IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 26, 2021, accepted October 10, 2021, date of publication October 13, 2021, date of current version October 21, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3119775

Next Generation Auto-Identification and Traceability Technologies for Industry 5.0: A Methodology and Practical Use Case for the Shipbuilding Industry

PAULA FRAGA-LAMAS[1], (Senior Member, IEEE), JOSÉ VARELA-BARBEITO[2], AND TIAGO M. FERNÁNDEZ-CARAMÉS[1], (Senior Member, IEEE)

[1]Centro de Investigación CITIC, Department of Computer Engineering, Universidade da Coruña, 15071 A Coruña, Spain
[2]Navantia S. A., 15403 Ferrol, Spain

Corresponding authors: Tiago M. Fernández-Caramés (tiago.fernandez@udc.es) and Paula Fraga-Lamas (paula.fraga@udc.es)

This work was supported in part by the Auto-Identification for Intelligent Products Research Line of the Navantia-Universidade da Coruña Joint Research Unit under Grant IN853B-2018/02, and in part by the Centro de Investigación de Galicia "CITIC," funded by Xunta de Galicia and the European Union (European Regional Development Fund-Galicia 2014–2020 Program) under Grant ED431G 2019/01.

ABSTRACT Industry 5.0 follows the steps of the Industry 4.0 paradigm and seeks for revolutionizing the way industries operate. In fact, Industry 5.0 focuses on research and innovation to support industrial production sustainability and place the well-being of industrial workers at the center of the production process. Thus, Industry 5.0 relies on three pillars: it is human-centric, it encourages sustainability and it is aimed at developing resilience against disruptions. Such core aspects cannot be fully achieved without a transparent end-to-end human-centered traceability throughout the value chain. As a consequence, Auto-Identification (Auto-ID) technologies play a key role, since they are able to provide automated item recognition, positioning and tracking without human intervention or in cooperation with industrial operators. Although the most popular Auto-ID technologies provide a certain degree of security and productivity, there are still open challenges for future Industry 5.0 factories. This article analyzes and evaluates the Auto-ID landscape and delivers a holistic perspective and understanding of the most popular and the latest technologies, looking for solutions that cope with harsh, diverse and complex industrial scenarios. In addition, it describes a methodology for selecting Auto-ID technologies for Industry 5.0 factories. Such a methodology is applied to a specific use case of the shipbuilding industry that requires identifying the main components of a ship during its construction and repair. To validate the outcomes of the methodology, a practical evaluation of passive and active UHF RFID tags was performed in an Offshore Patrol Vessel (OPV) under construction, showing that a careful selection and evaluation of the tags enables product identification and tracking even in areas with a very high density of metallic objects. As a result, this article serves as a useful guide for industrial stakeholders, including future developers and managers that seek for deploying identification and traceability technologies in Industry 5.0 scenarios.

INDEX TERMS Auto-ID, traceability, Industry 5.0, Industry 4.0, shipbuilding, shipyard, UHF RFID.

I. INTRODUCTION

Industry 5.0 envisions the development of human-centered, resilient and sustainable smart manufacturing systems that are able to make use of real-time pervasive networks to support coordinated and complex processes [1]. As it is illustrated in Figure 1, such a paradigm relies on a number of enabling technologies related to Auto-Identification (Auto-ID), Industrial Cyber-Physical Systems (ICPSs) or to the Industrial Internet of Things (IIoT), which are key for the digital transformation of manufacturing industries [2]–[5].

The associate editor coordinating the review of this manuscript and approving it for publication was Prakasam Periasamy.

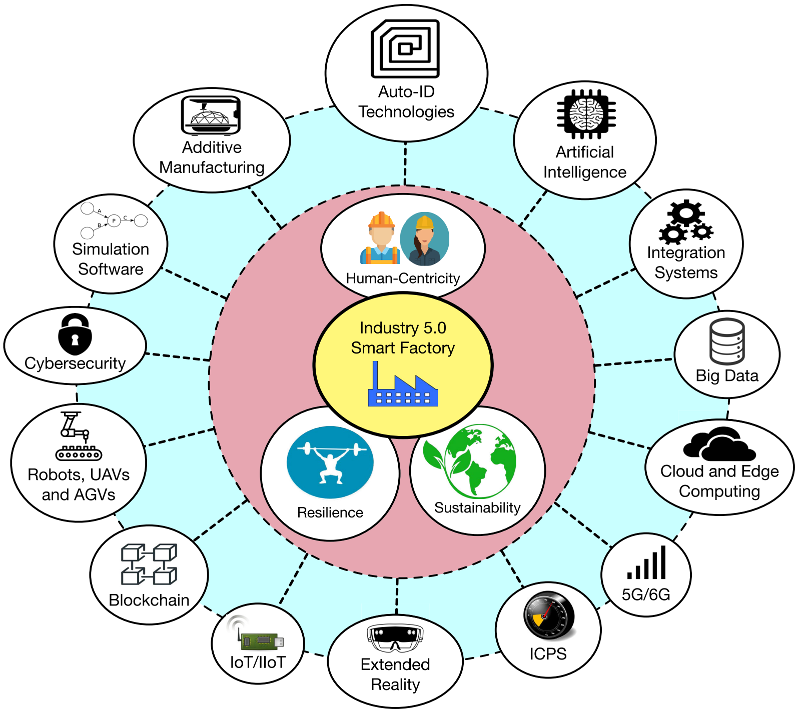


FIGURE 1. Key enabling technologies for Industry 5.0.

Auto-ID systems allow, in an industrial context, for connecting the physical world (e.g., products, tools, robots, factory facilities or Unmanned Aerial Vehicles (UAVs) [6]) with the virtual world (e.g., digital twins with simulation and Artificial Intelligence (AI) models and advanced analytics that automate operations). ICPSs are also a useful tool, since they enable the seamless integration of physical environments with embedded computing systems deployed over communications infrastructure [7]. The data collected by an ICPS can automatically be fed and linked to workshop machinery or robots (e.g., Computer Numerical Control (CNC) solutions or cutting and bending machines) so as to enable fully integrated ICPSs. Moreover, ICPSs usually rely on IIoT architectures that ease big data collection and processing, enable sensing and actuation capabilities, and provide a basic platform for interconnecting different ICPSs. At the same time, IIoT architectures require using Auto-ID technologies to provide an infrastructure with the ability to identify unambiguously thousands of objects. Thus, Auto-ID technologies lay the groundwork for supply chain traceability by identifying physical objects through unique identifiers that can be linked to a location. Moreover, in industrial environments, auto-identification, localization, communications and computing technologies must link both worlds while coping with harsh and complex deployments with strict requirements.

Shipbuilding is an example of an industry that can be optimized through Industry 5.0 technologies, since there are a number of complex daily processes that can be improved during the construction and repair of large vessels [7]. In fact, Industry 5.0 fits perfectly into shipbuilding needs, because:

- It requires a significant amount of human labor and its workers safety and well-being are critical.
- The involved processes demand the use of multiple materials, so supply chain disruptions have a significant impact on the productivity of a shipyard.
- It needs to make use of a huge amount of certain materials (e.g., steel), which can be processed and reused in a sustainable way.

To achieve such Industry 5.0 benefits, shipbuilding companies would need to make use of Industry 4.0 technologies, like the Spanish company Navantia did in the last years through a Joint Research Unit (JRU) called 'The Shipyard of the Future'. The JRU was established in collaboration with the University of A Coruña (UDC) and is devoted to study the applicability of different technologies to shipyards and ships. Among the research lines of the Shipyard of the Future project, the authors of this article have worked in the one called 'Auto-ID for Intelligent Products', which studies how to perform the automatic identification and traceability of different shipbuilding components, tools or products, throughout their lifetime. As a result, the researchers detected in the last years an increase in the number of available Auto-ID technologies that can be useful in Industry 5.0 scenarios, so the current landscape must be evaluated to have a holistic perspective and understanding to choose the best technologies. Thus, this article analyzes the most recent Auto-ID technologies for supply chain traceability and describes a methodology for deploying Industry 5.0 Auto-ID solutions. Such a methodology is based on the definition of use cases and, to validate it, a practical evaluation of a traceability system for an Offshore Patrol Vessel (OPV) is performed.

Specifically, this article includes the following main contributions, which, as of writing, have not been found together in the literature:

- It provides an extensive comparison on the latest and most popular Auto-ID technologies for Industry 5.0 applications.
- A specific use case is analyzed thoroughly: the deployment of an Auto-ID system for identifying and tracking items in a ship under construction. For such a use case, the performance of UHF RFID is evaluated in real environments when using different tags. It was not found in the literature any practical evaluation in a similar scenario and, in fact, to the knowledge of the authors, this is the first article that performs the mentioned analysis in a warship under construction.

The rest of this article is structured as follows. Section II reviews the related work on Industry 5.0 and on the use of Auto-ID and traceability technologies for factories and for the shipbuilding industry. Section III characterizes the proposed methodology, while Section IV describes the analyzed use case. Section V details the design of the system, including the communications architecture, and provides a thorough review on the currently available Auto-ID technologies. Section VI describes the implemented Auto-ID solutions and Section VII illustrates their validation through multiple tests performed in a ship under construction. Finally, Section VIII is devoted to the conclusions.

II. RELATED WORK

A. INDUSTRY 5.0: MAIN CHARACTERISTICS AND CHALLENGES

Industry 5.0 is a concept essentially put forward to push the European industry to make it future-proof, resilient, sustainable and human-centered [1]. Thus, Industry 5.0 goes beyond the Industry 4.0 paradigm and tries to reach societal goals in conjunction with jobs and growth. In this way, Industry 5.0 pursues prosperity in a sustainable manner, looking to increase productivity without removing human workers from the manufacturing industry.

It must be emphasized that Industry 5.0 should not be interpreted as a chronological continuation or as an alternative to the Industry 4.0 paradigm [1]. Instead, the concept can be regarded as a fusion of current European industrial and societal trends, so Industry 5.0 complements the key features of Industry 4.0. In fact, Industry 4.0, since its conception in 2011 [8], has been essentially focused on factory digitalization, production flexibility and efficiency optimization rather than on societal issues like social fairness or environmental impact. Therefore, Industry 5.0 refocuses Industry 4.0 principles and orients industrial research and innovation towards a human-centered and environmentally conscious future. Such goals are in part similar to the ones defined by Society 5.0, a concept presented by the Japanese government in 2015 [9], which tries to balance economic development with societal and environmental problems [1].

The European Commission has identified six Industry 5.0 categories that are considered key due to being part of future technological frameworks [10]:

- Individualized human-machine interaction.
- Bio-inspired technologies and smart materials.
- Digital twins and simulation.
- Data transmission, storage and analysis technologies.
- Artificial Intelligence.
- Technologies for energy efficiency, renewables, storage and autonomy.

Auto-ID technologies can be considered as part of individualized human-machine interactions (as tracking technologies), but they can also be used by digital twins (as part of cyber-physical systems) or as data transmission/storage technologies (in relation to traceability systems).

B. AUTO-ID AND TRACEABILITY TECHNOLOGIES FOR INDUSTRY 5.0 FACTORIES

Although certain Industry 5.0 technologies for auto-identification and traceability have been previously analyzed in the literature [11], [12], the large-scale and complex nature of industrial networks still present several challenges ranging from security to performance issues, especially in relation to communications protocols [13]. One of the most relevant challenges is the reliability of communications according to the requirements of the different applications (e.g., latency or packet loss rate). For instance, although there is a number of previous reviews on the evaluation of wireless technologies for mission-critical scenarios [14], there is a lack of in-depth research on the use of wireless technologies for practical industrial scenarios [15]–[20].

Among the different wireless communications technologies to identify, locate and trace items, Radio Frequency IDentification (RFID) is currently the most popular, since it has been already carefully evaluated and deployed successfully in multiple industrial scenarios [21]–[23]. Nonetheless, there is a number of less mature technologies that should be explored. This was the objective of the authors of [24], who reviewed the use of recent wireless technologies for Industry 4.0, but they only considered the ones with a range over a hundred meters. Other authors focused on specific technologies like ZigBee, WirelessHART, ISA100.11a or Wireless Network for Industrial Automation - Process Automation (WIA-PA) [25], or on Low-Power Wide-Area Network (LPWAN) solutions [26].

Regarding the application of Industry 4.0/5.0 technologies to the shipbuilding industry, it must be first noted that information about such an industry is not easily accessible, mainly due to confidentiality and competitive advantage reasons. Moreover, there are not many articles in the literature that apply Auto-ID and traceability technologies to shipbuilding. Furthermore, most of the available documentation is outdated or presents the proposed systems without giving a lot of detail.

Considering the previous clarifications, it can be highlighted the work from several authors that have studied the application of Industry 4.0 technologies to common shipbuilding tasks, like hull blasting [27], hull maintenance [28] or welding [29]–[32]. One of the few papers that describes an Auto-ID system for the shipbuilding industry is [33], where the authors make use of a Bluetooth-based positioning system to locate workers in a shipyard with roughly one meter of accuracy inside a workshop. A similar system is proposed in [34].

Other authors make use of wireless communications technologies that have not been explicitly developed for Auto-ID, but which can be used for such a purpose. For example, in [35] the authors target workforce safety in relation to the exposition to several potential hazards (e.g., toxic gases generated in confined spaces during welding), which can be critical in the case of very dynamic shipbuilding environments like ships under construction, where it is complicated to deploy fixed and wired infrastructure to monitor and detect dangerous situations (e.g., gas leaks). For such scenarios, Perez *et al.* [35] proposed a wireless multi-hop remote gas monitoring system based on Zigbee that connects gas detectors to control stations outside vessels. The network is auto-configured dynamically in case of network failure or redeployment, so sensor nodes communicate and are identified by using ZigBee.

Another example of a shipyard safety management system based on an Auto-ID technology is presented in [36]. Such a system makes use of RFID to provide a risk-free backward operation of forklift trucks with a sensor-based monitoring service to ensure driver safety during pipe transportation. More recent research is described in [37] and [38]. In [37] Jung *et al.* describe a Health, Safety and Environment (HSE) system for shipyards and onshore plants that uses LoRaWAN for identification and to improve packet reception rate in underground and confined spaces. In the case of [38], the authors use ultrasounds to increase workforce information updates from twice per day to twenty times per minute. However, the authors point out that further research is needed in emergency evacuation, hazard and explosion warnings, or in logistics optimization.

It is also possible to fuse the use of Auto-ID with other disruptive Industry 5.0 technologies. For instance, Extended Reality (ER) solutions have been introduced in the last years to enhance human-machine interaction in manufacturing processes carried out in shipyards. Specifically, Industrial Augmented Reality (IAR) can assist operators when visualizing the location of items [39], while virtual reality can be used jointly with sensor networks and RFID to track shipyard assembly processes and supplies [40].

Finally, it is important to emphasize that, in Industry 5.0 environments, metal has a strong impact on wireless communications [21]. For such a reason, the authors of [41] evaluated the performance of passive RFID tags on helical and toroidal metal pipes. In addition, the literature provides a number of identification tags and components that have been specifically designed to enable communications in such harsh environments (e.g., UHF RFID tags for containers [42]–[44]).

C. PREVIOUS WORK OF THE AUTHORS

For the sake of fairness and to emphasize the novelty of the work presented in this article, it is worth noting that during the last six years the authors of this article have tested a number of different Auto-ID and traceability technologies in shipbuilding scenarios. Therefore, this article departs from the authors' background knowledge on the design and implementation of advanced Auto-ID and traceability solutions for shipyards and ships.

First, it must be mentioned that one of the previous articles describes thoroughly the shipyard environment in relation to the main factors that impact wireless communications [7]. In addition, such an article presents accurate indoor positioning results in a pipe workshop using Multiple-Input Multiple-Output (MIMO) algorithms and Kalman filtering to stabilize the Received Signal Strength (RSS). A follow-up to such a work is provided in [45], where an Industrial Cyber-Physical System (ICPS) is devised for enabling automatic event detection in a shipyard workshop through an active RFID system that made use of fingerprinting and different RSS stabilization techniques. In addition, in [46] it is described an ICPS that uses edge computing devices that are integrated and tested together with Siemens Manufacturing Execution System (MES) (Simatic IT). The performed experiments showed that fog computing gateways, under regular loads and in the selected scenario, reacted up to 481 times faster than a cloud. A more recent work is [47], which validates the use of a Bluetooth 5 fog computing based ICPS architecture for a pipe workshop.

