorithms.

The AI algorithms can eventually form one or more perspectives that complement or that extend the views of the RA. The prime candidate is the addition of sublayers to the functionality model regarding different sub-functionalities that are common to typical AI algorithms. An example of modified functionality layer with specific AI steps such as learning, feature extraction, class detection, model optimization, etc., is shown in Fig. 6.

VII. Example use cases: preliminary alignment

A. Overview

We will show two examples of use cases and their preliminary alignment with the InSecTT RA. The full analysis is out of the scope of this paper. Therefore, we focus on the general overview of the two central models of the RA for two selected use cases. The first use case refers to a recent technology called Wireless Avionics Intra-Communications (WAICs). The second one is in the automotive domain targeting AI for wireless platoon intra-communications.

The term WAICs is used to describe any wireless sensor and/or actuator network operating on board an aircraft. While WAICs have been tested using multiple technologies and different frequency bands to verify potential interference to on-board equipment, this technology has been recently standardized by the ITU (International Telecommunications Unions) in the frequency bands of 4GHz (see [17]- [20]). WAICs is expected to be used mainly to replace or provide redundancy of wired infrastructure, such as control, sensing, and equipment management on board aircraft. In terms of cable infrastructure, gains can be expected for the reduction of aircraft design complexity. Reduced cable infrastructure also leads to weight losses, which in turn minimize fuel consumption, improve operational ranges and/or increase the size of the payload. In terms of configurability, wireless technology provides over-the-air (OTA) management and troubleshooting capabilities that facilitate network control and operation. Finally, wireless links can reach places of an aircraft difficult to cover with cables, thus facilitating design and reducing maintenance and troubleshooting costs for aircraft manufacturers.

In the second example, platoons are sets of cooperative autonomous or semi-autonomous vehicles with similar or identical routes that act as a single entity in terms of control and communication. The vehicles are usually arranged in linear convoys that communicate with each other control decisions that are usually made by one of the vehicles acting as leader or by a road side infrastructure with nearly real time traffic control information. The reliability of communication with low latency between the vehicular entities is critical to avoid any potential issue in the coordination between vehicles that could lead to safety issues. The emergence of 5G/6G technologies targeting ultra-low values of latency will enable the control of multiple autonomous or semi-autonomous vehicles in multiple platoons assisted by Edge/Cloud infrastructure.

B. Entity model

In the avionics use case, the ITU recommendations define two types of WAICs network topologies depending on the location: internal or external to the cabin. The gateways are positioned in places to provide good coverage for the intended applications. The entities of a WAICs network can be rearranged as a Bubble of the InSecTT Reference Architecture. Sensors or groups of sensors can constitute an InSecTT Bubble node. Several Bubble Nodes can form a Wireless Sensor Network (WSN) which is assumed to be controlled by a WSN Gateway (WGW). One or more WSNs can be designed to operate in different parts of the aircraft, using different channels, different frequency bands or different hopping or spreading sequences. This reduces interference between WSNs. All the WSNs that belong to the same Bubble are assumed to be controlled by a unique InSecTT Bubble Gateway (BGW). The Bubble GW is therefore the central control entity of all Bubble Nodes and WSNs inside the aircraft information system. The WSNs are thus interlinked to each other and to the Bubble GW using the internal aeronautics bus network. The most used standard is ARINC 664 or the commercial version

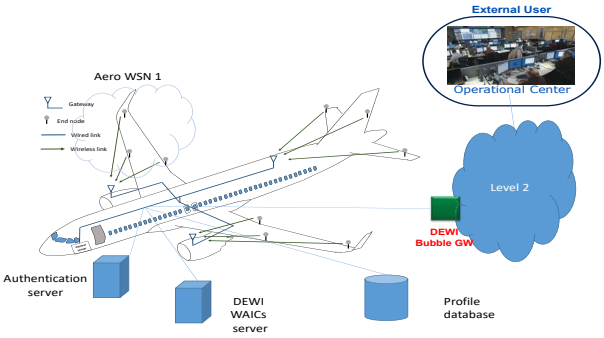

Fig. 7. Example of a WAICs network using the Bubble concept

called AFDX (Avionics Full-Duplex Switched Ethernet). This technology is a modified version of the Ethernet standard based on the concept of virtual links that ensure real-time and deterministic deadline allocation. The concept of Bubble is especially fit for aeronautical applications, where L1 is the internal, real time aircraft network, L0 is the wireless links, and L2 is the Cloud external connection of the aeronautical Bubble. We should emphasize that there are other ways of configuring the aeronautical infrastructure to have different deployments of the InSecTT Bubble. For example, different Bubbles can be operating in the same aircraft using an external L2 technology to achieve communication between Bubbles. The use of one Bubble per aircraft is illustrated in Fig. 7 for the aeronautical use case.

