IEEE Open Journal of the
Industrial Electronics Society

Received 18 January 2025; revised 28 February 2025 and 24 March 2025; accepted 29 March 2025. Date of publication 16 April 2025; date of current version 19 May 2025. The review of this article was arranged by Associate Editor Yuemin Ding.

Digital Object Identifier 10.1109/OJIES.2025.3560946

Artificial Intelligence for Wireless Communications: The InSecTT Perspective

RAMIRO SAMANO ROBLES [1] (Member, IEEE), GOWHAR JAVANMARDI [1,13], CHRISTOPH PILZ [2], PRZEMYSLAW KWAPISIEWICZ [3], MATEUSZ RZYMOWSKI [3] (Member, IEEE), LUKASZ KULAS [3] (Senior Member, IEEE), LUCA DAVOLI [4,12] (Member, IEEE), LAURA BELLI [4,12] (Member, IEEE), GIANLUIGI FERRARI [4,12] (Senior Member, IEEE), BERND-LUDWIG WENNING [5], BUGRA GONCA [6], R. VENKATESHA PRASAD [7], ASHUTOSH SIMHA [7], MARKKU KIVIRANTA [8] (Senior Member, IEEE), ILKKA MOILANEN [8], SEAN ROBINSON [9], GENNARO CIRILLO [9], MUJDAT SOYTURK [10] (Member, IEEE), YAVUZ SELIM BOSTANCI [10], AND LEANDER B. HÖRMANN [11]

[1]Research Centre in Real-Time and Embedded Computing Systems, 4249-015 Porto, Portugal
[2]Virtual Vehicle Research GmbH, 8010 Graz, Austria
[3]Gdansk University of Technology, 80-222 Gdansk, Poland
[4]Internet of Things Lab, Department of Engineering and Architecture, University of Parma, 43124 Parma, Italy
[5]Munster Technological University, T12 P928 Cork, Ireland
[6]NuRD Innovation Center, 06510 Ankara, Türkiye
[7]Technical University of Delft, 2628 CD Delft, The Netherlands
[8]VTT Technical Research Centre of Finland Ltd., FI-02044 Espoo, Finland
[9]F-Secure Corporation, 00181 Helsinki, Finland
[10]Marmara University, 34722 Istanbul, Türkiye
[11]Linz Center of Mechatronics GmbH, 4040 Linz, Austria
[12]National Interuniversity Consortium for Informatics, 00185 Rome, Italy
[13]Faculty of Engineering, University of Porto, 4099-002 Porto, Portugal

CORRESPONDING AUTHOR: RAMIRO SAMANO ROBLES (e-mail: rsr@isep.ipp.pt).

This work was supported in part by National Funds through FCT (Portuguese Foundation for Science and Technology), within the CISTER Research Unit under Grant UIDB/04234/2020, in part by the Operational Competitiveness Programme and Internationalization (COMPETE 2020) under the PT2020 Agreement, through the European Regional Development Fund (ERDF), in part by national funds through the FCT, within project and by the FCT and the EU ECSEL JU through the H2020 Framework Programme, under Project ECSEL/0002/2019, in part by JU under Grant 876038 (InSecTT), and in part by LASI under Grant LA/P/0104/2020.

ABSTRACT This article presents an overview of how Artificial Intelligence (AI) and edge technology have been used to improve wireless connectivity in multiple industrial Use Cases (UCs) of the EU project "Intelligent Secure Trustable Things" (InSecTT). We present a brief introduction of the InSecTT framework for cross-domain architecture design, which targets UCs assisted by reusable and/or interoperable technical Building Blocks (BBs). These BBs constitute the *"bricks"* containing AI and supporting components that were used to build different UCs. The framework consists of multiple stages based on the processing of UC/BB requirements (RQs). These stages include collection, harmonization, refinement, classification, architecture alignment, and functionality modeling of RQs. The most relevant results of these stages are discussed here, with emphasis on the need for a refined granularity of technical components with common functionalities named Sub-Building blocks (SBBs), where collaboration and cross-domain reusability were optimized. The design process shed light on how AI and SBBs were implemented across different layers and entities of our reference architecture for the Internet-of-Things (IoT), including the interfaces used for information exchange. This detailed interface analysis is expected to reveal issues such as bottlenecks, constraints, vulnerabilities, scalability problems, security threats, etc. This will, in turn, contribute to identifying design gaps of AI-enabled IoT systems. The article summarizes the SBBs related to wireless connectivity, including a general description, implementation issues, a comparison of results, adopted interfaces, and conclusions across domains.

INDEX TERMS Artificial intelligence (AI), edge computing, Internet-of-Things (IoT), reference architecture (RA), wireless.

NOMENCLATURE

3GPP	Third Generation Partnership Project.
5GAA	5G Automotive Association.
AI	Artificial intelligence.
AI-OTI	Alliance for AI, IoT, and Edge continuum innovation.
BB	Building bock.
BGW	Bubble gateway.
BLE	Bluetooth Low Energy.
CAN	Controller area network.
CMA	Constant modulus algorithm.
CNN	Convolutional neural network.
CVSS	Common vulnerability score system.
CWSS	Common weakness score system.
DEWI	Dependable Wireless Infrastructure.
DL	Deep learning.
EASA	European Union Aviation and Safety Association.
EM	Electromagnetic modeling.
ENISA	European Agency for Cybersecurity.
ETSI	European Telecommunications Standards Institute.
EUROCAE	European Organization for Civil Aviation Equipment.
ESPRIT	Estimation of signal parameters via rotational invariant techniques.
GRU	Gated recurrent unit.
HLA	High level architecture.
HW	Hardware.
ICA	Independent Component Analysis.
ICAO	International Civil Aviation Organization.
IEEE	Institute of Electrical and Electronic Engineer.
InSecTT	Intelligent Secure Trustable Thing.
IoT	Internet of Things.
IoE	Internet of Everything.
ISO	International Standards Organisation.
ITU	International Telecommunications Union.
LIN	Local area Interconnect.
LOS	Line of site.
LSTM	Long short term memory.
MIMO	Multiple input multiple output.
MVB	Multivehicle bus.
ML	Machine learning.
MQTT	MQ telemetry transport.
NB-IoT	Narrow band IoT.
NN	Neural network.
NLOS	Nonline of sight.
PARAFAC	Parallel factor.
PPCC	Power pattern cross correlation.
RA	Reference architecture.
RNN	Recurrent neural network.
RQ	Requirement.
RSSI	Received signal strength indicator.
SAE	Society of Automotive Engineers.
SBB	Subbuilding block.
SCOTT	Secure Connected Trustable Things.
SINR	Signal to interference plus noise ratio.
SNRA	Sensor network reference architecture.
SVM	Support vector machine.
SVR	Support vector regression.
SW	Software.
TCN	Train communication network.
TRL	Technology readiness level.
UC	Use case.
UWB	Ultrawide band.
V2V	Vehicle to vehicle.
V2x	Vehicle to everything.
WAIC	Wireless avionics intracommunications.
WTB	Wired train bus.

I. INTRODUCTION

A. BACKGROUND

In the postpandemic world, Artificial Intelligence (AI) has created an indelible footprint on multiple aspects of our everyday lives. Despite emerging skepticism, indicators show that this trend will continue to increase rather than recede [1]. Therefore, understanding the impact of AI on our society is key to generate regulatory frameworks that will emphasize its advantages and minimize potential problems [2].

In the field of wireless communications, the adoption of AI is progressing at a fast pace. Next-generation radio technologies are expected to incorporate new *AI-specific layers* [3] that will enhance their performance in aspects such as: latency reduction, resilience to fading, rejection of multipath distortion, resistance to shadowing phenomena, interference mitigation, and protection against multiple attacks (e.g., jamming, eavesdropping, tampering, impersonation, etc.) [4].

B. INSECTT PROJECT

This article presents a summary of how task T2.2 of the European project "Intelligent Secure Trustable Things" (InSecTT) [5] focused on improving connectivity in multiple industry-led Use Cases (UCs) with the help of AI tools. InSecTT was a project dedicated to the industrial demonstration of the convergence of edge computing, the Internet of Things (IoT), and AI. The InSecTT consortium was made up by more than 50 partners across Europe collaborating in 17 industrial UCs in strategic domains such as *automotive, railway, building, aeronautics, maritime*, and *health care* (see list of UCs in Table 1 and demonstration videos in [6]). As shown in Fig. 1, InSecTT proposed a bi-dimensional project structure: the horizontal axis represents the technical *Building Blocks* (BBs) (listed in Table 2), and the vertical axis shows the different UCs (listed in Table 1). This grid of BBs versus UCs facilitated reusability, interoperability, and cross-domain development. Table 3 shows the links between UCs and BBs.

C. TASK AI FOR WIRELESS (T2.2)

The objective of Task T2.2 in the InSecTT project was to provide a set of AI tools to improve wireless technologies

TABLE 1. Industry-Led UCs Defined in the EU InSecTT Project

UC	Description
UC1	Wireless Platooning communications based on AI-enhanced 5G
UC2	AI-enriched Wireless Avionics Resource Management and Secure/Safe Operation
UC3	Wireless Security Testing Environment for smart IoT
UC4	Intelligent wireless systems for smart port cross-domain applications
UC5	Smart and adaptive connected solutions across health continuum
UC6	Location awareness for improved outcomes and efficient care delivery in healthcare
UC7	Intelligent Transportation for Smart Cities
UC8	Intelligent Automation Services for Smart Transportation
UC9	Cybersecurity in Manufacturing
UC10	Robust resources management for construction of large infrastructures
UC12	Smart airport
UC13	Driver monitoring and distraction detection using AI
UC14	Secure and Resilient Collaborative Manufacturing Environments
UC15	Intelligent Safety and Security of Public Transport in Urban Environments
UC16	Airport security - Structured and Unstructured People Flow in Airports

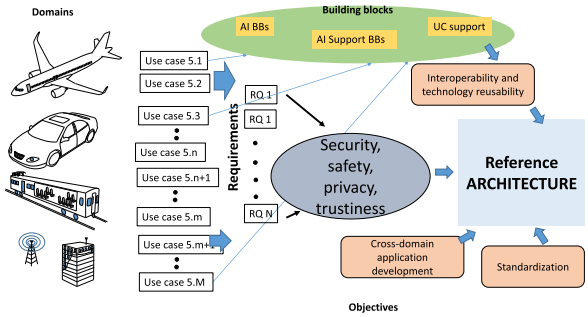

FIGURE 1. Infrastructure framework for cross-domain design of InSecTT: UCs, BBs, and RA.

TABLE 2 Technical BBs Defined in the EU InSecTT Project

BB	Description
BB2.1	AI on application level
BB2.2	AI wireless communication
BB2.3	AI on computational level
BB2.4	AI verification & validation
BB2.5	Trustworthy AI
BB3.1	Solutions for safety and security
BB3.2	Dependable wireless communication systems
BB3.3	Real-time monitoring and response
BB3.4	Real-time critical communication
BB3.5	Verification, validation, accountability

in different industrial scenarios. The need for better connectivity can be directly linked to the growing demand for IoT applications with higher criticality requirements. Therefore, wireless connectivity plays a central role in ensuring safety, security, and optimized performance in industrial IoT. The wireless component enables a key ingredient: *mobility*, which means that embedded processors with sensing, actuation, and resource-constrained intelligence can be easily deployed in multiple environments at moderate costs. This is important for the commercial viability of end products.