Moreover, the authors of this article studied the interaction with other Industry 4.0/5.0 technologies. For instance, in [48] an IAR communications architecture for a shipyard is presented and evaluated with payload sizes according to demanding Microsoft HoloLens applications [49] and when using a cloud, a cloudlet and a fog computing system. Packet communications delay and transmission latency requirements are carefully analyzed. A follow-up work is presented in [50], where an IAR application embeds a novel collaborative protocol that allows operators to interact among them and with virtual objects in a synchronized way.

Finally, with respect to workforce safety, the authors detail in [51] the design and evaluation of a near real-time decentralized monitoring system. Data are collected by Internet of Things (IoT) wearables that measure both personal and environmental data. Specifically, each shipyard operator wearable sends the collected data to the nearest LoRaWAN gateway, which transmits them to a number of nodes where information is stored in a distributed manner. Additionally, the system stores and processes the collected data through smart contracts in a blockchain, which ensures the immutability of data that can be shared with the involved stakeholders (e.g., insurance companies, supervisors or medical services).

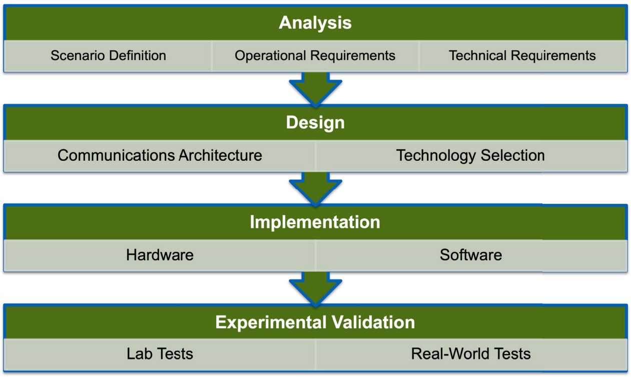


FIGURE 2. **Proposed development methodology.**

III. AUTO-ID SYSTEM DEVELOPMENT METHODOLOGY

Figure 2 illustrates the proposed development methodology, which is based on four stages that allow for analyzing, designing, implementing and validating Auto-ID solutions for Industry 5.0 scenarios. Specifically, the following are the main steps of the methodology when applied to shipbuilding:

1) Analysis. The selected use case is first described in a general manner, emphasizing its main goals. Then, the specific operational and technical requirements are detailed and analyzed together with the application scenarios.
2) Design. The communications architecture is proposed. The main hardware and software components of the Auto-ID system are determined and the most appropriate technologies are selected. Thus, it is first required to carry out a detailed analysis of the available Auto-ID technologies and then select the most convenient technologies that in the middle and long term will be able to cope with the requirements determined during the analysis stage.
3) Implementation. The designed Auto-ID system is implemented by using the selected hardware and software.
4) Experimental validation. The developed system is first tested in the lab and then in real-world scenarios so as to determine whether it fulfills the requirements established in the analysis stage.

The next sections apply the previously described methodology to a specific use case: the development of an Auto-ID system for identifying and keeping traceability of the components of a ship under construction.

IV. STAGE 1: USE CASE ANALYSIS

A. SCENARIO DEFINITION

The selected use case goal is to provide identification and to keep traceability of the most relevant components of a ship under construction. The ship was chosen because it represents one of the most challenging scenarios in a shipyard when deploying an Auto-ID system. It is a very dynamic environment (e.g., there are numerous metallic objects and structures, some of which are continuously being moved by operators, causing multiple and varying reflections). In addition, there are multiple confined spaces where it is complicated to deploy a communications infrastructure [52]. Specifically, a Navantia's Offshore Patrol Vessel (OPV) was selected as a reference scenario for the Auto-ID system: it is a modern military ship with advanced technology that operates as a Command and Control vessel, it is 90 m long, which is a moderate size, and has a life span of typically 30 years. The shipbuilder is responsible for providing lifecycle support for a period of five years with a five-year extension option.

Note that such a scenario can be considered an Industry 5.0 application scenario, since item identification and traceability can help to improve sustainability, to develop human-centric solutions or to enhance the resilience of the production chain.

Navantia has a Production Unit in the estuary of Ferrol (Galicia, Spain), where there is a shipyard for the construction and repair of ships like patrol vessels, frigates and other warships. As it was previously mentioned, this unit, and all the company, is involved in a major transformation to leverage the Industry 5.0 paradigm and thus upgrade its shipyards with the latest technological innovations. The aim of this transformation is to enhance the level of efficiency and competitiveness and, consequently, to ensure future sustainability. Such a transformation requires increasing the number of fully automated and robotized processes with connected machines and ICPSs. This enhanced intelligence will come from the supply chain, with the end result being ships that will maintain a high level of intelligence throughout their operating lives. Moreover, this intelligence, which will be found in the different facilities, equipment, materials and products of the shipyard and the ship, will also be extended beyond the shipyard, backed by a network that integrates the different stakeholders (e.g., suppliers, partners and customers) in a horizontal and vertical way. Thus, all processes will be supported by information and communications technologies that will manage design, manufacturing, maintenance and logistics in an integrated manner by using 3D design, process simulation tools and other Industry 5.0 technologies.

Inside Navantia's shipyard, the most relevant locations for traceability purposes are warehouses, workshops and ships under construction or repair. The construction of a ship is relatively straightforward: each ship is first divided at a design level into blocks, which are then manufactured into the different workshops of the shipyard and finally assembled in a slipway (a specific area that allows for sliding ships down to the sea). As an example, Figure 3 shows a picture of an already built ship block.

A ship repair involves working in a complex scenario and is composed by several phases. The first one is the stowage of the construction materials, which are stacked in a near-by dock, waiting for a crane to load them onto the ship to be repaired through any of the caesarean sections created for such a process. The stowage is carried out on demand.

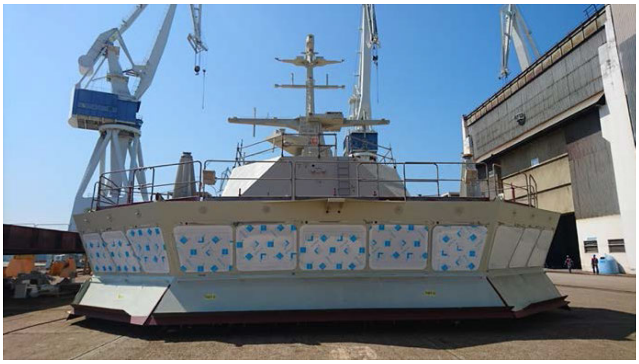


FIGURE 3. Example of a ship block.

The repair materials stacked on the dock may be labeled individually or stacked on pallets.

Once inside the ship, materials are placed near the location where they will be finally installed. There is no clear criterion on where to place the materials since the distance to the mounting point may vary for practical reasons (e.g., in order to avoid hindering the work of other operators). In the case of pipes, which exist in a huge number and are one of the key pieces of a ship, they have different characteristics that potentially influence their identification and location. Depending on such a location, pipes can be found exposed on the ceiling, either mounted (as it is shown in Figure 4), unconnected/connected and/or surrounded by multiple obstacles, which are made of metallic or plastic materials.

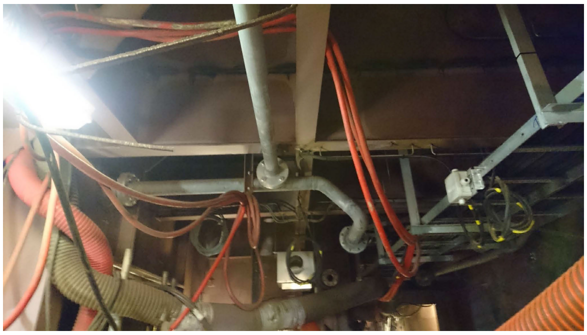


FIGURE 4. Mounted pipes on the ship ceiling.

The density of pipes varies significantly among the different types of ships. The difficulty of locating pipes depends on such a density, which is not particularly high except in specific areas. The most critical case of pipe density and metallic insulation occurs in the different spaces of the ship in which pipes go under the raised floor, which is also metallic (an example of open floor is shown in Figure 5). During ship assembly and repairs such an underfloor insulation is complemented with metal walkways that are added to ease the work of the operators.

In addition, it should be noted that most of the spaces are covered with a thermal and sound insulator. Such an insulator is located both on the ceiling above the pipes and surrounding the pipes, having a minimum thickness of about 50-60 mm.

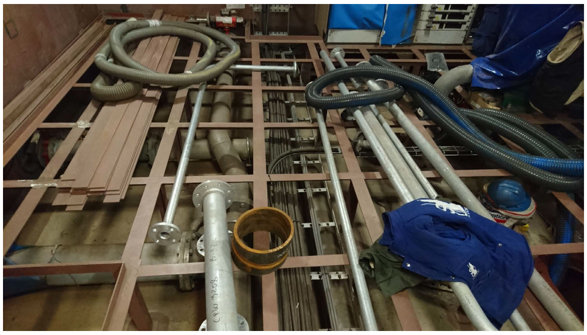


FIGURE 5. Pipes under metal floor.

In the same way, it must be considered the insulation produced by the doors, which are made of metal or of plywood and a metallic frame.

B. OPERATIONAL AND TECHNICAL REQUIREMENTS

Table 1 enumerates the main operational and technical requirements related to the selected use case.

Such requirements are grouped by capabilities: deployment features, mobility capabilities, security capabilities, network topologies, coverage capabilities, robustness capabilities, Services and Quality of Service (QoS) capabilities, interoperability capabilities, target platforms and proof of Return of Investment (ROI), which take into account the three main foundations of Industry 5.0: human-centricity, resilience and sustainability.

V. STAGE 2: DESIGN

A. COMMUNICATIONS ARCHITECTURE

Figure 6 shows the proposed communications architecture for the selected use case. Such an architecture can be divided into three main layers (the two lower layers are deployed inside the OPV, while the layer at the top is outside, in Navantia's internal cloud facilities):

- The bottom layer consists of the components of the Auto-ID system: the Auto-ID readers and the tracked industrial items. Each Auto-ID reader embeds four subsystems:
  - The Auto-ID subsystem makes use of tags that are attached to objects like industrial tools, accessories or products. Note that the tags can also be carried by operators to locate and to identify them, or to monitor different environmental parameters for hazard prevention [51].
  - The visual identification subsystem essentially makes use of a digital camera or of a barcode reader to read data from different types of barcodes (e.g., traditional 2D barcodes, QR codes).
  - The local storage is where the collected data and the relevant Auto-ID information are stored. This is key in environments like the OPV, where there are places with no communications coverage, but where operators need to access certain data about the tracked items.

TABLE 1. Capabilities and design goals of the development of an Auto-ID system for ship construction and repair.

Capability	Description of the main design goals/operational requirements
Deployment features	The Auto-ID system is part of a more complex ICPS with an IIoT architecture. An example of such an architecture will be further detailed in Section V-A. The deployment characteristics depend on the existences of confined spaces in the ship. The Auto-ID system operates both in cooperation with industrial operators or without human intervention. In the latter case, the system must be as automatic and autonomous as possible, ideally requiring no human intervention in the identification, data collection, processing and information exchange. Mechanisms to automate and ease machine-to-machine communications (e.g., smart contracts) must be added. Customized functionality (e.g., enable dynamic and automatic updates on the information [53], location and context awareness services for operators) should be considered. Since there is a number of obstacles inside a ship, Non-Line-of-Sight (NLoS) between the reader and the tags must be supported. Cost-effective deployment, plug-and-play capabilities [54] and easy maintenance are required. It is expected a progressive growth in the number of monitored items/products, therefore scalability should be guaranteed. Only technologies prepared to tolerate a significant presence of metal should be considered. In some specific scenarios within the ship, the selected tags should be ruggedized to support exposure to liquids, salinity, fuel, chemicals or other corrosive substances. In the shipyard, humidity levels are relatively high.
Mobility capabilities	Certain degree of mobility is necessary. For example, operators may make use of wearables or mobiles readers, while robots should be able to move quickly or to reach a relatively high speed.
Security capabilities	Resource-constrained IIoT devices may not be able to execute the necessary cryptographic algorithms for securing them [55], [56]. Additional security mechanisms should be considered.
Network topologies	The network architecture of the Auto-ID system should primarily address Point-To-Multipoint (PMP) or Point-to-Point (P2P) links. However, for mobile platforms, mesh communications should be considered.
Coverage capabilities	It should be distinguished between situations when a maximum distance of one hop is necessary and scenarios where the distance to be covered requires making use of intermediate relays.
Robustness capabilities	The Auto-ID system should provide robustness to signal interference and loss of network operation. The presence of metal inside a ship creates signal reflections, blockage and electromagnetic interference in RF communications [57] that can be caused by weapons, machinery or other ship's navigation, tactical or surveillance systems that operate at the same of similar frequencies, that degrade system performance and affect system reliability [21], [58]. For mesh and PMP modes, the network should provide redundancy and be robust to avoid single points of failure (e.g., the failure of one or a few nodes must not compromise the operation of the network as a whole). When deployed in locations where multiple technologies operate simultaneously, the Auto-ID system should consider measures to avoid electromagnetic interference from adjacent users in the same frequency band. Fault tolerance and enhanced resilience to cyber-attacks should be included in the computing architecture by design.
Services and QoS capabilities	The Auto-ID system should ensure a timely and successful delivery of different classes of services/applications. Such classes may range from critical applications with strict QoS requirements (e.g., with near real-time responses) to monitoring applications with more flexible QoS requirements. Examples of the main services are [17], [59]: • Safety critical systems that require immediate response on events, with a latency in the order of tens or hundreds of μs or a few milliseconds. • Control systems: – Closed-loop: systems controlled via feedback loops that operate either periodically or based on events. They may or may not have stricter latency requirements than safety systems. – Open-loop systems: non-feedback systems where the action is completely based on the input. • Alert systems that send periodical or event-based notifications. • Data collection systems that gather information and forward it to a server (e.g., logs).
Interoperability capabilities	Fully compliant with standards and legacy systems. Support for cross-industry collaboration with different stakeholders (e.g., suppliers, insurance, government).
Target platforms	A wide range of items and people can be tagged (e.g., pipes, tools, workers). The previously mentioned deployment and robustness features should be supported by the target platform.
Proof of Return on Investment (ROI)	The ROI generated by the Auto-ID system should be measured with metrics (i.e., KPIs) related to the increased productivity, workforce safety and sustainability.