In the automotive use case, each platoon can be considered as a Bubble, with the leader being the Bubble Gateway (see Fig. 8, top sub-figure). The Bubble Gateway uses a 5G link to connect to the Cloud. In addition, each node of the Bubble has also a link with the 5G Base Station (BS) / Road Side Unit (RSU). In this case, we can consider that the 5G BS/RSU is a direct connection with a virtual Bubble Gateway, as the 5G Base Station (BS) acts as relay and assistant of the main Bubble GW. This leads to an interesting feature of the Bubble and InSecTT architecture. The physical Bubble GW is not the unique access point to the Bubble Nodes from the external world. Nodes can have another link to the outer Bubble space using another direct Cloud interface. This issue paved the way to the concept of virtual Bubble Gateway to control the connections to the Bubble using modern devices with multiple interfaces. This preserves the properties of the Bubble in a modern multiple interface environments.

The platoon-BS architecture can also be adapted in a different way to the InSecTT RA by considering that nodes can communicate with two WSN gateways over two different L0 technologies. The 5G link can be regarded as L1 technology, and the Bubble GW is represented by the 5G BS. This is also illustrated in Fig. 8 (the bottom sub-figure). This last option implies that the 5G BS or RSU are included in the Bubble, and therefore it can be inadequate for high mobility scenarios.