TABLE 3. Use Cases Versus Building Blocks

UC/BB	2.1	2.2	2.3	2.4	2.5	3.1	3.2	3.3	3.4	3.5
UC1	x	x		x	x		x	x	x	x
UC2		x		x			x		x	x
UC3		x		x	x		x			x
UC4	x	x	x			x	x	x	x	x
UC5	x	x	x	x	x	x				
UC6		x	x			x	x	x	x	x
UC7	x	x	x			x		x		
UC8	x	x	x			x		x		
UC9	x	x	x	x	x	x				x
UC10	x							x		
UC11		x	x				x	x	x	
UC12	x		x		x			x		
UC13	x		x			x				
UC14	x		x		x					
UC15	x	x	x				x	x	x	x
UC16	x		x				x	x	x	x

Despite its importance and considerable evolution in recent years, wireless technology continues to be prone or vulnerable to issues caused by *harsh propagation settings* and *attacks due to the broadcast nature of its transmissions*. Therefore, the potential improvements offered by AI algorithms promise to achieve new goals for industrial applications of IoT. These goals include *real-time operation, high reliability (wireline-like), ultra-low latency, increased data rates, better scalability*, and *improved security* [7]. This will, in turn, enable a new generation of automated intelligent services in line with the concepts of the Internet-of-Everything (IoE) [8], [9], 5G [10], and 6G [11].

D. OTHER CONTRIBUTIONS AND ORGANIZATION

This article presents an overview of real-life industrial examples addressed by the InSecTT project on how to use AI to improve wireless communications. This cross-domain study reveals useful information on the common challenges that multiple industrial players face today. The work also involves how relevant industrial-level metrics have been addressed by such implementations. The article includes a brief summary of the InSecTT cross-domain architecture design process, which includes the collection of initial requirements and their eventual harmonization, alignment, and refinement, which then led to the definition of architectural functional models. We also introduce the concept of Sub-Building Block (SBB) as a new granularity of technical contributions that was found to be more useful to enable cooperation and cross-domain reusability. The new granularity lies between BBs and individual technical components. The article also presents an overview of the functionality analysis based on international standards of IoT Reference Architectures (RAs). This RA alignment is expected to contribute to generate fully interoperable, standardized, and certified AI-edge processing architectures in different industrial domains.

The rest of this article is organized as follows. Section II presents a non-exhaustive review of the work in the area.

Section III presents the processes of collection, refinement, and harmonization of RQs, while also providing results on the alignment of refined RQs with the InSecTT RA . Detailed issues of the different SBBs and their implementation in different UCs are presented in Section IV. A summary that highlights the cross-domain issues related to the implementation of SBBs and their differences is given in Section V. Finally, Section VI concludes this article. Annex 1 presents a summary of the InSecTT RA. Annex 2 describes other RQ-related approaches in the project, and Annex 3 presents the two candidate classifications of RQs in task T2.2, and the definition of SBBs.

II. RELATED WORKS

A. CHANNEL ESTIMATION AND EQUALIZATION

Channel estimation and equalization are core operations in wireless networks [12]. They share multiple aspects with AI and Machine Learning (ML) algorithms [13] that facilitate their convergence: a training/learning stage is usually followed by an adaptation/detection process. Unsupervised equalization/estimation tools are expected to reduce the signaling bandwidth required by future wireless networks, particularly in emerging deployments with large antenna arrays.

Single-carrier equalizers employ filter banks with adaptive weights that resemble Neural Networks (NNs) [12], [13]. The Kalman filter, which is a textbook topic in channel estimation, has been improved and extended in multiple works using AI (see overview in [14]). This shows the link between wireless networks, estimation theory, and AI.

B. SYMBOL DETECTION, DOA ESTIMATION, COGNITIVE RADIO, AND MIMO SYSTEMS

Other wireless signal processing operations can also be assisted or replaced by AI. For example, symbol detection [15] can be regarded as an AI-classification problem, while beamforming can be formulated as a supervised adaptation or Support Vector Machine (SVM) algorithm [16]. Other operations such as Direction-of-Arrival (DoA) estimation [17], subspace detection/adaptation [18], object tracking [19], etc., can also be solved using AI. A list of works using AI in communication problems, including wireless networks, can be found in [20]. A survey on AI for cognitive radio systems can be found in [21]. Other more recent surveys can be found in [22] and [23]. The release of 5G and the use of massive Multiple-Input–multiple-output (MIMO) systems to improve data rate and latency points toward the adoption of ML to exploit spatial diversity. The post in [24] reports the evaluation of ML-based MIMO transmission/reception systems. Kia et al. [19] used Convolutional Neural Networks (CNNs) for MIMO positioning.

C. CHANNEL PREDICTION

Channel/link prediction has multiple applications in wireless networks, including: reduction of training bandwidth, improved resource allocation, and higher efficiency in link adaptation. Liao et al. [25] focused on multistep prediction for Rayleigh channels using CNNs and Deep Learning (DL). DL-based channel prediction for railway MIMO communications has been presented in [26]. Real-time channel prediction based on NNs for dedicated short-range networks is presented in [27]. Massive MIMO prediction for mm-wave channels has been studied in [28].

D. MULTIPLE ACCESS INTERFERENCE

Mitigation of multiple access interference is particularly well suited for the use of supervised and unsupervised learning [29]. Conflict resolution can be formulated as a source separation problem that has been addressed using tools such as PArallel FACtor analysis (PARAFAC) [30], Independent Component Analysis (ICA) [31], and the Constant Modulus Algorithm (CMA) [32].

E. APPLICATION LAYERS AND ARCHITECTURES FOR THE INTERNET-OF-THINGS

AI is one of the main candidates to improve IoT applications. The information collected by distributed embedded processors will feed AI algorithms running on cloud or edge servers. Typical implementations include anomaly detection [33], [34], AI-based cyber-risk evaluation [35], [36], object detection/classification [37], tracking [19], resource management [38], and home network security [39]. In spite of these advances, a detailed analysis of how AI is employed across different functional layers, entities, or different types of applications and architectures remains with multiple open issues today. InSecTT has used the concept of RA to shed light on the interactions of AI with all these different functionality/entity layers. One of the first RAs for IoT was proposed in the European project IoT-A [40], using the concept of multiple views or perspectives of the system. This multidimensional approach is well suited for the diverse metric and stakeholder framework in modern system design. Several standardization bodies proposed different versions of RAs, for example, the International Telecommunications Union (ITU) architecture in [41], the Institute of Electrical and Electronic Engineers (IEEE) architecture [42], and the International Standards Organization (ISO) standard architecture [43]. The alliance for AI, IoT and Edge Continuum innovation (AIOTI) [44] proposed a framework of interoperability between existing RAs. The InSecTT RA is a hybrid architecture that combines the virtues of existing frameworks, enforcing the objectives and visions of the consortium. The entity and functionality views of the InSecTT RA are shown, respectively, in Figs. 2 and 3. An overview of the InSecTT RA is given in Annex 1.

F. TRUSTWORTHINESS METRICS AND SOFTWARE BILLS OF MATERIALS

InSecTT implemented the concept of trustworthiness metrics to evaluate functionalities and entities aligned with the InSecTT RA. These metrics are an extension of standard security metrics as explained in more detail in Annex 2. This approach can lead to a detailed evaluation of risks

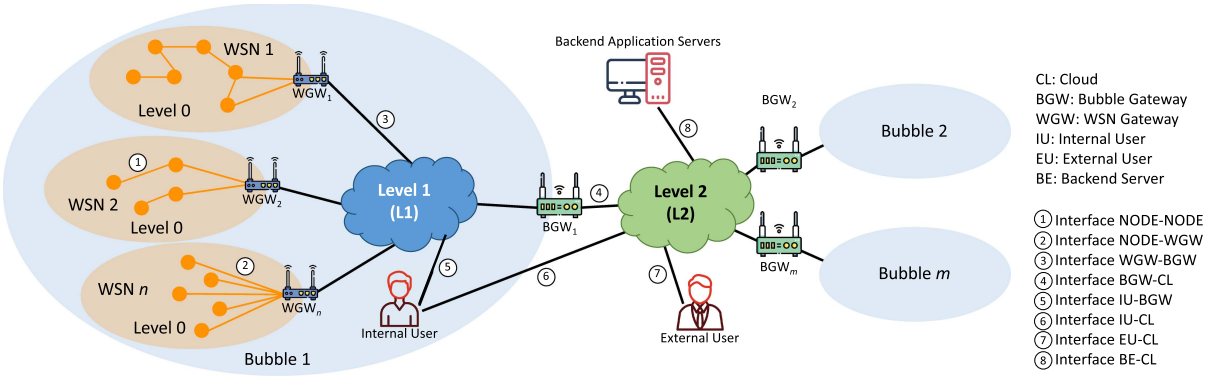

FIGURE 2. Entity model of the InSecTT RA.

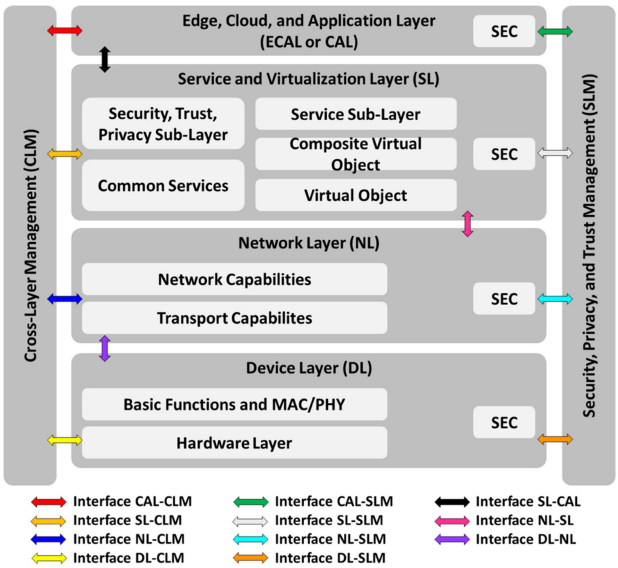

FIGURE 3. Functionality model of the InSecTT RA.

per interface and per functionality of the proposed BB and SBB granularity. InSecTT also proposed the use of AI-ML for the global evaluation of the variations of trustworthiness metrics. This is in line with recent approaches for AI in cybersecurity risk analysis based on the concept of Software Bill Of Materials (SBOMs). This approach aims to enhance security, transparency, and trustworthiness in AI systems. Radanliev et al. [45] explored cybersecurity threats, exploits, and vulnerabilities in AI-driven SBOMs and evaluated how memory safety features can mitigate these risks. They also discussed regulatory implications, AI risk management, and future directions for securing AI and ML technologies through structured AI BOM frameworks. Radanliev et al. [46] explored cybersecurity risks in low-memory IoT devices and evaluated existing risk management. The study integrated AI/ML techniques for real-time cyber-risk estimation and discussed the role of cyber insurance in mitigating IoT-related threats. The main categories of cyber-risk listed include ethical risk, privacy risk, and security risk, among others.

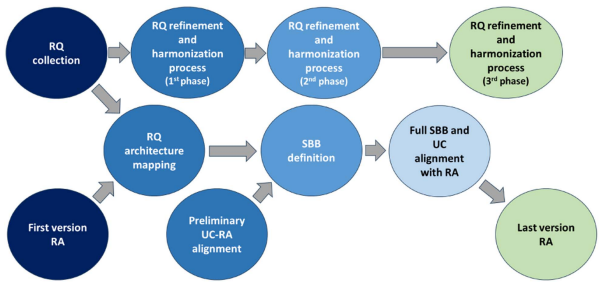

FIGURE 4. Timeline of RQ processing, SBB definition, and UC alignment process with the InSecTT RA.

While AI/ML enhance risk assessment by identifying vulnerabilities and predicting cyber-threats, their black-box nature raises concerns about trust, interpretability, and decision-making accountability. InSecTT has used the trustworthiness metric approach for the verification of AI (See Annex 2)

III. REQUIREMENTS AND ARCHITECTURE ALIGNMENT

A. OVERVIEW OF THE INSECTT CROSS-DOMAIN DESIGN PROCESS

The first step in the InSecTT cross-domain design process was the collection and architecture alignment of RQs. This first step is shown in Fig. 4, which displays the timeline for the entire design process. As observed in this figure, the initial collection stage was followed by successive stages of harmonization and refinement of RQs. This sequential processing approach was necessary to reflect possible changes in UC/BB contributions over the duration of the project.

B. HARMONIZATION, REFINEMENT, AND FUNCTIONALITY MODELING

The initial collection of RQs produced over 600 entries with different levels of abstraction and functional scope. Therefore, additional processing stages were needed to find common interests and similar functional scopes across different UCs. This also led to the consolidation of opportunities for collaboration and cross-domain fertilization.