  - The communications subsystem allows the Auto-ID reader to exchange information with the upper layers.
- The middle layer is the fog layer. Fog, mist and edge computing solutions enable cyber-resilience in aspects like no single-point-of-failure and geographically redundant distributed platforms, and decentralized processing [46], [55]. These computing architectures imply that resource-constrained IoT end-devices have storage, local processing capabilities and even high-security mechanisms [60] that allow for moving computational resources to the edge of the network to provide low-latency responses [61]. As it can be seen in Figure 6, the proposed fog layer is composed by local and remote fog gateways. Every fog gateway is essentially a Single-Board Computer (SBC) (e.g., Raspberry Pi, Beagle Bone, Odroid-C4 or Orange Pi PC) that provides fog services. Such services process the requests from the Auto-ID readers and provide fast or even real-time responses without requiring forwarding them to the upper layer, which is outside the OPV. Shipyard operators can use mobile devices like tablets, smart phones or Industrial Augmented Reality (IAR) glasses [62] through a wireless router to connect wirelessly to fog gateways to receive information about the Auto-ID system without needing an Auto-ID

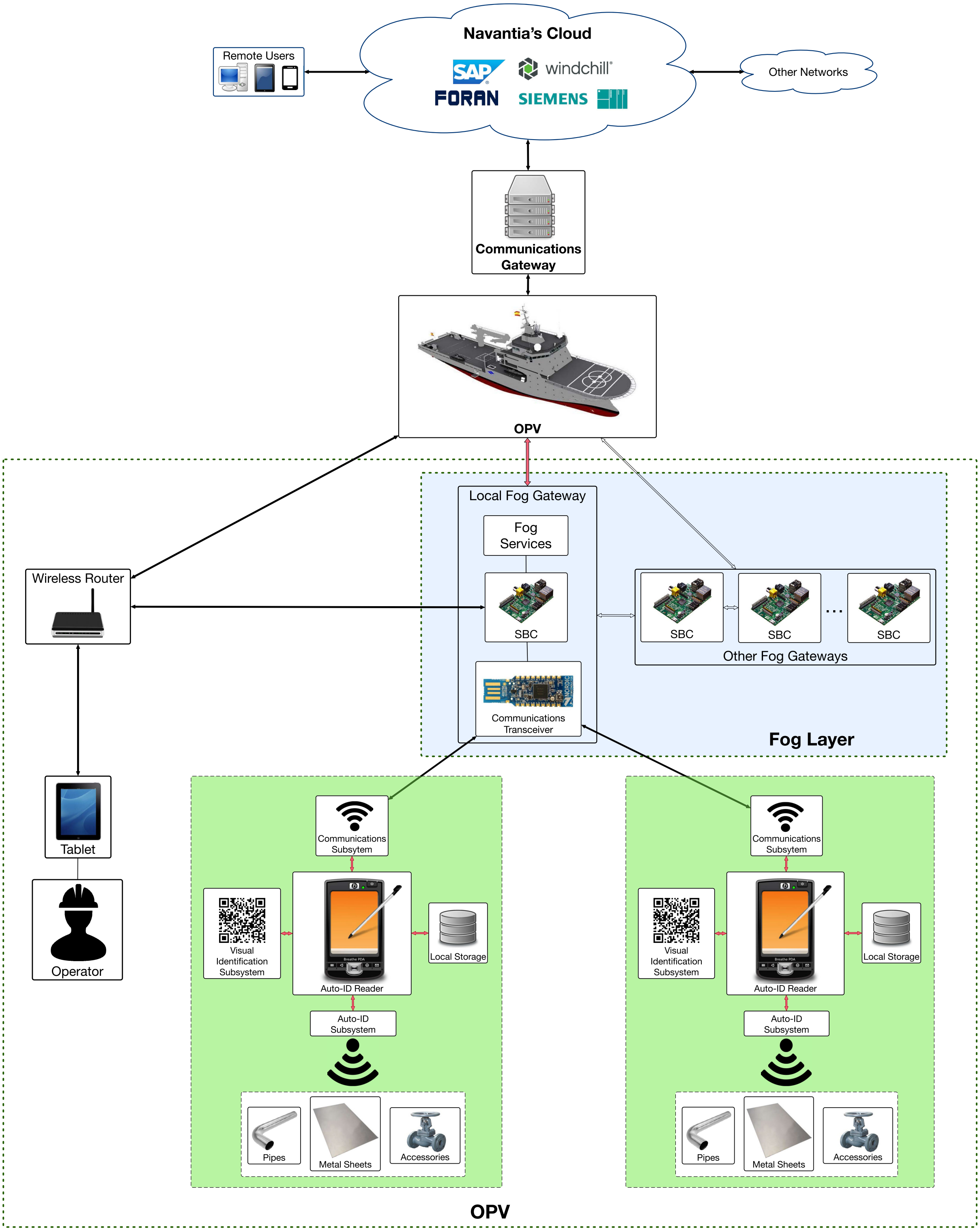


FIGURE 6. Proposed communications architecture.

reader. With respect to the deployment, in order to provide local ad-hoc services, fog gateways should be physically scattered close to the working areas. Nonetheless, the proposed communications architecture allows physically distributed fog gateways to communicate with each other in order to collaborate when providing services.

- The top layer is the cloud, which provides remote computational services. Fog gateways can communicate with the cloud, which is where the most compute-intensive tasks are executed. In addition, the cloud servers provide access to remote users and other industrial networks to the data collected by the Auto-ID system. In the case of Navantia, such tasks are essentially performed by either proprietary developments or third-party software, so the architecture should be fully integrated and interoperable with other products and services of the shipbuilding company (e.g., digital twin, Manufacturing Execution System (MES), Enterprise Resource Planning (ERP) or Product Lifecycle Management (PLM) software).

B. POTENTIAL AUTO-ID TECHNOLOGIES

Among the different technologies required to deploy the communications architecture described in the previous section, this article focuses mainly on the ones able to implement the Auto-ID, communications and visual identification subsystems. The most relevant Auto-ID and communications that can be used for providing identification capabilities in Industry 5.0 applications are enumerated in Tables 2 and 3. Such technologies are compared in the Tables in terms of their standardization body, operating frequency, maximum range, maximum data rate, modulation scheme, encryption, topology, latency, battery lifetime, cost, key advantages and limitations and main applications.

The presented comparison is carried out according to their current capabilities, but note that some technologies (and even specific features) evolve at a very fast pace. For example, while Tables 2 and 3 include Wi-Fi 6, some authors have already anticipated the novel features of Wi-Fi 7 (IEEE 802.11 be) [63] or Wi-Fi sensing (IEEE 802.11 bf [64]).

The following subsections analyze the most relevant factors that impact the selection and deployment of an Auto-ID system inside an OPV.

1) WIRED VERSUS WIRELESS COMMUNICATIONS

An OPV is a very aggressive environment that may present flammable gases, chemicals and/or exposure to humidity and high temperatures. Such conditions may severely affect a wired deployment. In addition, there are a number of areas that are hard to reach. As a result, the deployment and maintenance of wired technologies can become expensive and time-consuming. For such a reason, the vast majority of the technologies in Tables 2 and 3 are wireless, but it should be noted that wireless technologies present other challenges that will be identified in the next subsections.

2) BUSINESS MODEL

The technologies that rely on a subscription are not ideal for many industrial scenarios due to their fees and due to the dependence on the mobile carrier, who is the responsible in case of failures or maintenance. One example of such type of technology is SigFox, which is a network-operated technology that includes a subscription service fee that allows up to 140 messages (12 Bytes per message) per device per day, and a transmission rate of 100 bits/s when operating at 868 MHz.

In addition, it is important to consider the advantages of making use of open-standard non-vendor specific technologies instead of proprietary ones. For instance, NB-Fi is a proprietary technology approved by National Standard by the Russian Federal Agency on Technical Regulation and Metrology in February 2019. NB-Fi relies on different manufacturers: ST Microelectronics for the STM32 microcontroller, WAVIoT for the NB-Fi transceiver and ON Semiconductor for the AX5043 transceiver.

3) COMPUTER NETWORK TYPE

Tables 2 and 3 consider two types of wireless technologies that fit into the proposed Auto-ID scenario: short-range wireless and LPWAN technologies. Although there is not a unique definition for short-range wireless communications, it generally refers to Wireless Personal Area Network (WPAN) and Wireless Local Area Network (WLAN) technologies. Examples of these technologies are Thread, WirelessHART, Z-Wave, DASH7, ANT+ or Ultra-Wide Band (UWB).

Recently, LPWANs [65], [66] are gaining relevance due to their long range, low power capabilities and great scalability. Other aspects like security are currently being analyzed [67]. Examples of LPWAN technologies are LoRa/LoRaWAN, NB-IoT or SigFox.

For the proposed use case within the Navantia's OPV, short range wireless technologies are sufficient for identification, but LPWAN technologies must be considered in other cases when it is necessary to take the signal out from some areas inside the OPV (e.g., confined spaces) to the remote locations in the shipyard.

4) BANDWIDTH

In general, a higher bandwidth implies wider channels, higher data rates but worse penetration capabilities that may reduce the range considerably in industrial scenarios. On the contrary, sub-GHz technologies use narrow channels (e.g., a few hundred KHz) that have lower data rates but better signal penetration capabilities.

5) STANDARDIZATION BODY

Ideally, the used technologies should have been standardized to guarantee compatibility and a wide range of manufacturers. Thus, most of the wireless technologies analyzed in Tables 2 and 3 are regulated by standard organizations (e.g., ISO/IEEE, IEC, 3rd Generation Partnership Project (3GPP), ITU Telecommunication Standardization Sector (ITU-T), European Telecommunication Standards Institute (ETSI), Internet Engineering Task Force (IETF)) and different alliances that perform certification testing to make sure that wireless networking equipment complies with the standards (e.g., Wi-Fi Alliance, Enocean Alliance, LoRa Alliance, MIOTY Alliance).

TABLE 2. Most relevant characteristics of the latest Auto-ID and communications technologies for Industry 5.0.

Technology	Standardization Body	Operating Frequency	Maximum Range	Max. Data Rate	Modulation Scheme	Encryption	Topology	Latency	Battery Lifetime
Barcode/QR [68]–[70]	Different (e.g., ISO 15415, ISO 15416, ISO/IEC 18004:2015 [71])	-	Depends on code size, but usually less than 1 m	–	–	Information can be encrypted	Point to point	–	No batteries required when printed on paper
NFC [72]	ISO/IEC 14443, ISO/IEC 18092, ISO/IEC ECMA-340, ISO/IEC ECMA-352	13.56 MHz	<20 cm	424 kbit/s	ASK, FSK, OOK, BPSK	AES	Point to Point, Point to Multipoint	–	No batteries are required for most tags
LF RFID [73]	ISO/IEC 11785, ISO/IEC 14223, ISO 21007 (LF), ISO 18185-5 A/B, ISO/IEC 18000: Part 2, ASTM, EPCglobal [74]	30–300 KHz (125 KHz)	<10 cm	<640 kbit/s	ASK, FSK, OOK	May implement security mechanisms	Point to point, Point to Multipoint	–	Tags require no batteries
HF RFID [75]	ISO/IEC 15693, ISO/IEC 14443 A/B, ISO 21007 (HF), ISO/IEC 18000: Part 3, ASTM, EPCglobal [76]	3–30 MHz (13.56 MHz)	<10 m	<640 kbit/s	DBPSK, PJM, BPSK, ASK, FSK, OOK	May implement security mechanisms	Point to point, Point to Multipoint	–	Tags require no batteries
UHF RFID [77]	ISO 18185-5, ISO/IEC 18000-6, ISO 18000-6C (EPC Class 1 Gen 2), ISO 10374, ISO/IEC 18000: Part 7, ASTM , EPCglobal [78]	30 MHz–3 GHz	<120 m	<640 kbit/s	FSK, ASK, DSB/SSB/PR-ASK, PSK, BPSK, GMSK, DBPSK, OOK	May implement security mechanisms	Point to point, Point to Multipoint	–	From days to years
Infrared (IrDA) [79]	IEEE/ISO 11073 [80], Infrared Data Association (IrDA)	300 GHz to 430 THz	Up to a few meters	2.4 kbit/s – 1 Gbit/s (FIR, 4 Mbit/s)	Pulse (FIR, 4PPM)	No link-level security	Point to point	–	Years
Ultrasounds [81], [82]	–	>20 to 40 KHz	Up to a few meters (typically up to 10 m)	250 kbit/s	Different (e.g., ASK, FSK, PSK)	–	Point to point, Point to multipoint	–	Years
RuBee [83]	IEEE 1902.1 [84]	30–900 kHz	Up to 30 m	Up to 8 kbit/s	ASK, BPSK	–	Point to point	–	Several years
UWB [85], [86]	IEEE 802.15.3 [87] , IEEE 802.15.4 [88], UWB Alliance [89]	3.1 to 10.6 GHz	< 100 m	>110 Mbit/s, up to 27 Mbit/,s for 802.15.4a	BPSK, QPSK	AES, authentication: CBC-MAC (CCM), data protection: 32-bit CRC, error control/reliability: ACK, CSMA/CA	Piconet, peer-to-peer	–	Hours to months
BLE (Bluetooth 4.2) [90], [91]	IEEE 802.15.1 (inactive)	2.4 GHz	>100 m	250 kbit/s, 1 Mbps	GFSK	E0 stream cipher AES-128, authentication: shared secret, data protection: 16-bit CRC	Point-to-point, piconet (scatternet), star, mesh	Around 3 ms (less than 10 ms)	Several years on a single coin-cell battery
WirelessHART [92], [93]	Proprietary, IEEE 802.15.4 physical layer, IEC 62591:2016 [94]	2.4 GHz	<10 m	250 kbit/s	OQPSK	AES-128	Star, mesh	–	Several years
ZigBee [95]	IEEE 802.15.4 (layer 1 and 2) [96], Connectivity Standards Alliance [97]	868-915 MHz, 2.4 GHz	30 m (indoor) and <100 m (outdoor) for 2.4 GHz, up to hundreds of meters outdoors for 868-915 MHz	20−250 kbit/s	BPSK (+ASK), OQPSK	AES-128, authentication: CBC-MAC (CCM), data protection: 16-bit CRC, error control/reliability: ACK, CSMA/CA	Star, cluster tree, mesh	Around 15 ms	Very low power consumption, 100-500μW, batteries last months to years
Z-Wave [98]	Z-Wave Alliance [99], proprietary	868-915 MHz	30 m (indoor), 100 m (outdoor)	40-200 kbit/s	FSK/GFSK	AES-128, data protection: 8-bit CRC, error control/reliability: ACK, CSMA/CA	Mesh	1 s	Alkaline batteries last months to years
ANT+ [100]	Proprietary (ANT+ Alliance)	2.4 GHz (1 MHz channel bandwidth)	30 m	20 kbit/s (burst), 60 kbit/s (advanced burst)	GFSK	AES-128 and 64-bit key	Point-to-point, star, tree, mesh	–	Around one year
Wi-Fi [101]–[104]	IEEE 802.11b/g/n/ac	2.4–5 GHz (22 MHz channel bandwidth)	<150 m	Up to 600 Mbit/s	QPSK	AES block cipher, authentication: WPA2 (802.11i) and WPA3, data protection: 32-bit CRC	BSS, ESS	Less than 20 ms	High power consumption, 500 mW - 1 W (batteries usually last hours)
Wi-Fi HaLow [105]–[107]	IEEE 802.11ah [108]	License-exempt bands around 900 MHz (20 to 160 MHz channel bandwidth)	<1 km	100 Kbit/s per channel, up to 347 Mbit/s	BSK to 256 QAM	WPA-3	Star-bus	100 ms (typical beacon interval)	Power consumption of 1 mW

TABLE 2. *(Continued.)* **Most relevant characteristics of the latest Auto-ID and communications technologies for Industry 5.0.**