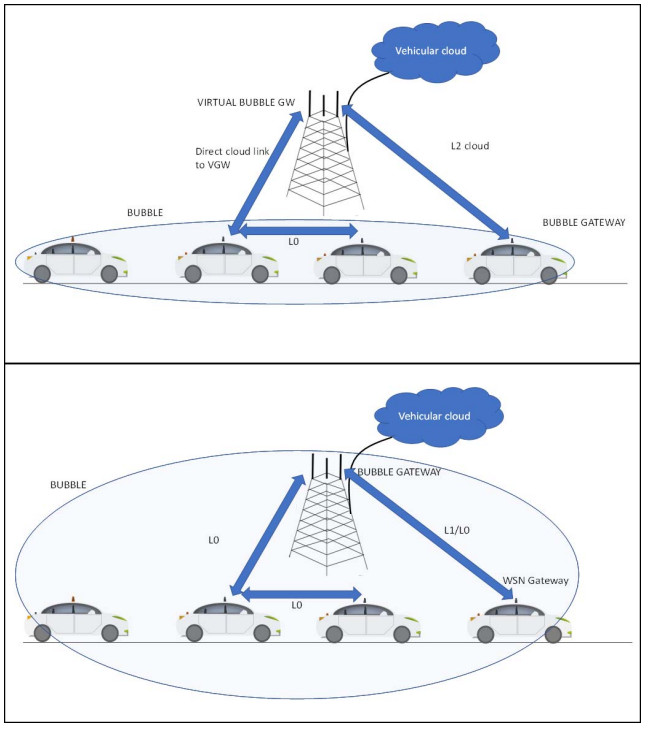

Fig. 8. Example of a Platoon network using the Bubble concept

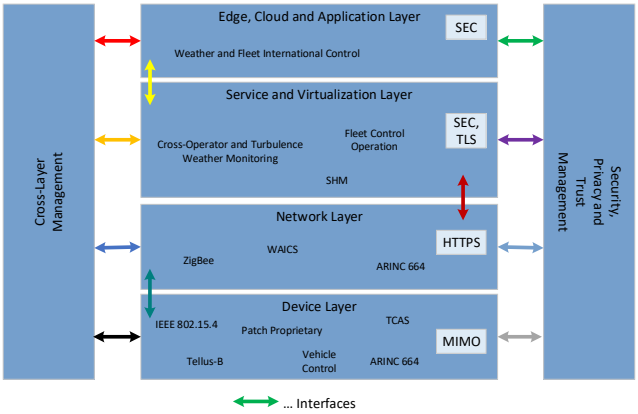

Fig. 9. Functional model WAICs use case

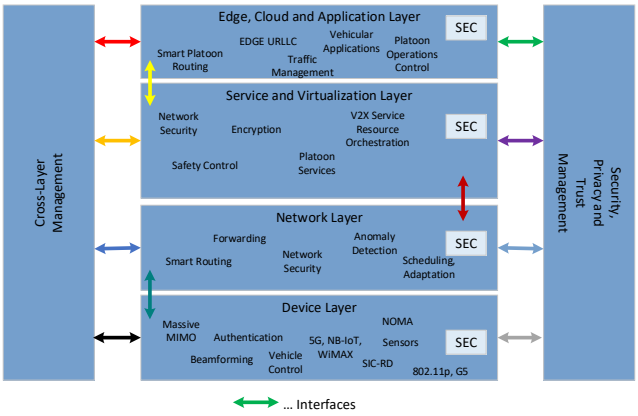

Fig. 10. Functional model platoon use case

C. Functionality model

In both use cases we have mapped all the requirements to the functionality model in Fig. 5. This information is useful to identify the type of functionality needed in each scenario of the use case and the different interfaces with other functionalities or building blocks. The preliminary functionality model of the two uses cases are shown in Fig. 9 and Fig. 10 for the WAICs and platoon use cases, respectively. The detailed functional decomposition is the basis for trustworthiness metrics evaluation. Each function of a use case is weighted by a vector of trustworthiness metric using different models. An overall composite metric can be calculated per entity or per Bubble. This methodology allows us to find potential issues, vulnerabilities or strengths of different building blocks.

D. Interfaces

The mapping between the entity and functionality models provides the detailed information of software and hardware interfaces. Interfaces between entities are hardware interfaces, while interfaces between layers of the functionality model are software interfaces. An example of this bi-dimensional mapping for the aeronautics use case can be seen in Table I (for the abbreviations, see Fig. 5). This bi-dimensional mapping provides a good overview of the communication protocols per layer and per entity and the type of software related to the encapsulation of each layer of the functionality model. The guidelines for trustworthy design of the InSecTT RA include the expertise in the design of each one of these interfaces to improve a number of metrics or solve different security/safety issues. This is done using empirical and/or numerical metric models.

TABLE I
MAPPING FUNCTIONAL VS ENTITY MODELS OF THE AERONAUTICS USE CASE

	Node	WGW	BGW	Cloud	EU
ECAL	-	-	-	-	-
SL	SSL	SSL	TLS/SSL	TLS/SSL	TLS/SSL
NL	HTTPS	HTTPS/VL	VL	HTTPS	HTTPS
DL	Patch	MIMO	ARINC664	Ethernet	Ethernet

E. General project overview for architecture alignment

A first version of the use case specifications of the project has been created as an internal document. The main aspects

considered in this preliminary analysis refers to the identification of the Bubble and possible configurations. In transportation systems, it was observed that at least two different ways are distinguished regarding the definition of the Bubble. For example, in autonomous driving use cases, the Bubble can be defined on each vehicle. However, in coordinated transportation systems, the Bubble can include multiple nodes or entities. Even in some cases, the Bubble may or may not include the Edge gateway in the road side units or the fixed access point. This selection depends on the needs of each use case. A similar approach can be followed for other types of use cases. For example, in the healthcare domain, the Bubble can be defined on the basis of isolation of entities or patients. Body Area Networks (BANs) can lead to define an individual Bubble for each patient, but in some cases it is better to define Bubbles for a full patient room or ward. In manufacturing, the Bubble can also be defined using the isolation provided between Bubble gateways. We recall that each Bubble can have several wireless sensor networks, using L1 technology to organize and schedule a different WSNs with potentially different technology. This makes the Bubble concept very flexible to adapt to a variety of scenarios, even with dynamic decomposition of the Bubble. The concept of virtual gateway allows us to expand the concept of Bubble to long range direct Cloud connections with 5G and 4G technologies. This adds an extra degree of flexibility with the definition of the Bubble that can be adapted to different scenarios in manufacturing, for example logistics, tracking, access control, and V2I solutions.