The *harmonization* stage addressed the consolidation of ideas and objectives across different UCs to create common

TABLE 4. RQs Identified in the Task T2.2 of the EU InSecTT Project and Assignment to SBB Classification

RQ	Description	C1	C2
1	Intelligent Routing Algorithms	B	C
13	Intelligent connection mgmt	B	C
70	Smart connectivity	B	C
109	Interference detection	A	A
110	Interference identification	B	A
111	Interference mitigation	B	A
113	AI Direction of Arrival	A	B
114	AI modulation recognition	A	A
116	Localization simulation	A	B
140	Predict Imminent Connection Loss	C	C
141	Rating of Interfaces	A	C
142	Redundant Transmission	A	A
143	Link Aggregation	B	C
144	Parallel Connections	A	A
145	Load Balancing on SW Level	B	A
152	Dashboard connectivity	A	C
158	Intelligent connectivity	A	C
164	Radar for vital sign monitoring	A	A
218	Learning representations	E	E
228	Device free localization	A	B
238	Network anomaly detection	D	D
242	Anomaly Detection Form Factor	D	D
245	Wireless Authentication	A	B
270	Wireless Failure Estimation	A	C
271	Link Quality Measurement	A	C
310	Energy Eff. Comm. Anom. Detect.	D	A
318	MIMO scalability	C	D
322	AI for conflict resolution	C	A
325	Non-linear processing	C	A
327	MAC-PHY security	C	B
329	AI-based resource allocation	C	C
349	Local access data collection	D	D
390	Data pre processing and filtering	D	D
391	Centralized cloud analysis	D	D
392	Learning and model update	E	E
393	Feedback for detection model	E	A

functional needs in the BBs. By contrast, the *refinement* stage usually led to a reduction or narrowing of the functional scope of requirements to maximize their reusability across different UCs. These two stages were essential to bring RQs to a similar level of complexity, which subsequently led to a more effective cross-domain design. Once these harmonization and refinement stages were completed, the processed RQs and their associated functionalities were classified, grouped, and eventually transformed into a more detailed architecture functionality model for the entire project.

C. ARCHITECTURE ALIGNMENT OF T2.2

The task of AI for wireless communications (T2.2) produced 27 initial RQs. These RQs are listed in Table 4, and were individually aligned with the functionality and entity models of the InSecTT RA (as shown in Fig. 5). More details of the InSecTT RA can be found in Annex 1. The classification of RQs in different subclasses is also shown in Table 4. The process followed for this classification and architecture alignment is detailed in Annex 3. The concept of SBB as a refined granularity of BBs is also given in Annex 3. The following section summarizes the SBBs of T2.2 using the classification C2 illustrated in Fig. 6. Classification C2 was the final SBB

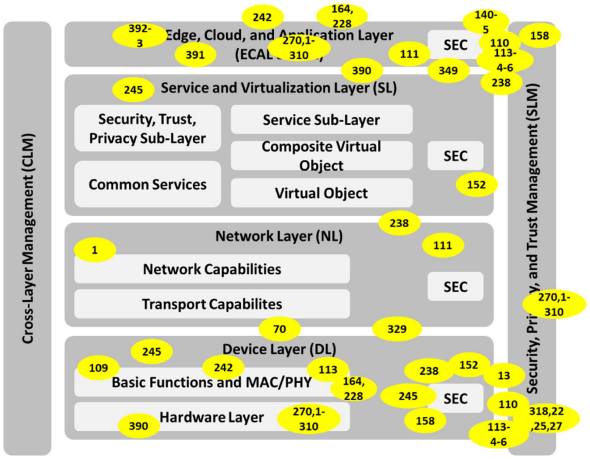

FIGURE 5. Mapping of the RQs of BB2.2 to the functionality model of the InSecTT RA.

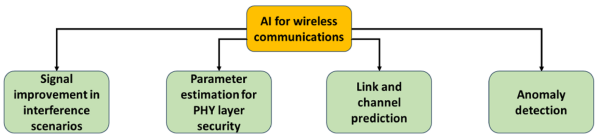

FIGURE 6. SBB classification based on communication concepts (category C2).

organization adopted in task T2.2. The other classification candidate, named C1,is described in more detail in Annex 3.

IV. SBB DESCRIPTION, INTERFACES, IMPLEMENTATION, AND INTEROPERABILITY

This section provides the details of the different SBBs of BB2.2, focusing on interfaces, links to the UCs, the information of the datasets used for training, implementation issues, etc. The information is also summarized in Table 5.

A detailed interface analysis (as described in Section III and in Annex 3) is useful to identify the functionalities triggered by the dynamic information flow of a UC. This approach aims to find potential security, scalability, capacity, signaling, and performance issues. The following subsections provide details of the architecture analysis of the SBBs of T2.2.

A. SBB2.2 A—SIGNAL IMPROVEMENT IN INTERFERENCE SCENARIOS

1) GENERAL DESCRIPTION

The objective of this SBB was to use resource diversity or a subspace refinement process, usually based on multiple antennas (MIMO systems), to improve signal reception, detect interference, and/or remove unwanted impairments (e.g., multipath interference, fading, shadowing, etc.).

2) DATASETS

There are multiple similarities between the datasets of all the SBBs in T2.2, mainly because they all rely on measurements or models of the wireless channel. However, there are

TABLE 5. SBBs Identified for the BB2.2 in the InSecTT Project

SBB	Description	UCs, BBs	Interfaces	Datasets Value/Format	Algorithms
2.2A-1	Artificial signal generation (for interference detection)	UC: 2,3,4,11 BB: 3.2,3.5	offline	Channel meas./CSV	SVM,CNN
2.2A-2	MIMO receiver	UC: 1,2,3 BB: 3.2,3.5,2.5	5G/WAICs	Synthetic model/CSV	CNN, Markov chain PARAFAC, ICA
2.2A-3	RadCom to minimize interferences	UC: 5	60GHz (5G)	OFDM signals	Chirp mod.
2.2B-1	Automatic setup of testing in laboratory and real-world environments	UC: 2,3,4,11 BB: 3.2,3.5	offline	CSV	N/A
2.2B-2	DoA estimation, Spatial authentication	UC: 1,2,3 BB: 3.2,3.5,2.5	5G/WAICs	Synthetic/ CSV	CNN,ESPRIT
2.2B-3	Fault detection and compensation in vehicular networks	UC: 1,6	UWB	CSV	Geometric Kalman
2.2B-4	RadCom based DoA, range and velocity estimation	UC: 5	60GHz	N/A	RIT
2.2C-1	Multi-interface GW (MIG)	UC: 15,16 BB: 3.2,3.3,3.4	BLE, Wi-Fi, LoRaWAN	CSV	Markov chain
2.2C-2	Channel prediction	UC: 1,2,3 BB: 3.2,3.4,3.5,2.5	5G/WAICs	CSV/synthetic	TCN, MM, LSTM, RNN
2.2C-3	Railway certified platform with AI HW accelerators	UC: 7 BB: 3.3,3.4	TCP, 5G	N/A	N/A
2.2C-4	Routing and connection management platform for multiple cellular links	UC: 7 BB: 3.3,3.4	TCP, 4G, 5G	CSV	SVR, LSTM, GRU Multi-armed Bandit
2.2C-5	Detection, estimation and compensation in vehicular networks of faults in decentralized vehicular net.	UC: 1,6	UWB	CSV	Geometric Kalman
2.2C-6	SW platform for V2x message exchange	UC: 3	5G, MQTT	N/A	N/A
2.2D-1	Anomaly detection in a consumer home network	UC: 13 BB: 3.3	Network flows	Real world customer data	Random forest
2.2D-2	Interference detection at bit-level	UC: 2	WAICs	Channel meas./ CSV	CNN, SVM
2.2D-3	MIMO-based anomaly detection	UC: 1,2,3 BB: 3.2,2.5,3.5	5G, WAICs	(meas.)CSV synthetic	CNN
2.2D-4	Anomaly detection for the EPhESOS communication protocol	UC: 3 BB: 3.5	2.4 GHz ISM	Channel meas./ CSV	Unsupervised Methods
2.2D-5	Network anomaly detection	UC: 4,9 BB: 2.1,3.2	RESTful MQTT	MQTT traffic	
2.2D-6	Anomaly detection OPA UC	UC: 9	TCP	TCP traffic	CNN
2.2D-7	Hybrid anomaly detection	UC: 4 BB: 3.1	TCP	TCP traffic	LSTM, RNN

specific differences that are discussed here for each type of algorithm. In this SBB, the datasets contain the information of both the propagation wave and more importantly the PHY-layer impairments to be removed. Many of the datasets in this SBB considered multiple antennas, as they are exploited to mitigate impairments. In some cases (such as vehicular channels with high speeds), the statistics can change very quickly, thus leading to non-stationary staistics. In this regime, channel measurements or conventional electromagnetic modeling (EM), commonly used to create accurate datasets, start experiencing a number of issues. For example, we found complexity constraints and incomplete information cases due to rapidly changing environments. To mitigate these impairments, synthetic channel modeling has been used. Some of the adopted solutions include hybrid algorithms using ray-tracing and geometric-based stochastic channels.

In the case of scenarios with stationary statistics, measurement campaigns have been conducted in different industrial domains. Some of the measurements in this SBB were conducted in realistic settings. For example, using nodes onboard operational trains, inside railway stations, by using antennas on the surface of moving vehicles (low speed), inside airports, and other industrial operational environments. In the case of Wireless Avionics Intracommunications (WAICs), extensive channel measurements were conducted on board commercial aircraft considering multiple sources of interference. Some of the measurements included the effects of the human users, such as shadowing, absorption, reflection, diffraction, etc. For example, some of the channel modeling on airplanes considered passengers inside the cabin. A similar measurement campaign was conducted inside hospitals and inside critical buildings where users or passing-by persons influenced the collected datasets.

3) BB INTERFACES

This BB has a strong connection with BB3.2, which was focused on channel models, measurements, and wireless signal processing algorithms. This partnership was expected to propel the lower layers of wireless networks to be more reliable, secure, and trusted. Thus, the adopted interfaces mainly connect the lower layers (PHY-layer information of BB3.2) with intermediate/upper layers (BB2.2), where AI resides. In

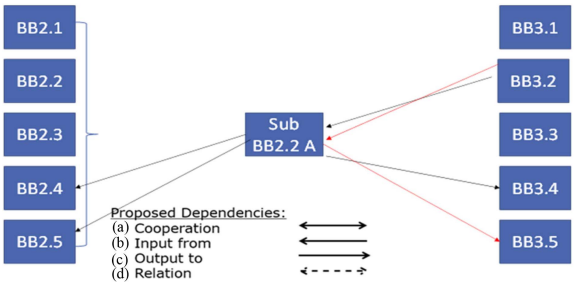

FIGURE 7. Interfaces of SBB2.2 A with other BBs.

some cases, this usually involves a hardware interface linking nodes that are distributed in the environment to the edge of the network or, in only a few of cases, directly to the cloud. The interface provides AI with access to the base-band processing information and the resources of routers or nodes. An issue identified in this BB is the potential impact of the use of AI on the capacity of the required cross-layer signaling interfaces. This interface bandwidth is needed to capture the full complexity of the wireless environment. Therefore, some of the developments in this SBB have assumed incomplete, inaccurate, and/or hybrid datasets. Alternatively, synthetic models have been used to compensate for the unavailability of information due to capacity constraints on the cross-layer interfaces. In the future, when AI sublayers need to collect information in real-time to train and/or update models, there will be a need to evaluate the capacity of existing signaling interfaces and potentially use unsupervised or hybridsupervised/unsupervised solutions to minimize the degrading effects.

SBB2.2a algorithms also have an interface with BB3.3 and BB3.4 to enable higher level services. For example, in the case of MIMO, it enables ultra-low latency resource allocation, PHY-layer security, and adaptive beam-forming per terminal. The interfaces of this SBB with other BBs of the InSecTT framework are illustrated in Fig. 7.