Technology	Standardization Body	Operating Frequency	Maximum Range	Max. Data Rate	Modulation Scheme	Encryption	Topology	Latency	Battery Lifetime
Wi-Fi 6 [109]	IEEE 802.11ax [110]	Between 1 and 6 GHz (2.5 and 5 GHz), 20 to 160 MHz channel bandwidth, 10 Gbit/s	<3 km	Around 1,200 Mbit/s	BSK to 1024 QAM	WPA 3	BSS, ESS	Around 10 ms	–
Insteon [111]	Proprietary [112]	902-924 MHz	50 m (outdoor)	13,165 Kbit/s	FSK	AES-256, rolling codes, publick key, error/control/reliability: 8-bit checksums	Full mesh	–	Several years
EIB/KNX RF [113]	KNX Association [114], ISO/IEC 14543-3 [115]	868 MHz and 2.4 GHz	150 m	16.4 kbit/s	FSK	AES-CCM	Line, tree and star	–	Several years
EnOcean [116]	EnOcean Alliance [117], ISO/IEC 14543-3-1X, proprietary	868 MHz, 902 MHz and 928 MHz (280 KHz channel bandwidth)	30 m (indoors), 300 m (outdoors)	120 kbit/s	ASK	AES-CBC and AES-CTR	Mesh	40 ms (typical for transmitting three identical radio telegrams)	Very low consumption or battery-less thanks to using energy harvesting
Thread [118]	IEEE 802.15.4 [119], Thread Group [120], OpenThread (open-source implementation by Google [121])	2.4 GHz band, with a roadmap to sub-GHz bands	Up to 200 m	250 kbit/s	IEEE 802.15.4 modulations	AES-128. Commissioning uses standard DTLS with ECJ-PAKE	Mesh	–	Several years
SAW (Surface Acoustic Wave) [122]–[124]	-	Variable, it can be in the GHz range (VHF/UHF)	3-10 m	-	Pulse, phase or frequency based modulations (typically)	-	Point to point, point to multipoint	-	No batteries for passive tags
IQRF [125]	IQRF Alliance [126]	Sub-GHz ISM bands (433 MHz, 868 MHz, and 916 MHz)	Hundreds of meters, up to 1 km	100 kbit/s	GFSK	AES-128	Mesh	400 ms	5-10 years
Bluetooth 5 [127], [128]	Bluetooth Special Interest Group (SIG) [129]	2.4 GHz (2400-2483.5 MHz)	<400 m	Up to 2 Mbit/s	GFSK	AES-CCM	Star-bus, mesh	<3 ms	Power consumption 1-20 mW
DASH7 [130]	DASH7 Alliance [131], ISO/IEC 18000-7 [132]	315–915 MHz	<10 km	27.8 kbit/s	2-GFSK	AES, 16-bit CRC	Tree, simple routing two hops	1-2 s (typical)	Low power (batteries can last months to 10 years)
EC-GSM-IoT [130]	3GPP Release 13	900 MHz, 2.4 GHz (200 kHz channel bandwidth)	15 Km	350 bit/s to 70 kbit/s (GMSK), 240 kbit/s (8PSK)	GMSK/8-PSK, TDMA, FDMA, Half Duplex	Yes (described in 3GPP Release 13)	Star	10 s	Several years
RPMA (INGENU) [133]	INGENU [134]	2.4 GHz (1 MHz channel bandwidth)	15 km (urban), 80 km (rural)	624 kbit/s (DL)/ 156 kbit/s (UL), 30 Mbit/s	RPMA-DSSS (UL), CDMA (DL)	128-bit and 256-bit AES	Star, tree, > 500K nodes	10 s	10+ years
LoRa, LoRaWAN [135]	LoRa Alliance [136]	868 MHz, 915 Mhz, 2.4 GHz (channel bandwidth of 125 kHz)	Kilometers (2-5 km urban, 15 km suburban, <50 km rural)	50 kbit/s	Chirp-based modulation	128-bit AES	Star on star, > 40K nodes	1-10 ms	>10 years
LTE-M [137]	3GPP	Different licensed UHF bands (1.4 MHz carrier bandwidth)	10-25 km	300/375 kbit/s (variable), up to 1 Mbit/s	QPSK, QAM (OFDMA Full-duplex)	3GPP AKA	Star, >1M nodes	10-15 ms	10+ years
MIOTY [138]	MIOTY Alliance [139], proprietary, ETSI (TS 103-357)	Sub 1 GHz, 2.4 GHz (200–600 kHz of channel bandwidth)	5 km (city), 15 km (rural) and 30 km (free space)	407 bits/s	Telegram Splitting Ultra-narrow Band (TS-UNB)	AES-128	Star	3.6–30 s (10–245 byte messages)	Up to 20 years
NB-Fi [140]	Proprietary but open [141]	Unlicensed ISM bands (868 MHz, 915 MHz, other sub-GHz bands), 50 Hz - 25.6 KHz channel bandwidth	Up to 10 km (urban), up to 40 km (rural)	50, 400, 3,200 and 25,600 bit/s	DBPSK	AES-256 or other symmetric block cipher algorithm with 256-bit encryption key	Typically star, mesh is possible with an NB-Fi transceiver	-	Up to 10 years on battery power
NB-IoT [142]	3GPP	700, 800 and 900 MHz (200 kHz carrier bandwidth)	10-15 km	200 kbit/s (typically 100 kbit/s)	BPSK, QPSK (OFDMA Half-duplex)	Yes (defined by 3GPP)	Star, > 200k	< 10 s	> 10 years with a battery capacity of 5 Wh
SigFox [133], [143], [144]	SigFox [145]	868-902 MHz, 915-928 MHz (100 Hz channel bandwidth)	3-10 km (urban), 30-50 km (rural)	100 kbit/s	GFSK (DL), DBPSK (UL)	AES	Star, > 25K nodes	1-30 ms	10 years sending 1 message, < 10 years sending 6 messages

TABLE 2. ***(Continued.)*** **Most relevant characteristics of the latest Auto-ID and communications technologies for Industry 5.0.**

Technology	Standardization Body	Operating Frequency	Maximum Range	Max. Data Rate	Modulation Scheme	Encryption	Topology	Latency	Battery Lifetime
Weightless-P [146], [147]	Weightless SIG [148]	License-exempt sub-GHz frequency bands (e.g., 138 MHz, 433 MHz, 470 MHz, 780 MHz, 868 MHz, 915 MHz, 923 MHz), 12.5 KHz channel bandwidth	15 Km	100 kbit/s	GMSK, OQPSK	AES-128/256	Star	Low	3-8 years
Weightless-N [149], [150]	Weightless SIG [148]	License-exempt sub-GHz frequency bands (200 Hz channel bandwidth)	3 Km (urban)	100 kbit/s	Differential binary PSK (DBPSK)	AES-128	Star	Low	10 years
Weightless-W [146], [147]	Weightless SIG [148]	License-exempt sub-GHz frequency bands, 470-790 MHz	5 km	100 Mbit/s	6-QAM, BPSK, QPSK, DBPSK	128/256-bit AES	Star	Low	3-5 years
Wi-SUN/IEEE 802.15.4g [151]	Wi-SUN Alliance [152]	<2.4 GHz	1 Km	50 kbit/s–1 Mbit/s	2-GFSK	AES-128	Mesh	0.02 s	FAN devices consumption is less than 2 uA when resting and only 8 mA when listening. Batteries can last more than 10 years

6) OPERATING FREQUENCY

It is important to distinguish between technologies that operate in licensed or unlicensed bands. The former implies that part of the spectrum is reserved, thus mitigating electromagnetic interference, but there is an entry barrier due to the spectrum scarcity and the expensive license fees. On the contrary, unlicensed bands have a more reduced cost but they have to implement additional mechanisms to protect against the electromagnetic interference and congestion caused by other networks that operate in the same frequency band. For instance, interference can be mitigated with PHY (e.g., frequency hopping) or MAC layer mechanisms. In addition, the use of unlicensed bands is often related to limitations in power transmission and duty-cycle, which may be optimized depending on application requirements like delay, energy consumption or collisions [153].

With respect to the technologies compared in Tables 2 and 3, there are some like ZigBee [52], LoRa or Sigfox that can use frequencies below 1 GHz, which have better signal propagation in industrial environments than frequencies above them [154].

In fact, technologies that work in the 2.4 and 5 GHz bands, like BLE, Wi-Fi, ZigBee and WirelessHART, must be carefully considered, since electromagnetic interference from other wireless systems that operate on the same frequency band can occur, which derives into having worse propagation characteristics in industrial scenarios than when lower frequencies are used [155]–[158].

In the case of UHF RFID and DASH7, they both operate in a frequency that is sensitive to some extent to the electromagnetic interference present in a shipyard, but which is slightly less aggressive than the one that may happen in the 2.4 GHz band [159].

Technologies like UWB, frequently used in indoor positioning [160], make use of very high frequencies, whose propagation is difficult in highly-metallic environments [161]. For the case of ultrasounds, although the technology uses frequencies that do not cause electromagnetic interference with the scenario under evaluation, they can interfere with the weapons of a warship (ultrasounds may induce the ignition of weapons [162]).

It must be noted that although channel modelling of metallic environments such as factories is well established, there is limited, and mainly outdated, literature on wireless radio propagation within ships [163]. Due to its unique structure and operation, the channel characteristics and multipath propagation are different from those reported in the literature for metallic industrial scenarios [164].

7) MAXIMUM RANGE

Barcodes are currently one of the most used Auto-ID technologies of Navantia and also in many industrial companies due to their cost and simplicity. They can be either 2D or 3D (e.g., QR codes), require Line-of-Sight (LoS) and can be read at distances that range from centimeters to several meters, depending on their type and size.

Technologies like LF/HF RFID or NFC are only appropriate for identifying objects at a short distance (e.g., under half a meter). As a consequence, when considering the deployment restrictions inside an OPV, the selection of such Auto-ID technologies would imply to not to be able to provide a ubiquitous Auto-ID system.

TABLE 3. Cost and main advantages, limitations and applications of the latest Auto-ID and communications technologies for Industry 5.0.

Technology	Cost	Main Advantages	Main Limitations	Main Applications
Barcode/QR [68]–[70]	Very low cost (< € 0.05)	Visual decoding, optical (laser)	LoS, only read, scanners need humans to operate, limited data capacity, limited reliability (no ruggedness: wrinkled and smeared tags will not work)	Asset tracking and marketing
NFC [72]	Low cost	Tags require no batteries	Short communications distance, reading range decreases in the presence of liquids and metal objects	Asset tracking, payments
LF RFID [73]	Low cost readers and tags	Tags require no batteries, can be read through metal and through items storing liquids	Short reading distance	Product tracking and security access controls
HF RFID [75]	Low cost readers and tags	Tags require no batteries, more reading range than LF RFID tags	Worse performance than LF RFID with liquids and metal objects	Product tracking, payments
UHF RFID [77]	Low cost tags, readers may be expensive	Longer reading range than other types of RFID tags	Batteries need to be recharged or replaced periodically	Asset tracking, access/security, supply chain, vehicle identification
Infrared (IrDA) [79]	Low cost	Physically secure data transfer, different data rates and coding schemes depending on the type (SIR, MIR, FIR, VFIR, UFIR, GigaIR)	Need for LoS for proper operation, low data rates	Remote control, data transfer
Ultrasounds [81], [82]	Moderate (around $20 per tag, hundreds of dollars per exciter/reader)	Based on sound wave propagation, sub-centimeter accuracy	Short reading distance and very low wall penetration, so its practical accuracy depends on the number of deployed readers	Asset positioning and location
RuBee [83]	Low cost tags ($6 per tag in high volumes)	Magnetic propagation, low energy consumption, good propagation with metal	Licensed solutions	Applications with harsh electromagnetic propagation
UWB [85], [86]	Moderate	High location accuracy (< 50 cm), low electromagnetic interference	Interference resilience is low with the simplest receivers, network size	Real-Time Location Systems, short-distance streaming
BLE (Bluetooth 4.2) [90], [91]	Low (<$100 gateway, $5 module)	Easy deployment, low electromagnetic interference, good for small data chunks	Not very flexible, eavesdropping issues, limited mobility, up to one master and 7 slaves (but scatternet unlimited)	Beaconing
WirelessHART [92], [93]	Expensive gateways	Compatibility with HART protocol	Deployments are expensive for large factories	Wireless sensor network applications
ZigBee [95]	Low ($50 gateway, $5 module)	Low power, reliable and scalable (up to 65,536 nodes)	Potential electromagnetic interference with other ISM-band devices, consumption is not low when sleep modes are not used appropriately	Sensor networks, smart buildings and industrial applications
Z-Wave [98]	Low cost	Very low power, up to 232 nodes	Up to 4 hops	Home automation
ANT+ [100]	Moderate	Ultra-low power, up to 65,533 nodes	Not adequate for strict QoS requirements	Health, sport monitoring
Wi-Fi [101]–[104]	Moderate	High-speed, ubiquity, easy to deploy and access	Security vulnerabilities, poor multipath performance, high electromagnetic interference with other ISM-band systems	Wireless LAN connectivity, Internet access
Wi-Fi HaLow [105]–[107]	–	Low power, different QoS levels (8192 stations per AP)	–	IoT applications
Wi-Fi 6 [109]	–	Backwards compatibility	–	Wireless LAN connectivity, Internet access
Insteon [111]	Moderate	Up to 2^{42} nodes	Gateway required	Home automation, access control
EIB/KNX RF [113]	Relatively expensive transceivers	Up to 256 nodes per line	–	Home and building automation
EnOcean [116]	Moderate	Up to 2^{32} nodes	–	Energy harvesting building automation applications
Thread [118]	–	Seamless integration with IP networks	Vulnerable to electromagnetic interference	Home automation and IoT applications
SAW (Surface Acoustic Wave) [122]–[124]	Low	Identification, sensor and wireless capabilities for passive devices, electromagnetic interference immunity	Niche market, few industrial implementations	Components (e.g., filters, resonators, delay lines, correlators), use for inaccessible locations

TABLE 3. *(Continued.)* Cost and main advantages, limitations and applications of the latest Auto-ID and communications technologies for Industry 5.0.

IQRF [125]	Low ($80 gateway, $8 module)	Low power and long range	–	IoT applications, telemetry
Bluetooth 5 [127], [128]	Low	Low power (batteries can last days to months)	Trade-off among different PHY modes	Beacons, IoT applications
DASH7 [130]	Moderate-High, $100 - $1000 /gateway	BLAST (Bursty, Light, Asynchronous, Stealth, Transitive) network technology	Low data rate	Product tracking and identification, smart industry and military, M2M communications
EC-GSM-IoT [130]	Low	Improved GSM/EDGE security, high number of subscriber terminals (i.e., 50.000 per cell)	Not design to support data throughput>10 kbps, requires paying a subscription	Machinery control, IoT/IIoT applications
RPMA (INGENU) [133]	Low cost	Multiple access, electromagnetic interference robustness, time/frequency synchronization, uplink power control, downlink data rate optimization, handover	Lack of mobility	M2M and IoT applications
LoRa, LoRaWAN [135]	Low cost	Resistant to interference	Limited size data packets, limited QoS (there is no acknowledgment of all packages)	Logistics, IIoT applications
LTE-M [137]	Low	Uses existing LTE network, multicasting, positioning, VoLTE	Coupling, repetitions slow down the transmission	IoT applications
MIOTY [138]	Moderate	Better scalability and scale than LoRa networks and a lower cost and better performance than low-power cellular networks (1.5 million messages per day or 500.000 nodes (3 msgs/day))	Use cases are limited	Industrial IIoT
NB-Fi [140]	N/A as of writing	Decentralized architecture, adaptive data rate, optimized spectrum utilization algorithms based on SDR technology and AI techniques, highly scalable (up to 2 million sensor nodes), full-duplex for BSs and half-duplex for devices	-	M2M communication applications
NB-IoT [142]	High, SIM needed, $15000 per base station	LTE in-band, guard-band, wide area coverage	No handoff support	IoT applications
SigFox [133], [143], [144]	Low cost	Global cellular network	No FEC, BS may not support multiple sectors, 140 messages per day per device	IoT applications
Weightless-P [146], [147]	Moderate	High reliability and scalability	Scarcity of hardware, infrequent update specification, require kit and AP to operate	IoT applications
Weightless-N [149], [150]	Low (lower than Weightless-P)	Supports mobility and connectivity among carriers	Unidirectional communications	IoT/IIoT applications
Weightless-W [146], [147]	Moderate	Designed to operate in TV white space spectrum, relatively high data rates	–	Industrial applications
Wi-SUN/IEEE 802.15.4g [151]	Moderate	Field Area Networking (FAN) and Home Area Networking (HAN) profile, Multi-hop support	–	Smart grid and metering

On the contrary, there are long range technologies that have a maximum range that can reach kilometers in unlicensed bands (e.g., LPWAN technologies like LoRa/LoRaWAN) or that are aimed at being global thanks to the use of a complex communications network (e.g., NB-IoT, SigFox, LTE-M). However, the latter require paying fees and the use of a SIM (Subscriber Identity Module) or an eSIM (electronic SIM).

Finally, it must be noted that the maximum range achieved by the technologies is also determined by the network topology: some technologies like ZigBee or Bluetooth are able to deploy mesh networks where relay nodes allow for significantly increasing the transmission distance (from a few hundred meters to kilometers).

8) MAXIMUM DATA RATE

The maximum data rate is related to PHY and MAC layer features like the operating frequency band, available bandwidth or the modulation and coding scheme.

Table 2 shows that there are technologies like LoRa and SigFox that have good signal propagation, but provide low data rates, so they are not suitable for Industry 5.0 scenarios that require transmitting payloads at high speed.

Other technologies such as IEEE 802.11 b/g/n/ac and Wi-Fi 6 are able to reach high data rates, but this is achieved at the expense of increasing energy consumption, thus decreasing their battery lifetime.

9) MODULATION SCHEME

The reliability of a technology over long distances depends largely on its modulation and coding scheme. Fewer points in the constellation diagram provide more reliability and, at the same time, less data rate. For example, Binary Phase Shift Keying (BPSK) is slower but more reliable than Quadrature Amplitude Modulation (QAM). Nonetheless, note that the robustness of a technology can also be improved by using retransmissions at the MAC layer and error control techniques, although such techniques imply additional latency.

10) ENCRYPTION AND TRANSMISSION SECURITY

Most of the technologies compared in Table 2 implement some kind of data encryption mechanism. One of the most used is Advanced Encryption Standard (AES), which is a symmetric algorithm that is currently considered secure for key lengths of 128 bits. However, note that the fast evolution of quantum computers threatens AES security, which will have to double its key length in the next years [165].

Moreover, most Auto-ID technologies make use of additional security mechanisms for authentication and data protection. In the case of the latter, Cyclic-Redundancy Check (CRC) is the most frequent choice.