VIII. Conclusion

In this paper, the importance of bringing together Artificial Intelligence and the Internet of Things was highlighted. This so called Artificial Intelligence of Things is their natural evaluation, enabling key developments based on constant interplay and integration between AI and IoT. The European project InSecTT was described as a key enabler for the AIoT. After a motivation and analysis of the initial situation, the overall objectives and goals of the project were discussed in detail. It develops intelligent, secure and trustworthy systems for industrial applications to provide comprehensive cost-efficient solutions of intelligent, end-to-end secure, trustworthy connectivity and interoperability for the AIoT. Afterwards, the first results of the proposed InSecTT Reference Architecture for infrastructure organization of AIoT use cases were described. The Reference Architecture allows to deliver a more secure AIoT solution with reduced design effort, decreased costs, and increased quality. Next steps will be the first integration round of the InSecTT technological developments with the 15 different use cases out of 9 different industrial domains, leading to early demonstrators becoming available within the next months.

Acknowledgment

The authors would like to thank all partners of the InSecTT consortium for their contributions to the project.

References

[1] The Guardian: Fitness tracking app Strava gives away location of secret US army bases, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases, 28 Jan 2018, last accessed May 2021.

[2] ZDNet: Move over Siri, Alexa: Google's offline voice recognition breakthrough cuts response lag, https://www.zdnet.com/article/move-over-siri-alexa-googles-offline-voice-recognition-breakthrough-cuts-response-lag 13 Mar 2019, last accessed May 2021.

[3] Google: Edge TPU, https://cloud.google.com/edge-tpu/, last accessed May 2021.

[4] DEWI (Dependable Embedded Wireless Infrastructure) EU ARTEMIS project. Available at: http://www.dewiproject.eu, last accessed May 2021.

[5] SCOTT (Secure Connected Trustable Things) EU ECSEL project. Available at : https://www.scottproject.eu, last accessed May 2021.

[6] InSecTT (Intelligent Secure Trustable Things) EU ECSEL project. Available at : https://www.insectt.eu, last accessed May 2021.

[7] High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI", European Commission, 8 Apr 2019.

[8] ISO/IEC 29182, Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA)- Part 1 to 7

[9] ISO/IEC 30141, Internet of Things (IoT) – Reference Architecture

[10] IEEE 2413-2019: IEEE Standard for an Architectural Framework for the Internet of Things (IoT). https://standards.ieee.org/standard/2413-2019.html. Last accessed May 2021

[11] ITU Y.4000/2060: Overview of the Internet of things (Reference Architecture). Available online at https://www.itu.int/rec/T-REC-Y.2060-201206-I/en, last accessed May 2021.

[12] Alliance for Internet of Things innovation http://www.aioti.eu/, last accessed May 2021.

[13] S. Kumar Singh, S. Rathore, and J. H. Park, BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence,Future Generation Computer Systems, Volume 110, 2020, Pages 721-743, ISSN 0167-739X, https://doi.org/10.1016/j.future.2019.09.002.

[14] S. B. Calo, M. Touna, D. C. Verma and A. Cullen, "Edge computing architecture for applying AI to IoT," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, pp. 3012-3016, doi: 10.1109/BigData.2017.8258272.

[15] Q. Wu et al., "Cognitive Internet of Things: A New Paradigm Beyond Connection," in IEEE Internet of Things Journal, vol. 1, no. 2, pp. 129-143, April 2014, doi: 10.1109/JIOT.2014.2311513.

[16] F. Shi et al., "Recent Progress on the Convergence of the Internet of Things and Artificial Intelligence," in IEEE Network, vol. 34, no. 5, pp. 8-15, September/October 2020, doi: 10.1109/MNET.011.2000009.

[17] Technical characteristics and operational objectives for Wireless avionics intra-communications (WAIC) Report M.2197 (ITU-R Report). Available at: http://www.itu.int/pub/R-REP-M.2197. Last accessed: May 2021

[18] Technical characteristics and protection criteria for Wireless Avionics Intra-Communication systems, Recommendation ITU-R M.2067, approved Nov. 2014. Available at: http://www.itu.int/rec/R-REC-M/recommendation.asp?lang=en&parent=R-REC-M.2067. Last accessed: May 2021

[19] Technical conditions for the use of the aeronautical mobile (R) service in the frequency band 4 200- 4 400 MHz to support wireless avionics intra-communication systems, Report ITU-R M.2283, approved July 2015. Available at: http://www.itu.int/rec/R-REC-M/recommendation.asp?lang=en&parent=R-REC-M.2085. Last accessed: May 2021

[20] Technical characteristics and spectrum requirements of Wireless Avionics Intra-Communications systems to support their safe operation, Report ITU-R M.2283, approved Dec. 2013. http://www.itu.int/pub/R-REP-M/publications.aspx?lang=en&parent=R-REP-M.2283, last accessed May 2021.