4) IMPLEMENTATION DETAILS AND ISSUES

Most the algorithms in this SBB were implemented in SW-defined radio platforms, wireless emulators, and/or system-level simulators enabled with realistic channel/network emulation. Some of them reside on state-of-the-art open source base station platforms that currently proliferate in wireless network design (e.g., [47], [48]). These platforms facilitate the development, implementation, and integration of algorithms with packet core networks such as [49], thus producing high Technology Readiness Level (TRL) prototypes. In aeronautics, a system-level simulator with new channel models developed in [50] was used to investigate the emerging technology of WAICs [51], [52].

In some UCs, the existing wireline infrastructure dictates the type of network platform to be used. For example, in aeronautics, the dominant data bus standard is ARINC 664 [53], while in the railway domain multiple standards were used to design the gateway server, e.g., Multi-Vehicle Bus (MVB) [54] and Wired Train Bus (WTB) [55] as part of the Train Communication Network (TCN) standard. In the automotive domain, some of the relevant standards are Controller Area Network (CAN) [56] and Local area INterconnect (LIN) [57]. The UC of vehicle platooning exploited the results of previous EU projects, such as Esemble [58], which produced V2x (Vehicle-to-Everything) HW and SW platforms to build new AI-based services.

From a reliability point of view, the aeronautics and vehicular data buses are more demanding in terms of real-time processing than the data-bus standards in other domains. This has consequences on implementation, because there is a need to provide a solution that regulates the network flows between the wireless and the wireline domains, while preserving the quality of service across the hybrid infrastructure.

5) TARGET METRICS

The main metrics addressed by these algorithms lie in the MAC and PHY layers, e.g., Signal-to-Interference-plus-Noise Ratio (SINR) [59], spectral efficiency, throughput, capacity, achievable data rate, signal-to-leakage ratio, rejection ratio, latency, queuing delay, etc. Most of the metrics constitute a measure of the desired indicator with respect to existing impairments. In critical applications, such as aeronautics and vehicle platooning, metrics have more critical thresholds than in other applications such as localization and object tracking inside buildings.

6) TYPES OF ALGORITHMS

CNNs [60] were used in MIMO receivers for vehicular beamforming. SVM [61] was used for beam-forming with reduced complexity compared to CNNs, while PARAFAC [62] and ICA [63] were used to remove multiple access interference and to reduce training bandwidth (i.e., unsupervised learning). DL has shown good results in MIMO systems, but the disadvantage is the complexity of calculations, particularly in scenarios with ultra-low latency requirements and with non-stationary statistics (i.e., rapidly changing datasets).

7) OUTCOMES

In this SBB, multiple AI algorithms for improving wireless signals have been compared in both simulation and real-life hardware platforms. For example, in wireless platooning, the use of AI for massive MIMO reduces the vehicle collision probability in multiple different subscenarios, including those with complicated propagation conditions such as in tunnel environments [64]. In the case of wireless avionics, AI was helpful in improving signal reception, thus enabling real-time operation and reduction of distortion of sensor readings collected across the aircraft [65]. In airport environments, AI was used to detect changes in line- or non-line-of-sight conditions (LOS and NLOS, respectively), thereby improving either network performance or the ability to detect the presence/absence of obstacles and/or passengers.

One of the findings in this SBB was the impact of nonstationary statistics on the effectiveness of ML. Future developments are foreseen to minimize the negative effects. The outcome of this SBB has also shown that capacity and performance limits can be effectively improved by AI, but the analysis is more complex than previously considered. The exact definition of the optimality regions for different AI and conventional signal processing algorithms was found to be a complex problem that needs to be addressed in future work.

B. SBB2.2B—PARAMETER ESTIMATION FOR PHY LAYER SECURITY

1) GENERAL DESCRIPTION

This SBB explicitly exploited or extracted information from physical waves about DoA or other spatial/geometrical patterns that can be used to improve reception, reject interference, increase security, and protect information from different types of attack, including jamming, eavesdropping, impersonation, etc. This type of PHY-layer information can also be used indirectly to estimate other environmental parameters. Examples include airflow estimation in avionics, patient health indicators by using waves bouncing back from target patients (Radcom), obstacle detection, and/or object tracking based on LOS/NLOS detection.

2) DATASETS

The datasets are similar to those discussed in Section IV-A2, but in this case, the estimated parameters explicitly contain geometric information about the environment. When using realistic datasets, it was important to have accurate environmental information to allow the learning algorithm to resolve the direction of incumbent transmissions. In the case of synthetic models, geometric-based stochastic channel distributions or ray tracing are typically needed to correctly replicate the scenario.

3) BB INTERFACES

The interfaces of SBB2.2B are similar to those presented in Section IV-A3, but in this case, the algorithms handle specific spatial information embedded in the measurements that can be used for security, encryption, and attack detection capabilities. Therefore, this additional information means the use of interfaces with application layers dealing with those security features. The interfaces of this SBB with other BBs of the InSecTT framework are illustrated in Fig. 8

4) IMPLEMENTATION DETAILS AND ISSUES

These algorithms have been implemented in SW defined radios, emulators, and/or system-level simulators enabled with realistic channel conditions. Most of the implementation details are the same as the previous SBBs. The main difference lies in which interfaces are used to enable security features on the application layers.

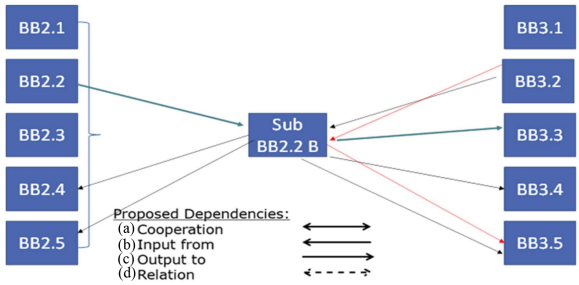

FIGURE 8. Interfaces of SBB2.2B with other BBs.

5) TARGET METRICS

The main target metrics were localization accuracy, DoA Mean Square Error (MSE) [66], interference rejection, SINR, and information secrecy ratio. These are metrics that directly measure the accuracy of the estimation process. However, secondary metrics that measure the impact on other processes, mainly security, safety, reliability, and trustworthiness have also been used across different UCs.

6) TYPES OF ALGORITHMS

Estimation of Signal Parameters via Rotational Invariant Techniques (ESPRITs) [67] was used in nondispersive vehicular channels. Subspace MIMO processing was used to resolve the DoA in more complex multipath scenarios. SVM was also used to estimate DoA inside buildings [68]. Conventional CNNs were used in some specific applications of vehicle platooning (e.g., emergency braking). A similar approach was used in the health care domain to achieve joint communication and radar operation (Radcom). The signals bouncing back from the bodies of patients were used to estimate health indicators.

7) OUTCOMES

The resolution of DoA information from wireless signals using AI has shown several improvements compared to conventional algorithms. However, NN-based ML showed limited gains in highly time-variant scenarios (such as vehicular networks). Hybrid schemes based on SVM and linear prediction, as well as other conventional schemes, such as ESPRIT-based tools or Power Pattern Cross-Correlation (PPCC), were used for this problem with good results. In the case of vehicle platooning, the elements of the platoon conform a reinforced entity for DoA-based PHY-layer security [69]. Each platoon with several vehicles forms a unique spatial signature made of the combined DoAs of all the vehicles. A similar effect can be achieved in cases with a network of distributed sensors on board an aircraft with fixed DoA signatures.

C. SBB2.2 C—LINK AND CHANNEL PREDICTION

1) GENERAL DESCRIPTION

The objective of SBB2.2 C was to use AI/ML to detect and/or predict future channel outcomes. The prediction was not only limited to channel outcomes, but it also addressed other parameters, for example, the number of retransmissions needed

to achieve reliable communications, upcoming system failures, and potential attacks (e.g., jamming, node misbehavior, impersonation, etc.).

2) DATASETS

These datasets are similar to SBB2.2 A and SBB2.2B (presented in Sections IV-A and IV-B, respectively). The datasets of this SBB also include channel measurements and/or synthetic channel models. However, in this case, the channel models have a strong temporal dependence (correlation), mainly because this feature was found to dictate the prediction capabilities of ML algorithms. Therefore, channel measurements or the synthetic models must follow the temporal dynamics of the UC. For example, in vehicular platoons, they must change according to the trajectory and control operations of the platoon. In wireless avionics, they must follow the relative changes inside the cabin or the external conditions of the aircraft across different moments of a mission. Multiple channel measurements with these time-domain features have been completed in several UCs of the EU InSecTT project (see the datasets of SBB2.2 A in Section IV-A).

This SBB has also considered imperfections of the datasets, mainly because multiple industrial applications will not have ideal or complete datasets. Some UCs with rapidly changing settings will have only a few past samples as reliable environmental information. These samples can be enriched with context information available from other functional layers (e.g., positioning/geographical information, etc.). The impairments considered in the datasets were the following: incorrect sampling conditions, incomplete or constrained datasets, and noisy samples.

3) BB INTERFACES

This SBB was one of the most used in the project. One of the reasons for this predominance is that this type of algorithm improves the ability of emerging wireless systems to predict the fast variations of the environment. This ability is ideal for improving efficiency, reducing energy consumption, and increasing data rate performance. Additionally, algorithms can exploit this feature in different layers of the network, with different interfaces and with flexible implementation in different physical entities. For example, in the lower layers, channel prediction can be used to reduce training sequence bandwidth, improve resource allocation, and reduce the number of required retransmissions. This has an impact on the load of the MAC and link-layer signaling overhead. In the upper layers, link prediction can be used to enable seamless vertical handover, reduce session drop probability, improve load balancing, reduce multipaths or trajectories, and optimum route selection. The interfaces of this SBB with other BBs of the InSecTT framework are shown in Fig. 9

4) IMPLEMENTATION DETAILS AND ISSUES

The algorithms in SBB2.2 C have been implemented in multiple platforms that include custom-made HW devices for

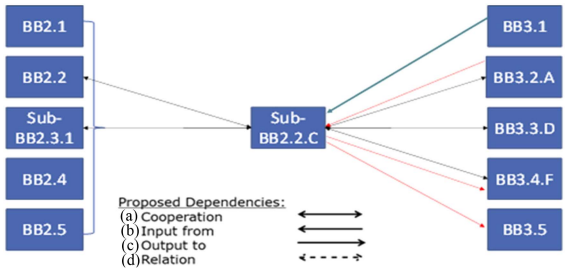

FIGURE 9. Interfaces of SBB2.2 C with other BBs.

V2X technology, Multi-Interface Gateways (MIGs) [70], [71], routers used for multiple link selection and optimization, and radio platforms that aim to detect the best link quality with line- or non-line-of-sight conditions [72], [73]. We highlight the level of maturity of the implementation in industrial prototypes of this class of algorithms as compared to other SBBs, particularly in the networking layers, where constraints are less strict than in the PHY-layer, which facilitates design and implementation.

5) TARGET METRICS

Some of the metrics used in this SBB included: MSE of predicted values, spectral efficiency to measure the impact of improved allocation based on prediction, latency, resource usage efficiency, load balancing, vertical handover success probability, call drop rate, and energy consumption/efficiency. In some cases, distortion metrics were used to compare the estimated/predicted feature with the real outcome of the target parameter. This SBB had a specific target on resource allocation, so multiple metrics of this type of solution were used to measure either directly or indirectly the performance of this type of algorithm.

6) TYPES OF ALGORITHMS

Polynomial weighted linear regression was used to predict oversampled channels in vehicular platooning applications. CNN, Long-Short-Term Memory (LSTM) [74], [75], and Recurrent Neural Networks (RNNs) [76] were used for datasets with near-undersampling distortion in both vehicular and avionics systems. Support Vector Regression (SVR) [77] was used for data rate estimation, while LSTM and Gated Recurrent Unit (GRU) [78], [79] for data rate prediction in railway domains. Finally, multiarmed bandit approaches were used for link selection in V2x communications and inside airports.