Furthermore, in order to avoid data corruption and, at the same time, control the access to the wireless channel, technologies like Wi-Fi, UWB or ZigBee implement protocols like Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA).

11) TOPOLOGY

Topology has a significant impact on the performance of a deployment. For example, in a single-hop network, robustness depends on a single link and the system can only be extended by deploying additional base stations. In practice, such an approach constrains the capabilities of a network, since the number of additional base stations is limited. In contrast, multi-hop networks provide more robustness and range extension, although they incur in additional latency and energy consumption due to data forwarding and routing.

There are technologies like Bluetooth or ZigBee that are able to implement mesh networks, which provide communications redundancy and cover long distances. However, such a kind of networks may suffer from bottlenecks that can occur when several devices communicate directly with the gateway of a mesh network.

In the case of star topologies, a device (e.g., a gateway) centralizes the message exchanges with the deployed end devices. Such a centralization frequently derives in the fact that the central device becomes a single-point-of-failure that can get saturated, so technologies like LoRaWAN implement protocols that negotiate communications frequency according to factors like distance or message length [166].

12) LATENCY

Latency has a significant impact on Auto-ID performance, especially in Industry 5.0 systems with real-time restrictions. Although Table 2 indicates estimations of the latency for part of the compared technologies, it is important to note that different factors can increase latency in industrial environments, like the deployment topology (e.g., the number of required intermediate relay nodes), traffic load, the existence of electromagnetic interference or the scenario complexity (in terms of the number of obstacles, which increase the communications path length).

Moreover, it is worth noting that latency for technologies like BLE or UWB is conditioned by the selected beaconing intervals. Nonetheless, in the case of Wi-Fi HaLow, there is recent research that mitigates the mentioned dependency on beaconing intervals by adjusting the Restricted Access Window (RAW), a configurable medium access feature of IEEE 802.11ah [167].

As a consequence, an Industry 5.0 developer should analyze every specific deployment case individually in order to estimate latency accurately.

13) BATTERY LIFETIME

Although there are many studies that model and/or evaluate energy consumption of emerging wireless communication technologies, there are many factors that may impact the battery lifetime of an Industry 5.0 deployment like the transmission power, data rate, topology (consumption is increased with forwarding and routing operations in multi-hop networks), MAC design (e.g., scheduling, contention resolution), coding or the use of Forward Error Correction (FEC), as well as the chosen hardware. For instance, for a specific technology and when transmitting at a fixed power, the lower the data rate, the longer the transmission time, which implies a higher consumption and, therefore, a reduction of the battery lifetime.

Nonetheless, it can be stated that there are certain Auto-ID technologies that have been conceived having low energy consumption in mind, while others have not. For example, Bluetooth 5 or EnOcean have been specifically designed to reduce energy consumption significantly under certain circumstances. In addition, there are other technologies like ZigBee, whose transmission power is not very low, but which make use of deep sleep states to reduce average power consumption dramatically.

In contrast, other technologies like Wi-Fi 6 have not been conceived for minimizing energy consumption but to provide good indoor range and fast WLAN communications (although mechanisms to manage certain aspects related to power consumption are frequently provided).

14) COST

The cost of an Auto-ID solution for Industry 5.0 scenarios needs to consider aspects like the price of the tags and readers, the communications network deployment cost or the need for paying service fees. Sometimes there is also an additional cost for the use of specific front-end and back-end industrial software, but, since such a software is related to certain manufacturers (not to the technology), it is not taken into account in Table 3.

Considering the previous clarifications, it can be stated that there are really cheap technologies (e.g., QR codes), low-cost technologies (e.g., LF/HF RFID, BLE), technologies whose tags are cheap, but their readers can be expensive (e.g., UHF RFID) and technologies that require paying data use or monthly fees (e.g., SigFox, NB-IoT). In any case, Industry 5.0 developers should make an economic feasibility plan that takes all costs into account before deciding on the deployment of a specific Auto-ID technology.

C. TECHNOLOGY SELECTION

The suitability of the different technologies analyzed in the previous subsection was evaluated. First, part of the technologies were discarded due to different reasons:

- The next technologies were not selected essentially because, although they could be potentially used for the proposed application case, they were actually devised for sensing/actuation IoT applications rather than optimized for Auto-ID applications: WirelessHART, ZigBee, Z-Wave, ANT+, Wi-Fi, Wi-Fi HaLow, Wi-Fi 6, Insteon, EIB/KNX-RF, EnOcean, Thread, IQRF, EC-GSM-IoT, RPSMA, LoRa/LoRaWAN, LTE-M, MIOTY, NB-Fi, NB-IoT, SigFox, Weightless-P/N/W and Wi-Sun.
- The following Auto-ID technologies were discarded due to their short reading range: bar/QR codes, NFC, LF RFID, HF RFID and IrDA.
- Ultrasounds and SAW were not selected due to the lack of standardization.

The remaining technologies were the ones actually compared. Table 4 shows the parameters that were considered to determine whether a technology was fully, partially or non-compliant according to the operational and technical requirements of the proposed application for the OPV. In Table 5 the technologies fully compliant with the operational and technical requirements are colored in green while the ones non-compliant are colored in red. The requirements that are partially fulfilled are colored in yellow. In addition, it is worth mentioning that the column ’Type’ was added in order to distinguish the technologies that have been conceived as Auto-ID technologies from the ones that can be used for such a purpose, but which are not optimized for it. Moreover, other columns were grouped or removed respect to Tables 2 and 3 in order to simplify the comparison:

- Maximum Data Rate considers jointly the different parameters from Table 2 that impact data rate.

TABLE 4. Technical requirements to be fulfilled to be a fully, partially and non-compliant technology.

Parameter	Fully	Partially	Non-compliant
Type	Auto-ID	WPAN	Others
Standardization	Open Standard	Proprietary Standard	No Standard
Operating Frequency	Unlicensed Bands	Licensed Bands	Restricted Bands
Maximum Reading Range	> 20 m	Between 10 m and 20 m	Up to 10 m
Maximum Data Rate	More than 5 kbit/s	Between 1 kbit/s and 5 kbit/s	<1 kbit/s
Security	Standard Encryption and Authentication Mechanisms	Non-Documented Security Mechanisms	No Security Support
Battery Lifetime	> 5 Years (Lifecycle-Support Period of the OPV)	Up to 5 Years	Up to 2 Years (Less than Half of the Lifecycle Support Period of the OPV)
Cost	Low	Moderate	High, Payment of Service Fees

- The topology is omitted from the comparison due to having a lower impact on the selected use case than other selection parameters.
- Latency is not included for the sake of carrying out a fair comparison, because, as indicated in the previous subsection, there are different parameters that influence it.
- Column Reading Range considers not only the maximum ranges indicated in the previous subsection, but also the fact of providing NLoS communications and good signal propagation, which are essential for the proposed use case.
- Cost considers deployment and running costs. For the selected scenario, technologies that require the payment of service fees (e.g., LTE-M, NB-IoT, SigFox) were considered as non-appropriate.

After a thorough comparison, four technologies were selected: UHF RFID, RuBee, BLE and Dash7. BLE was discarded because of its battery lifetime and the scarcity of industrial ruggedized tags. RuBee was also discarded due to the lack of a diversity of manufacturers (there is currently only one world-wide manufacturer), which supposes a clear dependency. As a consequence, two technologies were selected: UHF RFID and Dash7. In practice, active UHF RFID and Dash7 are similar in terms of performance, so the former was selected together with passive UHF RFID to carry out the implementation and empirical evaluations described in the next sections.

VI. STAGE 3: IMPLEMENTATION

A. HARDWARE

In order to test the selected active and passive RFID technologies, the hardware described in the next subsections was chosen.

TABLE 5. Comparison of the most promising Auto-ID technologies for the OPV use case. Color legend: green (fully compliant with the operational and technical requirements), yellow (partial fulfillment) and red (non compliant).

Technology	Type	Standardization	Operating Frequency	Reading Range	Maximum Data Rate	Security	Battery Lifetime	Cost
UHF RFID	Auto-ID	ISO 18185-5, ISO/IEC 18000-6, ISO 18000-6C (EPC Class 1 Gen 2), ISO 10374, ISO/IEC 18000: Part 7, ASTM , EPCglobal	30 MHz–3 GHz	<120 m	<640 kbit/s	Yes	From days to years (batteries need to be recharged or replaced periodically)	Low cost tags, readers may be expensive
RuBee	Auto-ID	IEEE 1902.1	30–900 kHz	Up to 30 m	Up to 8 kbit/s	No security documentation was found	Several years	Low cost tags, moderate cost of the readers
UWB	Auto-ID & WPAN	IEEE 802.15.3	3.1 to 10.6 GHz	< 100 m	>110 Mbit/s, up to 27 Mbit/,s for 802.15.4a	Yes	Hours to months (batteries need to be recharged)	Moderate
BLE	WPAN	IEEE 802.15.1	2.4 GHz	>100 m	250 kbit/s, 1 Mbps	Yes	A few years on a single coin-cell battery	Low (<$100 gateway, $5 module)
Bluetooth 5	WPAN	Bluetooth SIG	2.4 GHz	<400 m	Up to 2 Mbit/	Yes	Days to months (batteries need to be recharged)	Low (similar to BLE)
DASH7	Auto-ID	DASH7 Alliance, ISO/IEC 18000-7	315–915 MHz	<10 km	27.8 kbit/s	Yes	Months to 10 years	Moderate-High

1) PASSIVE RFID HARDWARE

A cost-effective mobile reader based on Windows CE (A6-UHF Long Range) was selected to provide mobile identification [168]. The A6 UHF RFID SEUIC terminal is an industrial PDA/UHF RFID reader with an external directional antenna and a 3.5” touch screen. It provides multiple connectivity options (e.g., Wi-Fi, Bluetooth, GPRS, GPS) and has the possibility of incorporating barcode, QR code and camera scanners.

For the sake of fairness, multiple tags were selected to carry out the passive RFID validation. They were all from Omni-ID [169], a company that manufactures a wide range of UHF RFID tags for industrial environments. Specifically, the following tag families were selected:

- Fit UHF Tag on-metal family. Model: Fit 400.
- Exo UHF Tag on-metal family. Models: Exo 600, Exo 750 and Exo 800.
- Dura UHF Tag family. Models: Dura 600, Dura 1500 and Dura 3000.
- Adept UHF Tag family. Model: Adept 360°-ID.

The main specifications given by the manufacturer on the selected tags are summarized in Tables 6 and 7, and are described next:

- Fit 400 tags [170] have a small form factor and support high temperatures, being able to withstand temperatures of up to 235°C. With a maximum reading range of 4 m, Fit 400 tags are well suited for reduced spaces or when the tracked asset is very small, but high performance is demanded.
- Omni-ID Exo 600 [171] tags have been designed for achieving a long reading range and a broad reading angle when attached to metal bars. Therefore, they are suitable for logistics, warehouse applications and Returnable Transport Items (RTI). These tags can be easily mounted using rivets or closed cell foam adhesive.
- Omni-ID Exo 750 [172] provides a broad reading angle. It is well suited for being attached to metal assets with a square form factor. Omni-ID Exo 750 offers reliability in both outdoor and industrial applications, specially RTI applications, with a moderate durability.
- Omni-ID Exo 800 [173] is a long reading range passive UHF RFID tag with a small size that is optimized to read on, off, and near metal surfaces. In addition, it has high durability and it has a ruggedized design for long term use outdoors. Furthermore, it can be embedded into a transparent case that can be used to provide full protection to a printed QR code or a barcode.
- Dura 600 [174] is a small form factor RFID tag, with extreme impact resistance and good on-metal performance. Its flexible durable thermoplastic elastomer case design and foam adhesive makes it optimal for asset management and heavy industrial applications with curved or contoured assets (e.g., valves, pipes).
- Omni-ID Dura 1500 [175] is a durable long-range tag with extreme impact resistance and high temperature ratings. According to the manufacturer, it is suited for outdoor heavy industry deployments (e.g., container tracking for yard management, defense asset management or cargo tracking).
- Omni-ID Dura 3000 [176] reaches a reading range of up to 35 m, on, off or near metals and liquids. Its main features are high impact resistance, waterproof and a durable case. It is optimized for tracking large assets in open storage environments, without worrying about battery duration.

TABLE 6. Specifications of the selected passive RFID tags.

Family	Model	Form factor	Max. Reading Range	Dimensions	Weight	Frequency Range	Material	Material Compatibility	IC Type (chip)	Protocol	Memory
Fit	400		4 m	13.1×7.1×3.1 mm	380 g	866-868 MHz (EU) 902-928 MHz (US)	Ceramic, painted black	Optimized for metal	Alien H3	EPC Class 1 Gen2v2	EPC - 96 bits, User - 512 bits, Unique TID - 64 bits
Exo	600		Fixed reader: 6 m, handheld: 3 m	With holes: 80×15×12 mm, without: 60×15× 12 mm	12 g	860-930 MHz (GS)	Grey ABS Rigid Plastic, supported impact: 10 kg from 1 m	Optimized for metal	Impinj Monza 4QT	EPC Class 1 Gen2v2	EPC - 128 bits, User - 512 bits, Unique TID - 48 bits
	750		Fixed reader: 7 m, handheld: 3.5 m	51×48×12.5 mm	25.6 g	860-930 MHz (GS)	ABS	Optimized for metal	Impinj Monza 4QT	EPC Class 1 Gen2v2	EPC - 128 bits, User - 512 bits, Unique TID - 48 bits
	800		Fixed reader: 8 m, handheld: 4 m	110×25×13 mm	26 g	860-930 MHz (GS)	Grey ABS Rigid Plastic, supported impact: 10 kg from 1 m	Optimized for metal	Impinj Monza 4QT	EPC Class 1 Gen2v2	EPC - 128 bits, User - 512 bits, Unique TID - 48 bits
Dura	1500		Fixed reader: 15 m, handheld: 7.5 m	140×66×14 mm	79 g (ABS) 82 g (PC)	860-930 MHz (GS)	ABS or Polycarbonate, supported impact: >25 kg from 1 m	Optimized for metal	Alien H3	EPC Class 1 Gen2	EPC - 96 bits, User - 512 bits, Unique TID - 64 bits
	3000		Fixed reader: 35 m, handheld: 20 m	210×110×21 mm	265 g	860-930 MHz (GS)	ABS or Polycarbonate, supported impact: >25 kg from 1 m	Metal and non-metallic substrates	Alien H3	EPC Class 1 Gen2	EPC - 96 bits, User - 512 bits, Unique TID - 64 bits
	600		Fixed reader: 5 m, handheld: 2.5 m	49×38×9.5 mm	12 g	902–928 MHz (US) 865–868 MHz (EU)	Durable Thermoplastic Material	Optimized for metal	Alien H3	EPC Class 1 Gen2	EPC - 96 bits, User - 512 bits, TID - 64 bits
Adept	850		8.5 m	65×45×8 mm	34 g	860-960 (GS)	ABS	Optimized for metal	Qstar-5A	EPC Class 1 Gen2	EPC - 240 bits User - 64 Kbits (high memory tag)
	360		10 m	136.5×48×5.5 mm	126 g	860-930 MHz (GS) 13.56 MHz (HF opt.)	Steel frame, supported impact: >25 kg from 1 m	Any (metal and non-metallic substrates)	Alien H3 (UHF) NXP I-Code (HF opt.)	UHF - EPC Class 1 Gen2, HF (Opt.) - ISO 15693	UHF EPC - 96 bits, UHF User - 512 bits, UHF TID - 64 bits, HF (opt.) - 1 Kbit

- Regarding the Omni-ID Adept family, Adept 360° [177] has a 360° reading angle for the harshest environmental applications. It is encased in an industrial steel frame with a tether attachment that is specially designed for heavy industry applications. It is ideal for tracking slings, shackles and heavy machinery. It is available with a range of options, including a surface etching/printing finishing option and a dual technology option. With respect to Omni-ID Adept 850 [178], it is a durable tag with 64 Kbits of user memory that is specifically designed to store production data throughout global manufacturing operations.

2) ACTIVE RFID HARDWARE

The selected active RFID reader was an NPR ActiveTrack-2 [179], which, according to the manufacturer, has a coverage radius of 45 meters with standard antennas. In addition, high-gain antennas were acquired to extend its coverage to about 90 meters. Among the different tags supported by such a reader, the Active RuggedTag-175S tag [180] was chosen, since it is designed to withstand aggressive environments and is sonically welded, which helps to resist the effects of maritime environments. Its lithium CR2032 battery lasts more than 4 years. With respect to its form factor, its dimensions are 63.75 × 37.72×25.4 mm with a weight of 51 g.

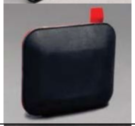
B. SOFTWARE

1) PASSIVE RFID

Data were collected through a specific application implemented in C# using the native Software Development Kit (SDK) of the A6 UHF RFID SEUIC reader. Such an application provides the following functionality:

- Configuration of automatic scanning operations for reading tags periodically.
- Read and write tags. The Received Signal Strength (RSS) values obtained from each tag are shown during the reading process. RSS values are internally stored and

TABLE 7. Specifications of the selected passive RFID tags (cont.).

Family	Model	Form factor	Operating Temperature	Max. Temperature Exposure (Max. constant exposure = 700 hours)	Ingress Protection	Shock and Vibration	Attachment	Typical Application	Indicative Price per Single Unit	Datasheet Reference
Fit	400		-20°C to +85°C	-20°C to +235°C	IP68	MIL STD 810-G	Film adhesive (included). For placement only in applications exceeding +85°C	Metal hand tools, metal IT assets including covert tracking, embedding into metal components, autoclaves and high temperature sterilizations	€5.8	[170]
Exo	600		–40°C to +85°C	–40°C to +85°C	IP68	MIL STD 810-G	Mechanical (std), cable tie, premium foam (option)	Logistics and postal, automotive, retail and warehousing	€3.48	[171]
	750		–40°C to +85°C	–40°C to +85°C	IP68, submersion proof to 3000 m depth	MIL STD 810-G	Mechanical (std), cable tie, premium foam (option)	Automotive supply chain, logistics and postal, manufacturing tote tracking	€3.48	[172]
	800		–40°C to +85°C	–40°C to +85°C	IP68, submersion proof to 3000 m depth	MIL STD 810-G	Mechanical (std), cable tie, premium foam (option)	Retail supply chain, logistics and postal, manufacturing tote tracking	€3.48	[173]
Dura	1500		ABS: –40°C to +65°C , PC: –40°C to +100°C	Long-term max. temp. exposure (days, weeks, years) ABS: +65°C , PC: +100°C , Short-term max. temp. exposure (minutes, hours) ABS: +75°C , PC: +120°C	IP68	MIL STD 810-G	Manual (standard), Standard foam adhesive (option), Premium foam adhesive (option)	Container tracking for yard management, cargo tracking, defense asset management	€11.6	[175]
	3000		ABS: –40°C to +65°C , PC: –40°C to +100°C	Long-term max. temp. exposure (days, weeks, years) ABS: +65°C , PC: +100°C , Short-term max. temp. exposure (minutes, hours) ABS: +75°C , PC: +120°C	IP68	MIL STD 810-G	Manual (standard), standard foam adhesive (option), premium foam adhesive (option)	Cargo and container tracking, heavy equipment tracking and maintenance, location identification in lay down zones	€17.4	[176]
	600		–40°C to +85°C	Long-term max. temp. exposure (days, weeks, years) +85°C, Short-term max. temp. exposure (minutes, hours) +105°C	IP68	MIL STD 810-G	Industrial foam tape 3M PT1100	Deployed production equipment, chemical drums, beverage kegs	€6.38	[174]
Adept	850		-20°C to +85°C	-20°C to +85°C	IP68	MIL STD 810-G	Rivet/screw (not included), foam or thin film adhesive (option), riveting is highly recommended for applications above 55°C. Attachment hole (diameter: 5.2 mm)	Manufacturing and supply, outdoor and industrial operations (engine carrier tags in assembly operations, trolley and carrier tags in power train operations, dunnage/RTI tags for warehouse operations)	€31.9	[178]
	360		-40°C to +85°C	Long-term max. temp. exposure (days, weeks, years) +120°C, Short-term max. temp. exposure (minutes, hours) +140°C	IP68	MIL STD 810-G	Tether attachment (not included)	Very heavy industry applications. Identification of lifting equipment for maintenance and inventory management (e.g., slings, shackles, heavy machinery)	€23.2	[177]

can be later sent wirelessly to a remote database on the Fog Layer or in Navantia's cloud.

- Configuration of the reading and writing frequency (e.g., in UHF 902-928 MHz).
- Configuration of the transmission power between 20-26 dBm.

In order to perform the previously mentioned operations, the application shows three main menus:

- The ''Inventory'' menu shows the Unique Identifiers (UIDs) of the read tags, their RSS values and the number of times they have been read.
- The ''Read Tag/Write Tag'' menu enables reading the information stored on tags and allows for editing it.
- The ''Pipe Details'' menu reads the information stored by a tag, process it and shows the details of the tagged item. As an example, Figure 7 shows a screenshot of such a menu. As it can be observed, the provided data ease the labor of operators when looking for a specific item (i.e., it shows a picture of the item) or when needing to obtain its characteristics fast.

2) ACTIVE RFID

In the case of the Active RFID software, no software was developed for the performed measurements, since the reader already includes an embedded web server that can be accessed through Ethernet and that provides all the information regarding the detected active tags and their signal strength.

VII. STAGE 4: EXPERIMENTAL VALIDATION

A. TEST METHODOLOGY

After performing successfully in the lab development tests on the hardware and software, real-world tests were conducted in a Navantia's OPV that was under construction in the shipyard of Ferrol [181]. A picture of the warship is shown in Figure 8.

The aim of the experiments was to validate the selected technologies in order to determine the maximum reading

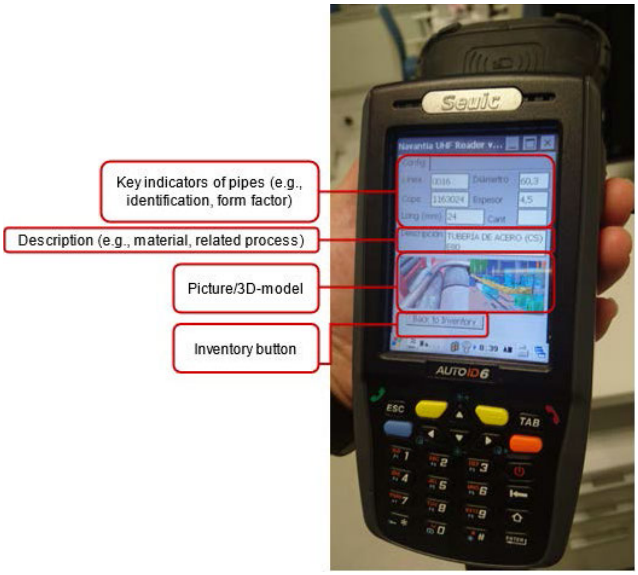


FIGURE 7. Passive RFID mobile reader running the developed software.

FIGURE 8. Ship where the tests were performed.

distances obtained by each RFID tag under in different locations of the ship that had different densities of metallic objects. The tests were primarily focused on assessing the most favorable cases for determining how far the selected RFID tags could be read: if the results for the best-case scenario are not as good as expected, then, obviously, the system will perform worse in more complex scenarios.

The tests were also designed to obtain results that could be compared with previous tests that were carried out in a lab and in shipyard workshops [7]. Specifically, experiments were performed to:

- Analyze how the physical characteristics of the test shipbuilding environments influence the RSS values collected by the Auto-ID system. As it is explained in our previous works [7], [21], such RSS values may be potentially processed and used by real-time location systems and ICPSs to estimate the location of the tag.
- Check whether additional challenges must be faced for such a specific scenario in order to deploy an Auto-ID system.

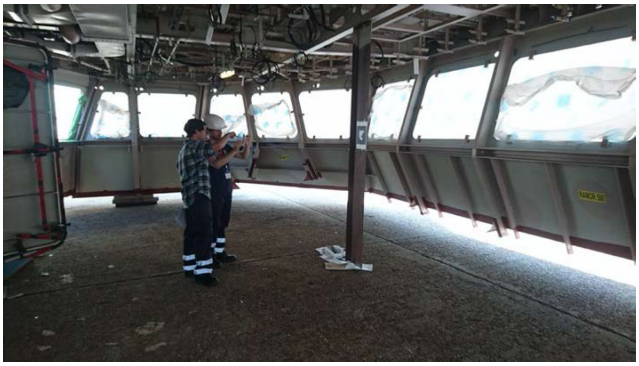


FIGURE 9. Inside the outdoor ship block.

- Evaluate whether the system will be able to serve as a basis for designing future traceability systems within ships that rely on IIoT devices.

Two types of experiments were performed with passive and active RFID:

- Outdoor ship block. With passive RFID tags, the maximum reading distance was obtained in a ship block that was being built outdoors, next to a shipyard workshop. Such a scenario represents a typical shipbuilding environment where communications are less exposed to multipath interference than inside a ship.
- Inside the OPV. Tests were performed inside the OPV, where four experimental scenarios were defined:
  - Maximum reading distance with LoS with passive UHF RFID. For each of the selected RFID tags, it was determined the maximum distance at which the tags could be read correctly when oriented in the most favorable position (when the tag and the reader antennas were in parallel).
  - Angle reading tests with passive RFID tags. The objective of these tests was to determine, for each of the selected tags, the maximum angle (with respect to the reader antenna) that allowed for obtaining a reading from the tags.
  - Scenario with a high density of metallic objects. For each passive RFID tag, the impact of metal object density was evaluated. A very high metal object density is usual in specific areas of the ship, such as where there is machinery like the wastewater processing plant or in certain areas with metallic floors or walkways.
  - Coverage inside the ship with active RFID tags. The coverage radius inside the vessel was estimated in a representative ship scenario.

B. PASSIVE RFID IN AN OUTDOOR SHIP BLOCK

As it was previously mentioned, a ship block (shown in Figures 3 and 9, as viewed from outside and inside, respectively) was chosen as a traditional shipbuilding scenario that represents an intermediate building stage carried out between individual element manufacturing (which takes place in the

TABLE 8. RSS values (in dBm) obtained for the different tags at different distances inside the ship block.

Reading Distance \ Tag Model	Exo 600	Adept 850	Exo 750	Exo 800	Adept 360	Dura 1500	Dura 3000	Dura 600	Fit 400
0.5 m	-37	-47	-50	-54	-57	-56	-62	64	-60
1 m	-53	-52	-55	-54	-62	-64	-61	X	X
2 m	-49	-62	-70	-60	-73	-68	-60	X	X
3 m	-61	-63	-65	-67	-73	-66	-65	X	X
4 m	-57	X	-70	-65	-72	-77	-61	X	X
5 m	X	X	-77	-71	-72	-76	-67	X	X
6 m	X	X	X	X	X	-69	X	X	X

X (in red) means that no readings were received continuously at such a distance (i.e., in some cases a signal was collected sporadically, but due to temporary reflections). Green: very good signal; yellow: good signal.

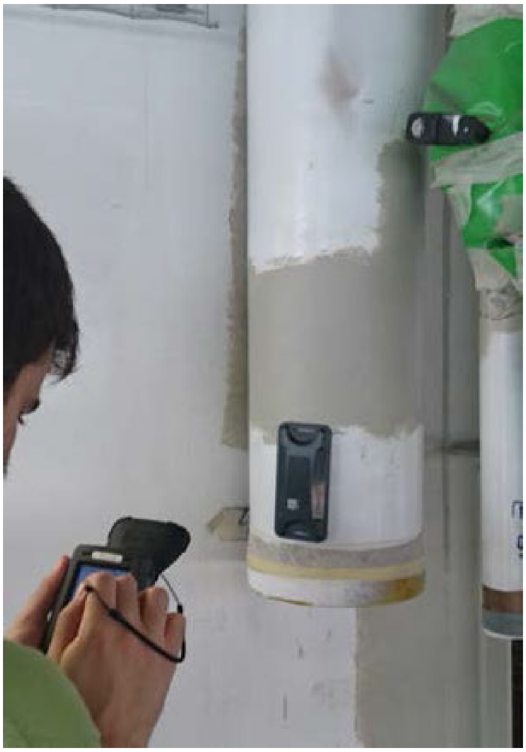


FIGURE 10. Testing of a passive RFID tag attached to one of the main pipes of the ship block.

workshops/warehouses of a shipyard) and the construction stages performed inside the ship.

1) MAXIMUM READING DISTANCE WITH LoS

A ship block is a scenario that has a lower density of pipes than most of the areas inside a ship and where LoS can be achieved. In such a scenario, the evaluated tags were attached to one of the main pipes of the ship block at a height of 1.5 m, as illustrated in Figure 10.

Table 8 shows the RSS values obtained when reading the selected nine passive tags at different distances (from 0.5 m to 6 m) in ideal circumstances (i.e., with LoS and with the antenna reader and the tag in parallel and at the same height). Thus, Table 8 allows for concluding that Dura 1500 was the only tag that could be read by the reader up to a 6 m distance. In contrast, Dura 600 showed a very short reading range, very similar to the one obtained by Fit 400, which has significantly smaller dimensions (13.1 × 7.1×3.1 mm versus 49×38 × 9.5 mm). The rest of the tags behaved as expected: with good tolerance to the fact of being attached to a metallic pipe and with a reading distance that was proportional to their antenna size.

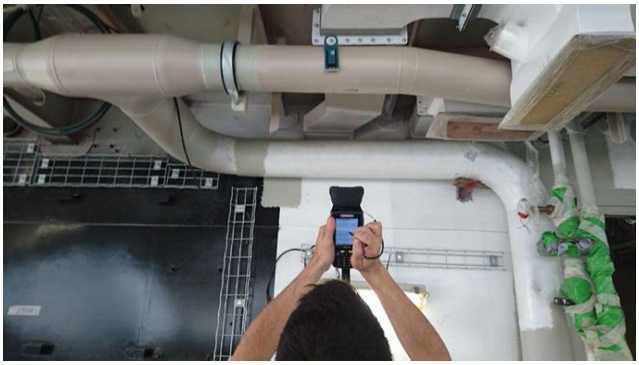


FIGURE 11. Testing of tag reading angles.

2) INFLUENCE OF THE TAG READING ANGLE

In an RFID UHF system, the beam of the antennas is typically narrow to increase reading distance, so the reading angle at which a tag can be read is limited. In order to quantify such an angle, additional measurements were taken in the ship block but attaching each tag to a pipe that was close to the ceiling of the ship block, as it is illustrated in Figure 11.

Table 9 shows the obtained RSS values at the maximum reading distances for the evaluated tags at different reading angles. As it can be observed, Dura 600 and Fit 400, which were the tags that performed worse in the previous experiment, cannot be read continuously at the evaluated reading angles (note that the previous experiment was performed at a 90° angle but with the tag at a 1.5 m height). Tags with an adequate performance in the previous reading range test (i.e., Dura 1500 and Exo 800), also showed acceptable RSS values for their maximum reading distance (between 2.6 and 6 meters). However, it must be noted that all tags obtained

TABLE 9. RSS values (in dBm) and maximum reading distances for the evaluated tags at different reading angles inside the ship block.

Reading Angle \ Tag model	Exo 600	Adept 850	Exo 750	Exo 800	Adept 360	Dura 1500	Dura 3000	Dura 600	Fit 400
0°	5 m | -63	1.9 m | -60	5.5 m | -60	5.5 m | -71	2.2 m | -72	3.7 m | -75	2.3 m | -67	X	X
45°	5.2 m | -50	0.8 m | -54	5.3 m | -67	4.9 m | -64	3.5 m | -71	6 m | -76	4.5 m | -66	X	X
90°	4 m | -63	0.7 m | -60	2.9 m | -63	2.9 m | -66	3.3 m | - 64	4.5 m | -75	3.6 m | -60	X	X
135°	4.4 m | -65	0.6 m | -61	3.6 m | -64	2.6 m | -65	2.8 m | - 73	4.5 m | -75	4.2 m | -63	X	X
180°	5 m | -65	1.5 m | -58	5 m | -60	4 m | -67	5 m | -69	5 m | -75	2.8 m | -63	X	X

X (in red) means that no readings were received continuously at such a distance (i.e., in some cases a signal was collected sporadically, but due to temporary reflections). Green: good reading distance; yellow: sufficient but short reading distance for the scenario.