7) OUTCOMES

The results of the implementation of this SBB showed how AI can be used effectively to optimize wireless network performance and resource management. However, it is equally clear how sensitive AI was to some of the realistic impairments considered in different UCs (constrained datasets, undersampled information, and low SNR). It became evident that in some conditions, AI can be outperformed by conventional algorithms. Despite these issues, when complete and nearly

ideal datasets were used, ML showed important advantages. The exact boundary for the optimum region of each solution is an open issue to be addressed in future research.

D. SBB2.2D–ANOMALY DETECTION

1) GENERAL DESCRIPTION

This family of algorithms uses ML and DL to capture normalized system behavior by training models over datasets that involve metrics or parameters that span different protocol layers. These algorithms can detect multiple system threats, potential failures, hazards in the PHY-layer environment, or intentional attacks to communication interfaces.

2) DATASETS

It is worth pointing out that the proposed SBB classification is not entirely orthogonal. Therefore, different algorithms presented in previous SBBs can also be considered here, with some modifications, as part of anomaly detection. This is the case of DoA detection and channel prediction. Based on existing datasets, these algorithms can be used to detect changes in the environment (i.e., a change from LOS to NLOS conditions), changes in received power or Received Signal Strength Indicator (RSSI) due to obstacles (e.g., AI-based object detection for platoons), or to detect the distortion of the spatial signature of a fixed network of sensors on board an aircraft. This detection of changes can be tuned to be used as an intrusion or anomaly detection.

The datasets used by anomaly detection in the PHY-layers are similar to those mentioned in the previous SBBs, except for the explicit security objective. This means that the datasets are obtained with the explicit purpose of detecting an inconsistency in the test data and then triggering the detection indicator(s). By contrast, algorithms running on edge application servers consider datasets that have a different granularity level compared to the PHY-layers. Therefore, the problem of nonstationary datasets of the PHY-layer environment is considerably minimized or non-existing in the application layers.

Anomaly detection algorithms in the network and application layers are usually based on a model that has been trained under conventional network operation. Therefore, when using test data, the trained model can detect deviations from the normal behavior as stored in the model.

3) BB INTERFACES

The algorithms of SBB2.2D used multiple interfaces across several layers. However, their operation mainly resides on security and application control layers. The detection and exchange of signaling information generally uses cross-layer and security management interfaces, as depicted in reference IoT architectures (see Annex 1). The interfaces of this SBB with other BBs of the InSecTT framework are shown in Fig. 10.

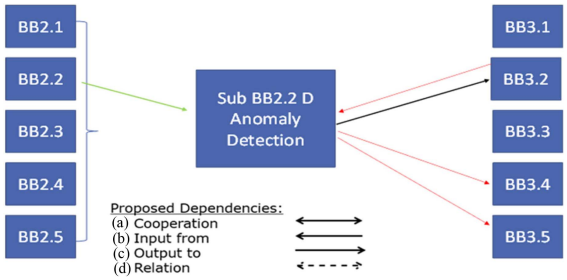

FIGURE 10. Interfaces of SBB2.2D with other BBs.

4) IMPLEMENTATION DETAILS AND ISSUES

Anomaly detection algorithms have been implemented in dedicated HW platforms for application layer management of the different UCs. For example, in vehicular networks, open source 5G core network platforms were used for the implementation of application layer anomaly detection, while in wireless avionics, an internal aeronautics network emulation platform of ARINC 664 has been used for all simulations and security testing. In consumer applications, realistic home routers and commercial firmware emulation platforms were used to detect anomalies and intrusion attacks.

5) TARGET METRICS

Some of the metrics used in this type of algorithm include the following: false alarm probability, and the percentage of anomalies correctly detected/rejected. Similar to other SBBs, secondary metrics can be used to measure the impact of the success of the different detection algorithms.

6) TYPES OF ALGORITHMS

CNNs were used to detect objects or obstructions in LOS in vehicular networks, triggering, for example, emergency braking. DoA distortion and localization errors were used in building, maritime, and airport scenarios to detect potential impersonations. Geometric Kalman was used to detect faults in vehicular scenarios. Random forest was used in anomaly detection for consumer home network protection. Unsupervised energy-based anomaly detection was used in short-range wireless communications. DL algorithms were used for anomaly detection in IoT networks based on MQ Telemetry Transport (MQTT). Hybrid algorithms based on ML and conventional statistical approaches were also reported. They provided flexibility of implementation and higher accuracy, as they exploited the virtues of both approaches.

7) OUTCOMES

Anomaly detection was implemented on multiple layers of the protocol stack. Several of the implementation examples targeted edge infrastructure for each UC. One of the main outcomes of this SBB is the clear tradeoff between the complexity of the algorithm, the granularity of events captured in the dataset, and the layer where the algorithm resides. Lower-layer events required a higher granularity, as the learning process, the dataset generation and, in general, the identification process are resource consuming and usually constrained in latency. By contrast, in the upper layers of the protocol stack, other issues were found, including privacy, confidentiality, and interface bottlenecks. These results also

point toward the need of frameworks specialized in AI cyber risk management [35], [36].

V. DISCUSSION

One of the main contributions of the InSecTT project is the cross-domain analysis of AI implementations. The SBBs described in the previous section have multiple cross-domain links and tradeoff issues. This section provides a summary of some of the relevant issues identified in the previous sections.

A. COMPARISON BETWEEN SBBS

The SBBs described in the previous subsections show multiple similarities and differences in terms of datasets, interfaces, and implementation details. We briefly summarize some of these similarities and differences. Most of the SBBs share the fact that datasets are related to the wireless propagation channel. Exceptions were found in some instances of anomaly detection and link prediction, which can also target upper layer protocol streams. The main difference observed is that SBB2.2B and SBB2.2 C algorithms require, respectively, spatial (geometric) and temporal features to operate, while SBB2.2 A algorithms need detailed information of the impairments to be removed. Different constraints have also been observed, mainly because SBB2.2 A seems to be more prone to nonstationary issues than the other SBBs, while SBB2.2 C seemed more prone to issues of noise, sampling, and incompleteness of datasets.

In terms of implementation, there were important differences among the different SBBs. SBB2.2 C was one of the most frequently deployed types of algorithms on a multitude of existing hardware platforms for several UCs. The flexibility of link prediction was key in its successful implementation across a number of layers and domains. Probably the second best SBB was anomaly detection, due to the strong security and robustness implications for multiple domains and also the decoupling from stringent physical layer real-time requirements and issues that may limit their operation.

Regarding interfaces, the difference is clear among the different SBBs. SBB2.2 A probably has the lower level type of interfaces, as it pertains mainly to symbol and PHY-layer impairment removal processes. However, it is also the most demanding as this type of processes require constant monitoring of environmental changes and adaptation. In contrast, SBB2.2B has a more flexible implementation margin, as DoA information depends on the mobility of the UCs. Only some of the UCs will experience DoA temporal variance that requires high signaling rates for their operation. In addition, this SBB has interfaces with upper-layer security applications, which, in general, handle a more relaxed time granularity in the event distribution than the ultra-low latency PHY-layer. The case of SBB2.2 C and SBB2.2D depends on the type of UC application, but in general, they also occur with less critical issues than in the lower layers. However, other types of issues start to emerge, including security, privacy, confidentiality, etc.

B. CRITICALITY AND EXISTING INFRASTRUCTURE

Wireless avionics and vehicle platooning control have shown some of the strictest requirements in terms of criticality, real-time operation, reliability, and ultra-low latency communications. This is mainly due to the need to comply with industry standards (buses) and also with the requirements of future applications, such as autonomous vehicles, intelligent transportation, and aircraft monitoring and control. Maritime vessels and trains use similar internal bus standards to the automotive domain. However, many of the applications of IoT in this domain focused on added features that are not explicitly interacting with, replacing, or modifying the internal buses. Instead, the investigated applications focused on overlay features such as logistics, localization, and infrastructure control and management, where different requirements and issues usually arise.

C. PERFORMANCE RELIABILITY AND DATASET ISSUES

Massive MIMO assisted by AI was used in urban vehicular scenarios, showing the possibility of considerably reducing interference and even preventing jamming attacks. In contrast, in the operation of WAICs, massive MIMO showed more limitations, mainly due to reduced antenna spacing, which yields stronger channel correlation. In contrast, DL-based channel prediction became more attractive and feasible in aeronautics and low-speed vehicular applications. This is mainly due to the issue of nonstationary datasets and limited measurements in time-varying vehicle applications. In this case, linear regression algorithms were used instead. In health care and indoor building applications, the nonstationary problem is considerably minimized. This means that more advanced and complex ML algorithms, such as DL, were used for purposes such as localization, channel prediction, and biometrical applications.

D. PROPAGATION ISSUES

The channel environment is also relevant for the performance of AI algorithms for wireless applications. The most complex propagation settings found in the project were mainly in indoor or dense urban vehicular scenarios that usually experience complex scattering, diffraction, and shadowing phenomena. Indoor scenarios include sensor communication between the nodes onboard an aircraft, and some of the airport UCs. The main difference between these two domains is that inside some of the vehicles or aircraft, channels can remain more stable over several moments of a mission (stationary), which can facilitate the use of more advanced ML algorithms. In contrast, in vehicular applications with high speeds or dense urban settings, inaccurate sampling frequencies, and constrained datasets were found to reduce the optimality of DL. Health care and building UCs were not found to be highly affected by significant channel time variations (low Doppler shift), but they can show coverage holes, dense multipath, and shadowing conditions. In the maritime domain, reflections over water were found to produce an effect that

resembles stochastic fading found in other domains. However, more research is needed to investigate its impact on different applications.

E. LOW-LAYER VERSUS APPLICATION-LAYER ISSUES

In many of our UCs, the use of AI for anomaly detection in the networking and application layers seems to be less prone to the critical problems of PHY-layer algorithms. However, other emerging issues were observed, such as privacy, confidentiality, robustness, incomplete datasets, etc. In terms of explainability, it was possible to verify some properties and bounds of AI algorithms, particularly when predicting fast-fading wireless channel components that are common in vehicular and aeronautical scenarios. These findings can also be applied in building, maritime, and health care scenarios, except for the existence and prevalence in some cases of long-term deterministic channel components. In such cases, the prediction can become more reliable for periods of time longer than the coherence time of the fast-fading components. This deterministic component changes the applicability of some of the prediction algorithms.

F. STANDARDIZATION AND REGULATION

In several industrial domains and their associated regulatory or standardization groups, there is a growing interest in AI, but the focus is generally on aspects central to the type of application of the industrial domain rather than wireless connectivity. Instead, we found more active work in those bodies with explicit working groups on wireless communications such as the European Telecommunications Standards Institute (ETSI) [80], IEEE [81], ITU [82], and the Third Generation Partnership Project (3GPP) [10]. In the IoT realm, ISO [83] has set up multiple groups working on AI for IoT. In contrast, in network and application layers, AI-based security is extensively covered by the main governmental bodies, such as the European Agency for Cyber Security (ENISA) [84].

In the automotive domain, AI for autonomous cooperative vehicle control has dominated the discussions in recent years, for example, in the Society of Automotive Engineers (SAE) [85] and in the 5G Automotive Association (5GAA) [86]. In the aeronautics domain, the International Civil Aviation Organization (ICAO) [87], the European Organization for Civil Aviation Equipment (EUROCAE) [88] and the European Union Aviation and Safety Association (EASA) [89] have considered AI mainly for control of functionalities on board aircraft, but not precisely for the improvement of WAICs. This is also due to the fact that, unlike solutions in other domains, WAICS is still in the phase of evaluation and standardization. The aeronautics industry has high-quality and secure/safety-critical standards for the integrity of aircraft. Therefore, it takes more time for a technology to gain the trust of the different stakeholders. This is not the same for terrestrial networks, where 5G, Bluetooth Low Energy (BLE), Wi-FI, long range (LoRA), Ultra-wideband (UWB), and other standard technologies have started to be used in airports, on board buses, etc.