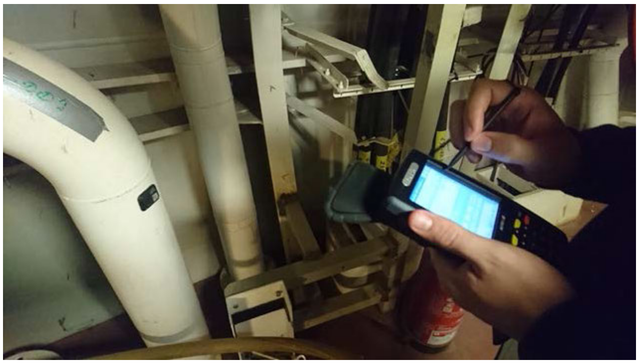


FIGURE 12. LoS scenario inside the OPV.

lower RSS values when modifying their reading angle respect to the optimal reading position (i.e., with the tag and the reader antennas in parallel (at 90°) and at the same height). Nonetheless, although different RSS values were obtained, all the selected tags except for Dura 600 and Fit 400 would be easily read in real-world conditions in the proposed scenario.

C. PASSIVE RFID PERFORMANCE INSIDE THE SHIP

The inner areas of the OPV have a higher density of metallic objects than the ship block (e.g., the floor is metallic, most of the equipment and pipes are already installed), so, in terms of electromagnetic propagation, it represents a tougher scenario than the ship block. The next subsections describe the experiments performed in such an environment, which were identical to the ones carried out in the ship block, but with distance restrictions (i.e., the elements mounted on the ship limited the distance at which tests can be performed) and with the presence of more metallic items.

1) MAXIMUM READING DISTANCE WITH LoS

For this set of tests, the evaluated tags were attached to a metallic pipe at a height of 1 m (as illustrated in Figure 12) and with LoS, in order to determine their maximum reading range in the proposed scenario.

Table 10 shows the obtained RSS values. Dura 600 and Fit 400 get similar results respect to the tests performed in the ship block. However, the rest of the tags reach the same or even longer reading distances. This gain may be surprising due to the complex communications scenario, but it is actually such a scenario, where signal reflections occur throughout the ship, which eventually increases reading distance. In contrast to the results obtained during the ship block tests, where the RSS values decreased in proportion to the reading range, inside the OPV there is not a clear correlation between RSS and distance, so the scenario makes it difficult to establish a mathematical model that relates tag location with RSS [7], [21]. A clear example can be observed with Exo 750: RSS is lower when reading the tag at 0.5 m than for larger distances due to the signal reflections that occur inside the ship.

The obtained larger reading distances may seem an advantage, but they can suppose a problem when trying to read a specific tag, since several of them might be read. Fortunately, in the developed Auto-ID system this potential issue can be easily solved: although the operator may read several tags at the same time, he/she can easily distinguish which is attached to an item, since the RFID reader software shows a picture and the characteristics of each object.

2) INFLUENCE OF THE TAG READING ANGLE

This set of experiments was performed in the scenario shown in Figure 13, where there is the same pipe density level than in the scenario described in the previous subsection, but it was modified the location of the tags to place them close to the ceiling, at a height of approximately 2 m. It must be noted that, inside the ship, the space in some of the compartments was limited, so reading distance was constrained by the characteristics of the area instead of by the selected RFID technology.

Table 11 shows the obtained results. The behavior of the different tags differs significantly with respect to the previous set of tests inside the ship. For instance, for the Exo 600 and Adept 850 their reading range was substantially reduced: while in the previous LoS scenario (where the tag was at a 1 m height) both tags could be read at 5 m, their maximum reading distance in the second set of tests did not reach 4 m at 90°. The rest of the tested tags, except for Dura 600 and Fit 400 (whose signal was not received for a distance of more than 0.5 m), show mostly lower RSS values than the ones obtained in Section VII-B.

Like in the LoS scenario, RSS fluctuations are noticeable, so it is not straightforward to determine a mathematical func-

TABLE 10. RSS values achieved (in dBm) with the different tags at different distances inside the OPV.

Tag model Reading Distance	Exo 600	Adept 850	Exo 750	Exo 800	Adept 360	Dura 1500	Dura 3000	Dura 600	Fit 400
0.5m	-49	-53	-63	-51	-68	-65	-60	X*	X**
1m	-47	-53	-54	-57	-69	-70	-67	X	X
2m	-53	-54	-55	-65	-68	-63	-60	X	X
3m	-53	-58	-60	-65	-72	-65	-64	X	X
4m	-62	-58	-63	-66	-71	-65	-64	X	X
5m	-59	-60	-68	-66	-70	-72	-65	X	X

X (in red): means that no continuous readings were obtained or when RSS values were collected sporadically. * Readings were obtained between 30-40 cm with an RSS value of -63. ** Readings were obtained between 30-40 cm with an RSS value of -55 (in dBm). Green: very good signal; yellow: good signal.

TABLE 11. RSS values achieved with the different tags at different distances and different reading angles inside the OPV.

Tag model Reading Angle	Exo 600	Adept 850	Exo 750	Exo 800	Adept 360	Dura 1500	Dura 3000	Dura 600	Fit 400
0°	3.6 m | -54	1.1 m |-60	6.9 m | -67	7 m | -64	4.3 m | -70	7.8 m | -77	6.1 m | -54	5 cm | -61	X
45°	3.7 m | -59	1.5 m | -59	4.3 m | -62	4.3 m | -67	4.3 m | -71	4.3 m | -73	4.3 m | -55	0.5 m | -62	0.3 m | -67
90°	3.25 m |-55	2 m | -61	3.8 m | -63	3.8 m | -63	2.9 m | -68	3.8 m | -65	3.8 m | -61	0.5 m | -63	0.4 m | -65
135°	3.1 m | -59	1.9 m | -62	4.3 m | -67	4.3 m | - 68	4 m | -64	4.3 m | -67	4.3 m | -64	0.2 m | -61	0.2 m | -63
180°	3 m | -58	1.1 m | -57	4 m | -67	4.4 m | -69	2.6 m | -70	4.4 m | -72	3.6 m | -68	5 cm | -62	0.1 m | -64

X (in red) means that no readings were received continuously at such a distance (i.e., in some cases a signal was collected sporadically, but due to temporary reflections). Green: good reading distance; yellow: sufficient but short reading distance for the scenario.

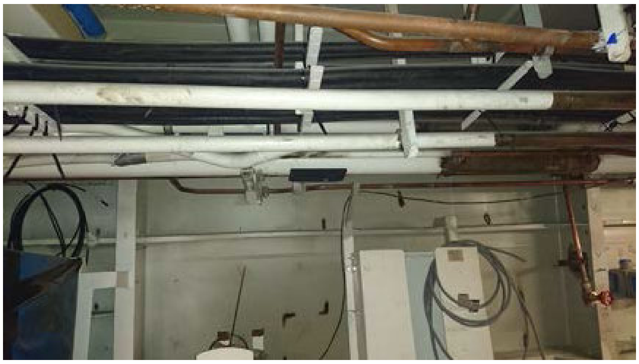


FIGURE 13. Testing of tag reading angles inside the OPV.

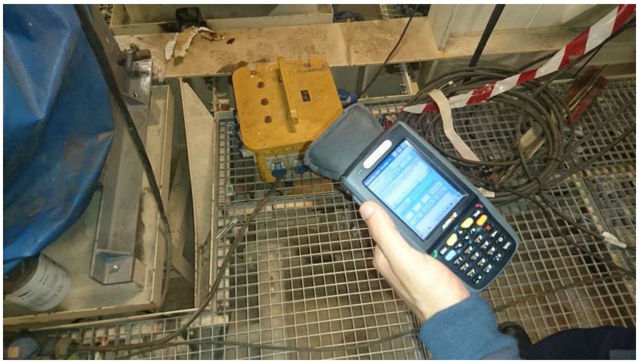


FIGURE 14. Tag reading in an area of very high density of metallic objects.

tion that takes the received signal level of a tag as an input and then returns as an output the estimated distance to the reader with a high level of precision. Nonetheless, it seems possible to stabilize the RSS by reducing noise (and, therefore, increase the accuracy) by exploiting spatial diversity techniques or by applying algorithms like Kalman filtering (such a stabilization is out of the scope of this paper, but the interested reader can find further information in [21]).

3) INSIDE THE OPV WITH A VERY HIGH DENSITY OF METALLIC OBJECTS

Figure 14 shows a picture of the selected scenario, where, as an example, a tag was located 0.5 m under a rack and the reader was at a 1.5 m height.

Table 12 shows the obtained RSS values. It can be observed that, except for Dura 600 and Fit 400, the tags could be read with high RSS values, ranging between -54 and -69 dBm, and with no significant oscillations.

D. ACTIVE RFID INSIDE THE OPV

In our previous article [7], tests were conducted with the selected active RFID reader by following a similar methodology to the one described in Section VII-B for measuring propagation loss with LoS in a shipyard workshop. Although the active RFID technology used in such an article was appropriate for a workshop scenario with real-time positioning requirements, it does not seem to be the optimal technology for identification, localization and traceability inside a ship, since, due to military restrictions, the selected active RFID tags should not be a source a potential electromagnetic communications interference or emit signals that can be detected by enemies when used for lifetime product traceability.

TABLE 12. RSS values achieved with the different tags under a very high density of metallic objects.

Tag model	Exo 600	Adept 850	Exo 750	Exo 800	Adept 360	Dura 1500	Dura 3000	Dura 600	Fit 400
RSS value	-60	-58	-69	-65	-68	-69	-54	X	X

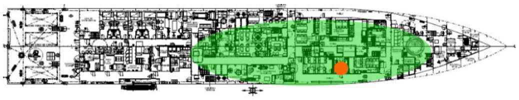


FIGURE 15. Blueprint of the OPV showing the active UHF RFID coverage (horizontal projection).

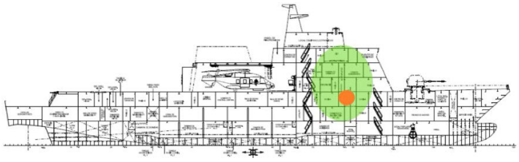


FIGURE 16. Blueprint of the OPV showing the active UHF RFID coverage (vertical projection).

In addition, active RFID is not usually recommended for tracking components in a ship during their lifetime, since tags rely on batteries. Nevertheless, a coverage test was performed to check if it would be possible to use the developed Auto-ID system for future use cases during the ship construction stage (e.g., for inventory tracking or asset management).

During these tests the active RFID reader remained in a static spot, in the dining room of the OPV. Then, an active RFID tag was moved throughout the ship to determine the coverage radius (e.g., the maximum reading distance inside the OPV for such a scenario). The obtained results are illustrated in Figures 15 and 16, which depict the horizontal and vertical projections of the blueprint of the ship, respectively. Such Figures include an orange circle that indicates where the active RFID reader was located and a green area that represents the area where the active RFID tag could be read continuously. Note that the total length of the OPV is around 90 m, the maximum breadth around 14 m and the design draught around 4 m, and, as it can be observed in Figures 15 and 16, the whole OPV could be covered by using a limited number of active RFID readers.

E. KEY FINDINGS

After analyzing the results obtained in the ship block and inside the OPV, it seems that passive UHF RFID system is suitable for traceability inside the ship, achieving a promising reading range and RSS values, even when the tags and the reader were surrounded by numerous metallic objects. However, it was clear that some of the tag models were not appropriate for the test scenarios due to their poor performance (e.g., Dura 600 and Fit 400). In addition, tags with better performance were, in certain scenarios, a worst fit in terms of usability (i.e., it was hard to attach them to certain pipes due to their physical characteristics). Furthermore, as it can be observed in Table 13, some of the claims of the manufacturer could not be corroborated in the evaluated empirical scenarios. Such claims affect Dura 600, Dura 3000 and Adept 360°. In the case of Dura 600, the expect reading range was supposed to reach 2.5 m when the tag was read with a handheld reader, but in the performed tests it could only be read up to 0.5 m (different tags of the same model were tested in case the first one was damaged, but yielded the same result). Regarding Dura 3000, it could be read up to roughly a 5 m distance in the ship block, but no farther, so in such a scenario it could not be obtained the maximum claimed 35 meter reading range or even a third of it. Finally, with respect to Adept 360°, it actually obtained a good reading range and angle results (up to 5 m in the ship block and a 0 to 180° reading angle), but it did not reach the claimed 10 meter reading distance.

The results of some of the passive RFID tags can be compared with the ones obtained in a shipyard workshop in [7]. Such a comparison is performed by means of Table 14, where the maximum reading distance results achieved in the two scenarios analyzed in this paper with the ones obtained in a shipyard pipe workshop in [7]. As it can be observed, for every tag, the maximum reading distance in the pipe workshop is equal or larger than in the ship block or inside the OPV. The most relevant differences occur with Exo 800 and Dura 1500, whose reading distance in the workshop triples and almost quadruples, respectively, the best reading distances obtained for the scenarios studied in this paper. This is due to the fact that the measurements carried out in the pipe workshop had LoS and barely any surrounding metallic objects that may impact signal propagation.

The results obtained in this article can also be compared with the ones shown in [7] regarding the impact of the reading angle of Dura 1500 and Exo 800, but considering that the measurement scenario described in [7] differs significantly. Specifically, in [7] it is obtained the maximum reading distance for the pipe workshop and when using two different antenna array configurations that made use of four antennas: in one configuration the four antennas were in parallel while in the other the antennas formed and 'L-shaped' array. Thus, Table 15 shows that the use of a linear array of directional antennas in the workshop scenario improves remarkably reading distance respect to when using a handheld reader, but only in the direction where the antenna array beam is pointing at, so, in contrast to the handheld reader, reading distance decreases significantly with reading angle. Such a decrease can be compensated with specific designs

TABLE 13. Validation of the manufacturer's claims on the features of the selected passive RFID tags.

Tag	Manufacturer's claim	Is it true for the ship block scenario?	Is it true for the OPV scenario?
Exo 600	Long reading distance (3 m with a handheld reader)	Yes	Yes
Exo 600	Broad reading angle when attached to metal bar	Yes	Yes
Exo 750	Broad reading angle	Yes	Yes
Exo 750	Well suited for being attached to metal assets	Yes	Yes
Exo 800	Long reading range (4 m with a handheld reader)	Yes	Yes
Exo 800	Optimized to read on, off, and near metal surfaces	Yes	Yes
Dura 600	Good on-metal performance (expected reading range: 2.5 m with a handhenld reader)	No	No
Dura 1500	Long range (7.5 m with a handheld reader)	Yes	Yes
Dura 1500	Suited for outdoor heavy industry deployments (e.g., container tracking for yard management, defense asset management or cargo tracking)	Yes	Yes
Dura 3000	Reaches reading ranges of up to 35 m, on, off or near metals	No	N/A (it could be read at the maximum tested reading distance)
Adept 360°	It has a 360°reading angle for the harshest environmental applications	Yes (for the tested for 0 to 180°)	Yes (for the tested 0 to 180°)
Adept 360°	Ideal for tracking slings, shackles and heavy machinery (10 m reading distance)	No	N/A (it could be read at the maximum tested reading distance)

TABLE 14. Maximum reading distance results compared to the ones obtained in a shipyard workshop in [7].

Tag	Ship Block	Inside the OPV	Pipe Workshop [7]
Fit 400	X	0.4 m	2 m
Exo 600	4 m	3.25 m	4 m
Exo 750	2.9 m	3.8 m	6 m
Exo 800	2.9 m	3.8 m	12 m
Dura 1500	4.5 m	3.8 m	15 m
Dura 3000	3.6 m	3.8 m	15 m
Dura 600	X	0.5 m	2 m
Adept 360°	3.3 m	2.9 m	11 m

of antenna arrays like the evaluated 'L-shaped' array, thus providing the handheld reader a good compromise between reading distance and angle for Dura 1500 and Exo 800, even in complex communications scenarios like the ship block or inside a warship.