VI. CONCLUSION

This article presented a summary of how AI has been used to improve the wireless connectivity of multiple industrial UCs of the InSecTT EU project. The article also described some of the details of the alignment process of UCs and their BBs with the InSecTT RA and the investigation of which interfaces or sublayers of the different protocol stacks are more used by new AI functionalities. This investigation returns interesting results, providing details to designers on how AI is being used in realistic industrial applications, the issues that are being faced, challenges, and potential benefits that are currently being more exploited. More specific information for each UC can be found on the website of the project. The article also highlights the multiple gaps found in the project on how AI behaves in different types of impairments and different challenging situations. As an example, in the lower layers of the protocol stack with critical requirements, such as low latency and high reliability, DL still faces several practical challenges, including nonstationary, incomplete, or corrupted datasets. This gap seemed to be filled by conventional algorithms, such as linear regression, SVM, ESPRIT, Random Forest, etc., particularly for applications such as beam-forming, PHY-layer security, and interference rejection. In contrast, in the upper layers of the protocol stack, the obstacles found in the applicability of AI and ML were related to aspects such as information confidentiality, privacy, storage, and security. All of the above-mentioned issues showed different details depending on the industrial domains. As an example, in the vehicular domain, challenges are also the adaptation of ML to multiple issues and realistic situations with the lack of datasets or with distorted or inaccurate information due to the highly time-varying media. In contrast, in health care and in general in indoor applications, privacy, confidentiality, and the probability of eavesdropping were found to be issues of more concern. The railway UCs showed some issues similar to the vehicular UCs, but with interesting deviations. One major difference is the extension of the wireless footprint required for long-distance railway infrastructure. Another difference is the propagation between contiguous vehicles of a train, which shows considerable deviations from a vehicular platoon scenario, including scattering, shadowing, and interference distributions. Furthermore, railway control and operation of the applications investigated in the project showed no major need for ultralow-latency requirements, unlike the critical vehicular link reliability and latency needed in autonomous vehicular applications. These are examples of how the InSecTT cross-domain perspective and the RA can provide in the study of the implementation tradeoffs of AI in different entities and stack layers of IoT UCs.

ANNEX 1: INSECTT REFERENCE ARCHITECTURE

The InSecTT RA is a collection of views, models, perspectives, and/or recommendations for the design of UC architectures based on the objectives of the InSecTT project (i.e., convergence of AI, edge computing, and IoT) targeting

trustworthiness and security metrics. The InSecTT RA (presented in a preliminary form in [7]) is based on a combination of modern standard RAs and was the result of an evolution of two previous EU projects, namely "Dependable Wireless Infrastructure" (DEWI) [90] and "Secure Connected Trustable Things" (SCOTT) [50]. In particular, the InSecTT RA inherits functional layers of the ISO Sensor Network RA (SNRA) [91] through the evolution of the DEWI high-level architecture (HLA), and adopts a convergence of functionality models previously used in SCOTT, including components from ISO IoT RA [43], the ITU RA [41], the IEEE [42], and the AIOTI [44] RAs. Therefore, by aligning UCs to the InSecTT RA, UCs are also largely compatible with the main views of these standard RAs. Figs. 2 and 3 show the two central perspectives of the InSecTT RA: 1) the *entity* and 2) the *functionality models*, respectively. The InSecTT entity model is an evolution of the representation of physical entities of legacy architectures with devices, objects, and network elements. These elements interact with each other via hardware (HW) interfaces. By contrast, the functionality model consists of layers and sublayers of organized functionalities running on each entity, and mainly interacting with each other via software (SW) interfaces. A *hybrid entity-functionality model* can also be used to illustrate the interaction between functionality sublayers across different HW entities (see Annex 3).

The analysis of functionalities of multiple UCs and BBs using a standard RA can help not only to gain insight into the project infrastructure and its organization, but it can also reveal stress points, vulnerabilities, scalability issues, technical needs, or even future technology trends.

One of the main aspects that differentiates the InSecTT RA from other architectures is the concept of "*Bubble,*" inherited from previous projects (DEWI and SCOTT). The Bubble can be defined as a construct used for the organization of infrastructure in industrial networks, encapsulating legacy technology via wrapping layers based on modern IoT protocols, where the *Bubble gateway (BGW)* orchestrates and manages all the interactions between the internal legacy network and the modern IoT cloud-edge continuum (see Fig. 2). The Bubble has a specialized three-tier (L0/L1/L2) entity model that is useful for industrial scenarios with an existing wired or critical infrastructure (e.g., internal bus of a vehicle or an aircraft). The Bubble concept has evolved in recent years to encapsulate new features, such as objects with multiple interfaces, direct cloud links based on technologies like 5G [10] or Narrow-Band IoT (NB-IoT) [92], and new technologies such as edge computing, blockchain [93], and now, in the current project, using edge technology and AI.

ANNEX 2: OTHER USAGES OF THE INSECTT REQUIREMENTS PROCESSING FRAMEWORK

The InSecTT framework for the processing of RQ information (Section III) was inherited from previous projects. This processing framework, as detailed in the main body of this article, was used for architecture design. However, it has evolved and has additional usages. For example, the status of implementation of RQs was used for monitoring and objective completion evaluation. This methodology consists of providing scores to the implementation progress of each requirement and its associated objectives. This scoring methodology provided us with a useful perspective on how the project was being completed at different stages, and it became a valuable tool to detect potential risks or issues in the technical work of the project. Another RQ-based scoring methodology was also developed for the evaluation of trustworthiness metrics of SBBs. These metrics were based on well-known certification metric methodologies such as *Common Weakness Score System* (CWSS) [94], *Common Vulnerability Score System* (CVSS) [95], and certification frameworks such as ARMOUR [96]. This trustworthiness approach constitutes a more realistic evaluation of complex IoT systems.

ANNEX 3: FUNCTIONALITY MODEL AND SBBS DEFINITION

The objective of the alignment of the RQs with the InSecTT RA was the layered organization of the functional components of the BBs, and the eventual definition of the InSecTT functionality model. These functionality components can be seen as the "*basic bricks*" that enable the main features of the different UCs. An important result of our analysis was the need for an intermediate granularity level between the raw technical components and the BBs listed in Table 2. This intermediate granularity was needed to consolidate contributions with similar scope across industrial domains. The new granularity was called *SBB*, where cross-domain development was more effective due to the narrowing and alignment of the functional scope of each category across domains. Therefore, a *SBB is defined as a group of functionalities that are common to multiple UCss in different industrial domains, thus fostering cross-domain collaboration*. Fig. 4 shows the timeline of the InSecTT cross-domain design process and the stage at which the definition of SBBs was achieved in the project.

Two possible SBB classifications for BB2.2 are shown in Table 4. The first classification, denoted as C1, considers AI functionalities as classification criteria. These functionalities include parameter extraction, estimation, classification, detection, learning, and adaptation. By contrast, the second classification, denoted as C2, considers communication-related goals as classification criteria. C2 was selected as the official SBB definition of T2.2 in the project. Both classifications were not entirely orthogonal, meaning that some algorithms could belong in more than one subdivision. For example, a link prediction algorithm can also be used (with modifications) for anomaly detection. For simplicity, they were assigned the most relevant classification (see Table 4).

A. CLASSIFICATION BY AI FUNCTIONALITY (C1)

As portrayed in Fig. 11, this category has employed AI-related functionalities as classification criteria.

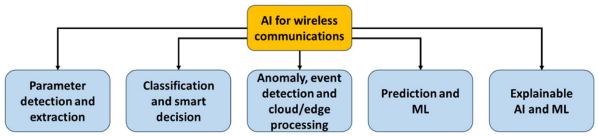

FIGURE 11. SBB classification based on AI-related functionalities (C1).

1) PARAMETER ESTIMATION

These algorithms are used to estimate a value, parameter, metric, or functional rule embedded or inherent to a dataset. The estimated quantities can be used explicitly by another process or an application layer algorithm (e.g., localization, identification, etc.).

2) CLASSIFICATION AND SMART DECISION

The objective of this category is to distinguish the outcomes of a set and assign them to categories. In order to achieve this goal, the training is conducted over sets that capture the possible outcomes of the experiment.

3) PREDICTION AND ML

The prediction of a parameter (such as channel and/or interference attack) is helpful in wireless opportunistic systems that aim to improve the transmission of information by adapting its configuration to the foreseen impairments. Because the wireless medium consists of random phenomena, any information ahead of potential impairments or attacks can be used to improve the reliability of the system by assigning additional resources to compensate for the negative effects and keep link quality at the desired level.

4) ANOMALY DETECTION AND CLOUD/EDGE PROCESSING

Wireless system indicators/metrics can be used to train ML models to capture the patterns of correct or normalized system behavior. An attack occurrence, as well as a failure, can be detected by the ML model in almost real-time, particularly when such ML algorithms are running at the edge. The ability to detect these anomalies in the shortest amount of time and with the highest possible accuracy is one of the main objectives of research in critical industrial environments.

5) EXPLAINABLE AI AND ML

One central objective of the EU InSecTT project was to understand *how* and *why* various AI algorithms work, under which circumstances they show stable operation, and how impairments can lead to failure. This aspect has received the name of *explainability* of AI [97], a topic that currently attracts more attention in academic and industrial communities.

B. CLASSIFICATION BY COMMUNICATION FUNCTIONALITY (C2)

The second proposed category (denoted as C2) used communication aspects as classification criteria. This is in contrast withC1 presented in Section VI-A, which used specific AI-related functionalities. C2 was also the finally selected category for task T2.2 in the EU InSecTT project. A graphical representation of C2 is given in Fig. 6. We recall that this classification was used to foster collaboration between different partners that were dealing with similar design issues in different UCs or industrial domains.

1) SIGNAL IMPROVEMENT IN INTERFERENCE SCENARIOS

The main goal of this type of algorithm is to improve wireless signal reception by explicitly optimizing a target signal domain or the information subspace of a MIMO wireless system [98] while removing the sources of impairments (such as fading, noise, and interference). The learning process can be conducted along the physical resources (space, time, frequency, etc.) that carry the desired information symbols.

2) PARAMETER ESTIMATION/EXTRACTION FOR PHY-LAYER SECURITY

In this category, the goal is the extraction of PHY-layer information from the wireless signal. For exampleposition, angle-of-arrival (AoA) [99], distance, etc.. The focus was on spatial (geometric) information to achieve security in the PHY-layer. For example, AoA or DoA [100] information constitutes unique a spatial signature of the elements of a network, which can be used to improve authentication protocols.

3) LINK AND CHANNEL PREDICTION

Algorithms explicitly target the prediction of future channel or link states (as detailed in Section VI-A3). In the C1 classification, link and channel prediction are aligned with communication-related goals, such as resource allocation, link adaptation, beam-forming, equalization, etc.

4) ANOMALY DETECTION

In this category, the models have been trained with datasets that capture normalized network behavior and that can be used to detect deviations from such behavior (as detailed in Section VI-A4). Anomaly detection has been conducted in the project at different layers of the protocol stack, feeding, or triggering events in the same or across other layers/entities of the architecture that contain security-specific BBs. This triggering usually depends on an interface that wraps-up information from one layer to present it in a higher security layer (i.e., cross-layer interface).

C. ARCHITECTURE ALIGNMENT

The first step in the alignment process with the InSecTT RA was the grouping of RQs into technical components that contain the common functionalities of each UC and/or BB. These components were initially mapped to the two central views of the InSecTT RA: the entity and functionality model views. To illustrate this process, Figs. 12 and 13 show, respectively, the explicit mapping of functionalities and components of BB2.2 and BB3.2. BB3.2 deals with reliable wireless models, datasets, and algorithms, particularly to be optimized by the AI algorithms of BB2.2. Therefore, BB3.2 can be considered

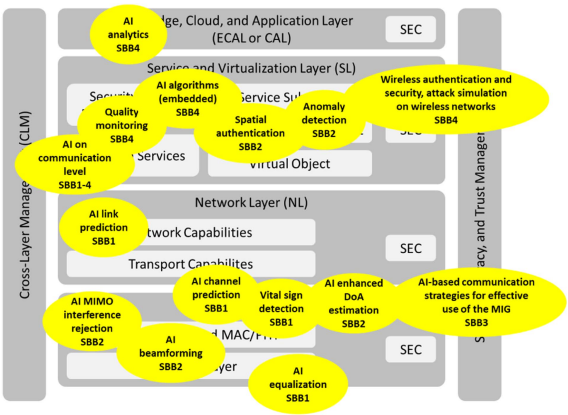

FIGURE 12. Alignment of BB2.2 to the functionality model of the InSecTT RA.

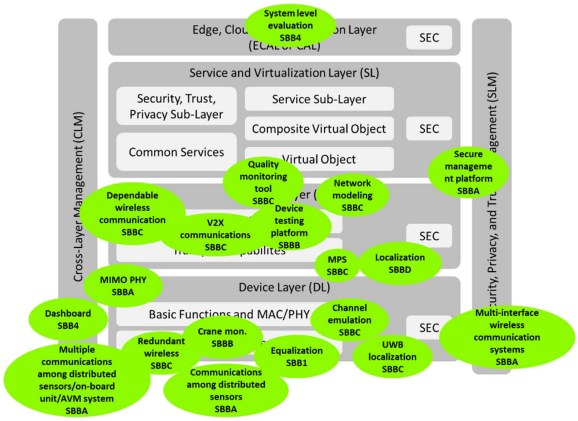

FIGURE 13. Alignment of BB3.2 to the functionality model of the InSecTT RA.

as the twin partner of BB2.2. It can be observed that all the AI algorithms of BB2.2 lie in higher functionality layers with respect to BB3.2. This denotes the synergy between the real world (PHY-layer) models and the optimization and organization functionalities provided by BB2.2.

An example of the alignment of all BB components of a UC and their functionality information flow is illustrated in Fig. 14 for the case of UC1 (Wireless platooning intra-communications). In this figure, different colors denote the different BBs; arrows denote the interface and the direction of the information flow in the UC; and the text inside the arrows denotes the technological interface or data format used. This mapping/alignment process can also be conducted over a hybrid entity-functionality model, which provides us with a more detailed perspective of both HW and SW interfaces used in a UC. An example of this hybrid modeling is illustrated in Fig. 15 for the particular case of UC1. Each entity of each UC replicates a copy of the functionality layered model of the InSecTT RA. In this hybrid model, the SBBs are placed in different functional layers of different entities and the communication between them takes place over a combination of HW/SW interfaces.

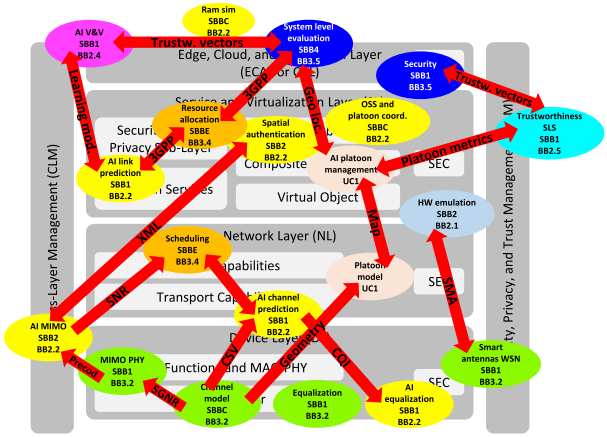

FIGURE 14. Alignment of the BBs of UC1 to the functionality model of the InSecTT RA.

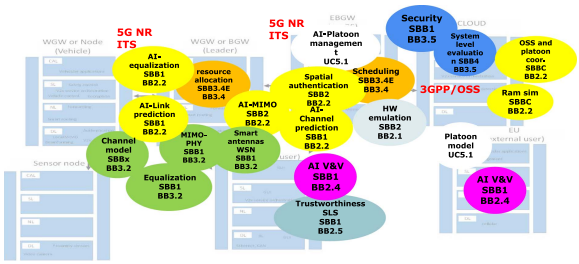

FIGURE 15. Alignment of the SBBs of UC1 to the hybrid entity versus functionality model of the InSecTT RA.

ACKNOWLEDGMENT

Disclaimer: 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.

REFERENCES

[1] AI market size. Accessed: Feb. 9, 2024. [Online]. Available: https://www.statista.com/statistics/1365145/artificial-intelligence-market-size/

[2] EU artificial intelligence act. Accessed: Jan. 26, 2024. [Online]. Available: https://artificialintelligenceact.eu/the-act/

[3] N. A. Khan and S. Schmid, "AI-RAN in 6G networks: State-of-the-art and challenges," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 294–311, 2024.

[4] M. E. Morocho-Cayamcela, H. Lee, and W. Lim, "Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions," *IEEE Access*, vol. 7, pp. 137184–137206, 2019, doi: 10.1109/ACCESS.2019.2942390.

[5] Intelligent secure trustable things (InSecTT). Accessed: Jan. 26, 2024. [Online]. Available: www.insectt.eu

[6] InSecTT project videos and demonstrators. Accessed: Feb. 14, 2024. [Online]. Available: https://www.youtube.com/,insecttproject9852

[7] M. Karner, J. Hillebrand, M. Klocker, and R. Sámano-Robles, "Going to the edge - Bringing Internet of Things and artificial intelligence together," in *Proc. 24th Euromicro Conf. Digit. Syst. Des.*, Palermo, Italy, 2021, pp. 295–302, doi: 10.1109/DSD53832.2021.00052.

[8] X. Kong, Y. Wu, H. Wang, and F. Xia, "Edge computing for Internet of Everything: A survey," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 23472–23485, Dec. 2022, doi: 10.1109/JIOT.2022.3200431.

[9] V. C. Farias da Costa, L. Oliveira, and J. de Souza, "Internet of everything (IoE) taxonomies: A survey and a novel knowledge-based taxonomy," *Sensors*, vol. 21, no. 2, 2021, doi: 10.3390/s21020568.

[10] Third Generation Partnership Project (3GPP), "5G system overview," Accessed: Jan. 26, 2024. [Online]. Available: https://www.3gpp.org/technologies/5g-system-overview

[11] J. Kaur and M. A. Khan, "Sixth generation (6G) wireless technology: An overview, vision, challenges and use cases," in *Proc. IEEE Region 10 Symp.*, Mumbai, India, 2022, pp. 1–6, doi: 10.1109/TENSYMP54529.2022.9864388.

[12] S. Haykin, *Unsupervised Adaptive Filtering*. Hoboken, NJ, USA: Wiley, 2000.

[13] S. Haykin, *Neural Networks and Learning Machines*. London, U.K.: Pearson, 2008.

[14] S. Kim, I. Petrunin, and H.-S. Shin, "A review of Kalman filter with artificial intelligence techniques," in *Proc. Integr. Commun. Navigation Surveill. Conf.*, 2022, pp. 1–12.

[15] N. Farsad and A. Goldsmith, "Neural network detection of data sequences in communication systems," *IEEE Trans. Signal Process.*, vol. 66, no. 21, pp. 5663–5678, Nov. 2018.

[16] O. P. Awe, A. Deligiannis, and S. Lambotharan, "Spatio-temporal spectrum sensing in cognitive radio networks using beamformer-aided SVM algorithms," *IEEE Access*, vol. 6, pp. 25377–25388, 2018.

[17] M. Tarkowski, M. Burtowy, M. Rzymowski, K. Nyka, M. Groth, and L. Kulas, "Improved RSS-Based DoA estimation accuracy in low-profile ESPAR antenna using SVM approach," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom.*, 2019, pp. 1759–1763.

[18] Y. Chen, J. Mohammadi, S. Wesemann, and T. Wild, "Turbo-AI, Part I: Iterative machine learning based channel estimation for 2D massive arrays," in *Proc. IEEE 93rd Veh. Technol. Conf.*, 2021, pp. 1–6.

[19] G. Kia, L. Ruotsalainen, and J. Talvitie, "A CNN approach for 5G mm Wave positioning using beamformed CSI measurements," in *Proc. Int. Conf. Localization GNSS*, 2022, pp. 1–7.

[20] Research library machine learning for communications. Accessed: Feb. 10, 2024. [Online]. Available: https://mlc.committees.comsoc.org/research-library/

[21] A. He et al., "A survey of artificial intelligence for cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1578–1592, May 2010.

[22] A. Celik and A. M. Eltawil, "At the dawn of generative AI era: A tutorial-cum-survey on new frontiers in 6G wireless intelligence," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2433–2489, 2024.

[23] D. C. Nguyen et al., "Enabling AI in future wireless networks: A data life cycle perspective," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 553–595, First Quarter 2021.

[24] *Rohde & Swartz*, "Thinksix," Accessed: Feb. 11, 2024. [Online]. Available: https://www.youtube.com/watch?v=BQyxBYzdg5k

[25] R.-F. Liao, H. Wen, J. Wu, H. Song, F. Pan, and L. Dong, "The Rayleigh fading channel prediction via deep learning," *Wireless Commun. Mobile Comput.*, vol. 2018, 2018, Art. no. 6497340.

[26] T. Zhou, H. Zhang, B. Ai, C. Xue, and L. Liu, "Deep-learning based spatial-temporal channel prediction for smart high-speed railway communication networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 7, pp. 5333–5345, Jul. 2022.

[27] T. Zhang, S. Liu, W. Xiang, L. Xu, K. Qin, and X. Yan, "A real-time channel prediction model based on neural networks for dedicated short-range communications," *Sensors*, vol. 19, no. 16, 2019, Art. no. 3541.

[28] J. P. Lemayian and J. M. Hamamreh, "Massive MIMO channel prediction using recurrent neural networks," *RS Open J. Innov. Commun. Technol.*, vol. 1, no. 1, 2020, Art. no. 8.

[29] I. Abidi, M. Hizem, I. Ahriz, M. Cherif, and R. Bouallegue, "Convolutional neural networks for blind decoding in sparse code multiple access," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf.*, 2019, pp. 2007–2012.

[30] R. Zhang, N. Sidiropoulos, and M. Tsatsanis, "Collision resolution in packet radio networks using rotational invariance techniques," *IEEE Trans. Commun.*, vol. 50, no. 1, pp. 146–155, Jan. 2002.

[31] B. Ozgul and H. Delic, "Wireless access with blind collision-multiplicity detection and retransmission diversity for quasi-static channels," *IEEE Trans. Commun.*, vol. 54, no. 5, pp. 858–867, May 2006.

[32] R. Zhang, J. Wang, H. Zhou, and T. Ban, "An improved least squares constant modulus algorithm for collision messages separation in multichannel space-based AIS," *Int. J. Satell. Commun. Netw.*, vol. 36, no. 5, pp. 440–450, 2018.

[33] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A malicious Bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3242–3254, Mar. 2021.

[34] M. H. Moghadam, M. Rzymowski, and L. Kulas, "Enabling smart retrofitting and performance anomaly detection for a sensorized vessel: A maritime industry experience," 2024, *arXiv:2401.00112*, doi: 10.48550/arXiv.2401.00112.

[35] R. Mohandas, K. K. Vaigandla, N. Sivapriya, and K. Kirubasankar, "Detection and evaluation of cybersecurity threats in MANET based on AI," in *Proc. 2024 4th Int. Conf. Ubiquitous Comput. Intell. Inf. Syst. (ICUIS)*, Gobichettipalayam, India, 2024, pp. 1486–1492, doi: 10.1109/ICUIS64676.2024.10867165.

[36] P. H. Kim and K.-H. Kim, "Deep learning-based SBOM defect detection for medical devices," in *Proc. 2024 Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Osaka, Japan, 2024, pp. 47–51, doi: 10.1109/ICAIIC60209.2024.10463483.

[37] B. Sudharsan, J. G. Breslin, and M. I. Ali, "ML-MCU: A framework to train ML classifiers on MCU-based IoT edge devices," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 15007–15017, Aug. 2022.

[38] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1251–1275, Second Quarter 2020.

[39] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surv. Tuts.*, vol. 22, no. 3, pp. 1686–1721, Third Quarter 2020.

[40] Internet of Things architecture. EU project. Accessed: Jan. 26, 2024. [Online]. Available: https://www.iot-a.eu/

[41] *ITU- Y.2060: Overview of the Internet of things (Reference Architecture)*. Accessed: Jan. 26, 2024. [Online]. Available: https://www.itu.int/rec/T-REC-Y.2060-201206-I

[42] *IEEE 2413-2019–IEEE Standard for an Architectural Framework for the Internet of Things (IoT)*. Accessed: Jan. 26, 2024. [Online]. Available: https://standards.ieee.org/ieee/2413/6226/

[43] *ISO/IEC 30141:2018, Internet of Things (IoT), Reference Architecture*. Accessed: Jan. 26, 2024. [Online]. Available: https://www.iso.org/standard/65695.html

[44] Alliance for Internet of Things innovation. Accessed: Jan. 26, 2024. [Online]. Available: http://www.aioti.eu/

[45] P. Radanliev, O. Santos, and A. Brandon-Jones, "Capability hardware enhanced instructions and artificial intelligence bill of materials in trustworthy artificial intelligence systems: Analyzing cybersecurity threats, exploits, and vulnerabilities in new software bills of materials with artificial intelligence," *J. Defense Model. Simul.*, 2024, Art. no. 15485129241267919.

[46] P. Radanliev, D. De Roure, C. Maple, J. R. Nurse, R. Nicolescu, and U. Ani, "AI security and cyber risk in IoT systems," *Front. Big Data*, vol. 7, 2024, Art. no. 1402745.

[47] OPNsense: Open source platform. Accessed: Jan. 26, 2024. [Online]. Available: https://opnsense.org/

[48] Open platform communications unified architecture. Accessed: Feb. 14, 2024. [Online]. Available: https://opcfoundation.org/about/opc-technologies/opc-ua/

[49] Open network architecture platform. Accessed: Feb. 14, 2024. [Online]. Available: https://www.onap.org/

[50] Secure connected trustable things (SCOTT). Accessed: Jan. 26, 2024. [Online]. Available: https://scottproject.eu/

[51] Technical characteristics and operational objectives for wireless avionics intracommunications (WAIC) Report M.2197 (ITU-R Report). Accessed: Feb. 14, 2024. [Online]. Available: http://www.itu.int/pub/R-REP-M.2197

[52] Technical characteristics and spectrum requirements of Wireless Avionics IntraCommunications systems to support their safe operation, Report ITU-R M.2283, approved Dec. 2013. Accessed: Feb. 14, 2024. [Online]. Available: http://www.itu.int/pub/R-REP-M/publications.aspx?lang=en&parent=R-REPM.2283

[53] Aeronautical Radio Incoporated, ARINC 664. Accessed: Feb. 14, 2024. [Online]. Available: http://www.aviation-ia.com

[54] IEC 61375-3-1:2012 Electronic railway equipment - Train communication network (TCN) - Part 3-1: Multifunction Vehicle Bus (MVB). Accessed: Feb. 14, 2024. [Online]. Available: https://webstore.iec.ch/publication/5402

[55] IEC 61375-2-1:2012 Electronic railway equipment - Train communication network (TCN) - Part 2-1: Wire Train Bus (WTB). Accessed: Feb. 14, 2024. [Online]. Available: https://webstore.iec.ch/publication/5398

[56] CAN (controller area network), ISO 11898 . Accessed: Feb. 14, 2024. [Online]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=59165

[57] ISO/CD 17987-8 Road vehicles - Local interconnect network (LIN) – Part 8: Electrical physical layer (EPL) specification: LIN over DC power line (DC-LIN). Accessed: Feb. 14, 2024. [Online]. Available: https://www.iso.org/standard/71044.html

[58] Esemble EU project platooning. Accessed: Feb. 14, 2024. [Online]. Available: https://platooningensemble.eu/

[59] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009, doi: 10.1109/JSAC.2009.090902.

[60] A. Mazinani, L. Davoli, D. P. Pau, and G. Ferrari, "Air quality estimation with embedded AI-Based prediction algorithms," in *Proc. Int. Conf. Inf. Technol. Res. Innov.*, Jakarta, Indonesia, 2023, pp. 87–92, doi: 10.1109/ICITRI59340.2023.10249864.

[61] A. Kurani et al., "A comprehensive comparative study of artificial neural network (ANN) and support vector machines (SVM) on stock forecasting," *Ann. Data Sci.*, vol. 10, no. 1, pp. 183–208, 2021, doi: 10.1007/s40745-021-00344-x.

[62] R. A. Harshman and M. E. Lundy, "PARAFAC: Parallel factor analysis," *Comput. Statist. Data Anal.*, vol. 18, no. 1, pp. 39–72, 1994, doi: 10.1016/0167-9473(94)90132-5.

[63] A. Hyvärinen and E. Oja, "Independent component analysis: Algorithms and applications," *Neural Netw.*, vol. 13, no. 4, pp. 411–430, 2000, doi: 10.1016/S0893-6080(00)00026-5.

[64] P. Duarte et al., "5G network as key-enabler for vehicular platooning," in *Proc. 20th Annu. IEEE Int. Conf. Sens. Commun. Netw.*, 2023, pp. 369–371.

[65] R. Sámano et al., "Active flow control using dense wireless sensor and actuator networks," *Microprocessors Microsystems*, vol. 61, pp. 279–295, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S014193311830036X

[66] D. C. Montgomery and G. C. Runger, *Applied Statistics and Probability for Engineers*. Hoboken, NJ, USA: Wiley, 2011.

[67] R. Roy and T. Kailath, "ESPRIT-Estimation of signal parameters via rotational invariance techniques," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 37, no. 7, pp. 984–995, Jul. 1989, doi: 10.1109/29.32276.

[68] M. Tarkowski and L. Kulas, "RSS-based DoA estimation for ESPAR antennas using support vector machine," *IEEE Antennas Wireless Propag. Lett.*, vol. 18, no. 4, pp. 561–565, Apr. 2019.

[69] M. Rzymowski and L. Kulas, "Two-row ESPAR antenna with simple elevation and azimuth beam switching," *IEEE Antennas Wireless Propag. Lett.*, vol. 20, no. 9, pp. 1745–1749, Sep. 2021.

[70] E. Pagliari, L. Davoli, A. Cilfone, and G. Ferrari, "A modular multi-interface gateway for heterogeneous IoT networking," in *Proc. Int. Symp. Adv. Elect. Commun. Technol.*, Marrakech, Morocco, 2020, pp. 1–6, doi: 10.1109/ISAECT50560.2020.9523689.

[71] E. Pagliari, L. Davoli, and G. Ferrari, "Harnessing communication heterogeneity: Architectural design, analytical modeling, and performance evaluation of an IoT multi-interface gateway," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 8030–8051, Mar. 2024, doi: 10.1109/JIOT.2023.3317672.

[72] K. Yu and Y. J. Guo, "Statistical NLOS identification based on AOA, TOA, and signal strength," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 274–286, Jan. 2009, doi: 10.1109/TVT.2008.924975.

[73] F. Carpi et al., "Experimental analysis of RSSI-based localization algorithms with NLOS pre-mitigation for IoT applications," *Comput. Netw.*, vol. 225, 2023, Art. no. 109663, doi: 10.1016/j.comnet.2023.109663.

[74] A. Mazinani, L. Davoli, D. P. Pau, and G. Ferrari, "Accurate classification of sport activities under tiny deployability constraints," in *Proc. IEEE Int. Conf. Internet Things Intell. Syst.*, Bali, Indonesia, 2023, pp. 261–267, doi: 10.1109/IoTaIS60147.2023.10346056.

[75] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997, doi: 10.1162/neco.1997.9.8.1735.

[76] M. Tovar, M. Robles, and F. Rashid, "PV power prediction, using CNN-LSTM hybrid neural network model. case of study: Temixco-Morelos, México," *Energies*, vol. 13, no. 24, Dec. 2020, Art. no. 6512, doi: 10.3390/en13246512.

[77] M. Awad and R. Khanna, *Support Vector Regression*. New York, NY, USA: Apress, 2015, pp. 67–80, doi: 10.1007/978-1-4302-5990-9_4.

[78] A. Mazinani, L. Davoli, and G. Ferrari, "Deep learning-based cryptocurrency price prediction: A comparative analysis," in *Proc. 5th Conf. Blockchain Res. Appl. Innov. Netw. Serv.*, Paris, France, 2023, pp. 1–8, doi: 10.1109/BRAINS59668.2023.10317011.

[79] J. Chung et al., "Empirical evaluation of gated recurrent neural networks on sequence modeling," 2014, *arXiv:1412.3555*, doi: 10.48550/arXiv.1412.3555.

[80] European Telecommunications Standards Institute" Accessed: Feb. 14, 2024. [Online]. Available: https://www.etsi.org/

[81] Institute of Electrical and Electronics Engineers. Accessed: Feb. 14, 2024. [Online]. Available: https://www.ieee.org/

[82] International Telecommunicatuions Union. Accessed: Feb. 14, 2024. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx

[83] International Standards Organisation. Accessed: Feb. 14, 2024. [Online]. Available: https://www.iso.org

[84] European Union Agency for Cybersecurity. Accessed: Feb. 14, 2024. [Online]. Available: https://www.enisa.europa.eu/

[85] Society of Automotive Engineers. Accessed: Feb. 14, 2024. [Online]. Available: https://www.sae.org/

[86] 5G Automotive Association. Accessed: Feb. 14, 2024. [Online]. Available: https://5gaa.org/

[87] International Civil Aviation Organiztaion. Accessed: Feb. 14, 2024. [Online]. Available: https://www.icao.int/

[88] The European Organisation for Civil Aviation Equipment. Accessed: Feb. 14, 2024. [Online]. Available: https://www.eurocae.net/

[89] European Union Aviation Safety Agency. Accessed: Feb. 14, 2024. [Online]. Available: https://www.easa.europa.eu/

[90] Dependable Embedded Wireless Infrastructure (DEWI). Accessed: Jan. 26, 2024. [Online]. Available: https://cordis.europa.eu/project/id/621353

[91] ISO/IEC 29182-7:2015, Information technology, Sensor networks: Sensor Network Reference Architecture (SNRA). Accessed: Jan. 26, 2024. [Online]. Available: https://www.iso.org/standard/57097.html

[92] E. M. Migabo, K. D. Djouani, and A. M. Kurien, "The narrowband Internet of Things (NB-IoT) resources management performance state of art, challenges, and opportunities," *IEEE Access*, vol. 8, pp. 97658–97675, 2020.

[93] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54478–54497, 2021.

[94] *ITU-T Rec. X.1525, Common weakness scoring*. Accessed: Feb. 14, 2024. [Online]. Available: https://www.itu.int/rec/T-REC-X.1525/en

[95] *ITU-T Rec. X.1521 (03/2016) Common vulnerability scoring*. Accessed: Feb. 14, 2024. [Online]. Available: https://www.itu.int/rec/T-REC-X.1521/en

[96] Large-scale experiments of IoT security trust (ARMOUR). Accessed: May 26, 2024. [Online]. Available: https://cordis.europa.eu/project/id/688237

[97] M. Quinn, B. Piper, J. P. Bliss, and D. Keever, "Recommended methods for using the 2020 NIST principles for AI explainability," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, 2020, pp. 2034–2037.

[98] H. Sampath, S. Talwar, J. Tellado, V. Erceg, and A. Paulraj, "A fourth-generation MIMO-OFDM broadband wireless system: Design, performance, and field trial results," *IEEE Commun. Mag.*, vol. 40, no. 9, pp. 143–149, Sep. 2002, doi: 10.1109/MCOM.2002.1031841.

[99] R. Peng and M. L. Sichitiu, "Angle of arrival localization for wireless sensor networks," in *Proc. Annu. IEEE Commun. Soc. Sensor Ad Hoc Commun. Netw.*, Reston, VA, USA, 2006, pp. 374–382, doi: 10.1109/SAHCN.2006.288442.

[100] H. Abeida, Q. Zhang, J. Li, and N. Merabtine, "Iterative sparse asymptotic minimum variance based approaches for array processing," *IEEE Trans. Signal Process.*, vol. 61, no. 4, pp. 933–944, Feb. 2013, doi: 10.1109/TSP.2012.2231676.