In relation to the tests performed for this article, it is worth noting that additional challenges were detected for the deployment of an Auto-ID system inside a ship or ship block:

- The tags with the worst reading ranges required to hold the handheld reader in a non-comfortable way to collect readings. Therefore, if any of such tags is selected for a practical deployment, the positioning of the tags should be carefully considered to ease the operator work.
- Some of the tags, due to their form factor, were difficult to attach to the monitored pipes. Besides selecting the most appropriate tags, the Auto-ID system designer will have to determine which items should be monitored and whether it is worthy to tag certain small size or low value parts.
- As a general conclusion, it can be stated that some of the selected passive RFID tags can be used for implementing a traceability system for shipbuilding, but system designers should be aware of the issues that arise mainly inside a ship: reflections lead to larger-than-expected reading distances, which can suppose a problem when trying to read a specific tag, since several of them might be read simultaneously in spite of being scattered throughout nearby locations. In this situation, the Auto-ID system would need to implement disambiguation techniques, like only showing the tags with the highest RSS or, as it was implemented in the system presented in Section VII, the reader software can show a picture and the characteristics of the identified items.

With respect to the tested active RFID system, the reading distance was surprisingly high but, in contrast to other scenarios like workshops or the shipyard [182], its use for traceability in a ship in operation is unsuitable due to the reader deployment needs and potential electromagnetic interference caused by weapons, machinery or other ship's navigation,

TABLE 15. Maximum reading distance results at different angles compared to the ones obtained in a shipyard workshop in [7].

Reading Angle	Dura 1500 in Ship Block (with handheld reader)	Dura 1500 inside OPV (with handheld reader)	Dura 1500 inside Pipe Workshop (with Linear Antenna Array)	Exo 800 in Ship Block (with handheld reader)	Exo 800 inside OPV (with handheld reader)	Exo 800 inside Pipe Workshop (with Linear Antenna Array)	Exo 800 inside Pipe Workshop (with 'L-shaped' Antenna Array)
90°	4.5 m	3.8 m	15 m	2.9 m	3.8 m	12 m	7m
135°	4.5 m	4.3 m	4 m	2.6 m	4.3 m	4 m	6 m
180°	5 m	4.4 m	1 m	4 m	4.4 m	0.5 m	7 m

tactical or surveillance systems that operate at the same or near-by frequencies (e.g., active radar [183], [184]). Nevertheless, in a ship under construction, active RFID technology could be used for inventory purposes, to know in real-time whether an asset or product is inside a certain area. The active RFID results are in line with the ones specified by the manufacturer, around 90 m in a LoS scenario. In addition, such results can be compared with the ones previously obtained in a shipyard workshop in [7]: the maximum reading distance is similar to the one obtained in the workshop, where tags could be read 95% of the time at a distance of 100 m when using high-gain antennas. However, in [7] it was concluded that, the longer the distance, the less accurate the RSS-based distance estimations, so multi-antenna algorithms and Kalman filtering were needed to stabilize RSS and thus improve the accuracy of the positioning system.

Finally, it must be emphasized that the previous findings and conclusions are specific for the selected scenarios and for the purpose of technology validation, so future researchers should adapt the proposed methodology to their own scenarios and carry out an appropriate validation campaign on them.

VIII. CONCLUSION

This article described a methodology for analyzing, designing, implementing and validating Auto-ID solutions for Industry 5.0 scenarios. After reviewing the main characteristics and challenges of Industry 5.0, the proposed methodology was described and applied to the development of an Auto-ID system for identifying and keeping traceability of the components of a ship under construction, where supply chain traceability is a unique industrial challenge. First, the selected use case was defined and the specific operational and technical requirements were analyzed. Second, the communications architecture was detailed. Next, the article reviewed the most relevant Auto-ID and communications technologies that can be used for providing identification capabilities in Industry 5.0 applications. The proposed technologies were evaluated in order to select the most appropriate technology to cope with the requirements of the analysis stage. As a result, passive and active UHF RFID hardware and software components were selected, and the Auto-ID system was implemented and validated in an Offshore Patrol Vessel (OPV) under construction. The obtained results show that passive UHF RFID was appropriate for traceability applications, while active RFID can be used for inventory management. As a general conclusion it can be stated that, while the selection of the Auto-ID technology is highly dependent on the specific use case and technologies are rapidly evolving, the proposed methodology and empirical evaluations can ease the work of future developers and help them to design and implement future Industry 5.0 Auto-ID applications.

ACKNOWLEDGMENT

The authors would like to thank M. A. Díaz-Bouza, M. Suárez-Albela, and D. Noceda-Davila for their help during different stages of the proposed methodology.

REFERENCES

[1] European Commission, *Industry 5.0—Towards a Sustainable, Human-Centric and Resilient European Industry* Accessed: Jul. 17, 2021. [Online]. Available: https://ec.europa.eu/info/publications/industry-50_es

[2] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, "Smart factory of Industry 4.0: Key technologies, application case, and challenges," *IEEE Access*, vol. 6, pp. 6505–6519, 2018.

[3] P. Fraga-Lamas, T. M. Fernández-Caramés, O. Blanco-Novoa, and M. A. Vilar-Montesinos, "A review on industrial augmented reality systems for the Industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 13358–13375, 2018.

[4] A. W. Colombo, S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin, "Industrial cyberphysical systems: A backbone of the fourth industrial revolution," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 6–16, Mar. 2017.

[5] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure Industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019.

[6] P. Fraga-Lamas, L. Ramos, V. Mondéjar-Guerra, and T. M. Fernández-Caramés, "A review on IoT deep learning UAV systems for autonomous obstacle detection and collision avoidance," *Remote Sens.*, vol. 11, no. 18, p. 2144, Sep. 2019.

[7] P. Fraga-Lamas, D. Noceda-Davila, T. M. Fernández-Caramés, M. Díaz-Bouza, and M. Vilar-Montesinos, "Smart pipe system for a shipyard 4.0," *Sensors*, vol. 16, no. 12, p. 2186, Dec. 2016.

[8] Federal Ministry of Education and Research, Germany. *Industry 4.0: Project*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html

[9] Council for Science, Technology and Innovation, Government of Japan. (Dec. 18, 2015). *Report on The 5th Science and Technology Basic Plan*. Accessed: Jul. 28, 2021. [Online]. Available: https://www8.cao.go.jp/cstp/kihonkeikaku/5basicplan_en.pdf

[10] Directorate-General for Research and Innovation (European Commission), and J. Müller, *Enabling Technologies for Industry 5.0. Results of a Workshop With Europe's Technology Leaders*. Accessed: Jul. 17, 2021. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/8e5de100-2a1c-11eb-9d7e-01aa75ed71a1/language-en

[11] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.

[12] G. Aceto, V. Persico, and A. Pescapé, "A survey on information and communication technologies for Industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3467–3501, 4th Quart., 2019.

[13] X. Li, D. Li, J. Wan, A. V. Vasilakos, C.-F. Lai, and S. Wang, "A review of industrial wireless networks in the context of Industry 4.0," *Wireless Netw.*, vol. 23, no. 1, pp. 23–41, Jan. 2015.

[14] P. Fraga-Lamas, L. Castedo-Ribas, A. Morales-Méndez, and J. M. Camas-Albar, "Evolving military broadband wireless communication systems: WiMAX, LTE and WLAN," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, May 2016, pp. 1–8.

[15] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[16] J. C. Cano, V. Berrios, B. Garcia, and C. K. Toh, "Evolution of IoT: An industry perspective," *IEEE Internet Things Mag.*, vol. 1, no. 2, pp. 12–17, Dec. 2018.

[17] K. Ovsthus and L. M. Kristensen, "An industrial perspective on wireless sensor networks—A survey of requirements, protocols, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1391–1412, 3rd Quart., 2014.

[18] X. Li, D. Li, J. Wan, A. V. Vasilakos, C.-F. Lai, and S. Wang, "A review of industrial wireless networks in the context of Industry 4.0," *Wireless Netw.*, vol. 23, pp. 23–41, Jan. 2017.

[19] D. Christin, P. S. Mogre, and M. Hollick, "Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives," *Future Internet*, vol. 2, no. 2, pp. 96–125, Apr. 2010.

[20] C. Lu, A. Saifullah, B. Li, M. Sha, H. Gonzalez, D. Gunatilaka, C. Wu, L. Nie, and Y. Chen, "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1013–1024, May 2016.

[21] P. Fraga-Lamas, T. M. Fernández-Caramés, D. Noceda-Davila, and M. Vilar-Montesinos, "RSS stabilization techniques for a real-time passive UHF RFID pipe monitoring system for smart shipyards," in *Proc. IEEE Int. Conf. RFID (RFID)*, Phoenix, AZ, USA, May 2017, pp. 161–166.

[22] R. Y. Zhong, Q. Dai, T. Qu, G. Hu, and G. Q. Huang, "RFID-enabled real-time manufacturing execution system for mass-customization production," *Robot. Comput.-Integr. Manuf.*, vol. 29, no. 2, pp. 283–292, Apr. 2013.

[23] P. Fraga-Lamas and T. M. Fernández-Caramés, "Reverse engineering the communications protocol of an RFID public transportation card," in *Proc. IEEE Int. Conf. RFID (RFID)*, Phoenix, AZ, USA, May 2017, pp. 30–35.

[24] A. Seferagić, J. Famaey, E. De Poorter, and J. Hoebeke, "Survey on wireless technology trade-offs for the industrial Internet of Things," *Sensors*, vol. 20, no. 2, p. 488, Jan. 2020.

[25] Q. Wang and J. Jiang, "Comparative examination on architecture and protocol of industrial wireless sensor network standards," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2197–2219, 3rd Quart., 2016.

[26] R. Sanchez-Iborra and M. D. Cano, "State of the art in LP-WAN solutions for industrial IoT services," *Sensors*, vol. 16, no. 5, p. 708, May 2016.

[27] A. Faí na, D. Souto, A. Deibe, F. López-Pe na, R. J. Duro, and X. Fernández, "Development of a climbing robot for grit blasting operations in shipyards," in *Proc. IEEE Int. Conf. Robot. Automat. (ICRA)*, New York, NY, USA, May 2009, pp. 200–205.

[28] V. Prabakaran, A. V. Le, P. T. Kyaw, R. E. Mohan, P. Kandasamy, T. N. Nguyen, and M. Kannan, "Hornbill: A self-evaluating hydro-blasting reconfigurable robot for ship hull maintenance," *IEEE Access*, vol. 8, pp. 193790–193800, 2020.

[29] M. Y. Kim, K.-W. Ko, H. S. Cho, and J.-H. Kim, "Visual sensing and recognition of welding environment for intelligent shipyard welding robots," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, Takamatsu, Japan, Nov. 2000, pp. 2159–2165.

[30] A. Kuss, U. Schneider, T. Dietz, and A. Verl, "Detection of assembly variations for automatic program adaptation in robotic welding systems," in *Proc. 47st Int. Symp. Robot. (ISR)*, Munich, Germany, Jun. 2016, pp. 1–6.

[31] S. Mun, M. Nam, J. Lee, K. Doh, G. Park, H. Lee, D. Kim, and J. Lee, "Sub-assembly welding robot system at shipyards," in *Proc. IEEE Int. Conf. Adv. Intell. Mechtron. (AIM)*, Busan, South Korea, Jul. 2015, pp. 1502–1507.

[32] D. Lee, N. Ku, T.-W. Kim, J. Kim, K.-Y. Lee, and Y.-S. Son, "Development and application of an intelligent welding robot system for shipbuilding," *Robot. Comput.-Integr. Manuf.*, vol. 27, pp. 377–388, Apr. 2011.

[33] S. Kawakubo, A. Chansavang, S. Tanaka, T. Iwasaki, K. Sasaki, T. Hirota, H. Hosaka, and H. Ando, "Wireless network system for indoor human positioning," in *Proc. 1st Int. Symp. Wireless Pervas. Comput.*, Phuket, Thailand, Jan. 2006, pp. 1–6.

[34] T. Hirota, S. Tanaka, T. Iwasaki, H. Hosaka, K. Sasaki, M. Enomoto, and H. Ando, "Development of local positioning system using Bluetooth," in *Mechatronics for Safety, Security and Dependability in a New Era*, E. Arai and T. Arai, Eds. Amsterdam, The Netherlands: Elsevier, 2007, pp. 309–312, doi: 10.1016/B978-008044963-0/50063-1.

[35] C. Pérez-Garrido, F. J. González-Castaño, D. Chaves-Díeguez, and P. S. Rodríguez-Hernández, "Wireless remote monitoring of toxic gases in shipbuilding," *Sensors*, vol. 14, no. 2, pp. 2981–3000, Feb. 2014.

[36] J.-M. Yun and P. Park, "Development of industrial safety management system for shipbuilding industry using RFID/USN," in *Proc. 9th Int. Conf. Ubiquitous Intell., Comput. 9th Int. Conf. Autonomic Trusted Comput.*, Fukuoka, Japan, Sep. 2012, pp. 285–291.

[37] W.-S. Jung, T. H. Yoon, D. Seung Yoo, J. H. Park, and H.-K. Choi, "Limitation of LoRaWAN in the smart HSE system for shipbuilding and onshore plant," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DySPAN)*, Seoul, South Korea, Oct. 2018, pp. 1–2.

[38] J. Park, H. Kim, J. Yoon, H. Kim, C. Park, and D. Hong, "Development of an ultrasound technology-based indoor-location monitoring service system for worker safety in shipbuilding and offshore industry," *Processes*, vol. 9, no. 2, p. 304, Feb. 2021.

[39] Ó. Blanco-Novoa, T. M. Fernández-Caramés, P. Fraga-Lamas, and M. A. Vilar-Montesinos, "A practical evaluation of commercial industrial augmented reality systems in an Industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 8201–8218, 2018.

[40] M. A. D. A. Bichet, E. K. H. D. Freitas, R. S. Rocha, A. Nunez, G. N. Schroeder, R. A. P. D. Santos, and S. S. D. C. Botelho, "Utilization of hyper environments for tracking and monitoring of processes and supplies in construction and assembly industries," in *Proc. Symp. Comput. Autom. Offshore Shipbuilding*, Rio Grande, Brazil, Mar. 2013, pp. 81–86.

[41] D. D. Arumugam and D. W. Engels, "Characterization of RF propagation in helical and toroidal metal pipes for passive RFID systems," in *Proc. IEEE Int. Conf. RFID*, Las Vegas, NA, USA, Apr. 2008, pp. 269–276.

[42] K. V. S. Rao, S. F. Lam, and P. V. Nikitin, "UHF RFID tag for metal containers," in *Proc. Asia–Pacific Microw. Conf.*, Yokohama, Japan, Dec. 2010, pp. 179–182.

[43] S. Bovelli, F. Neubauer, and C. Heller, "Mount-on-metal RFID transponders for automatic identification of containers," in *Proc. Eur. Microw. Conf.*, Manchester, U.K., Sep. 2006, pp. 726–728.

[44] M. Heiss and R. Hildebrandt, "High-temperature UHF RFID sensor measurements in a full-metal environment," in *Proc. Smart SysTech Eur. Conf. Smart Objects, Syst. Technol.*, Nuremberg, Germany, Jun. 2013, pp. 1–5.

[45] P. Fraga-Lamas, T. M. Fernández-Caramés, D. Noceda-Davila, M. A. Díaz-Bouza, M. Vilar-Montesinos, J. D. Pena-Agras, and L. Castedo, "Enabling automatic event detection for the pipe workshop of the shipyard 4.0," in *Proc. 56th FITCE Congr.*, Sep. 2017, pp. 20–27.

[46] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and M. A. Díaz-Bouza, "A fog computing based cyber-physical system for the automation of pipe-related tasks in the Industry 4.0 shipyard," *Sensors*, vol. 18, no. 6, p. 1961, Jun. 2018.

[47] P. Fraga-Lamas, P. Lopez-Iturri, M. Celaya-Echarri, O. Blanco-Novoa, L. Azpilicueta, J. Varela-Barbeito, F. Falcone, and T. M. Fernández-Caramés, "Design and empirical validation of a Bluetooth 5 fog computing based industrial CPS architecture for intelligent Industry 4.0 shipyard workshops," *IEEE Access*, vol. 8, pp. 45496–45511, 2020.

[48] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and M. Vilar-Montesinos, "A fog computing and cloudlet based augmented reality system for the Industry 4.0 shipyard," *Sensors*, vol. 18, no. 6, p. 1798, Jun. 2018.

[49] *Microsoft HoloLens 2 Official Web Page*. Accessed: Jul. 18, 2021. [Online]. Available: https://www.microsoft.com/en-us/hololens

[50] A. Vidal-Balea, O. Blanco-Novoa, P. Fraga-Lamas, M. Vilar-Montesinos, and T. M. Fernández-Caramés, "Creating collaborative augmented reality experiences for Industry 4.0 training and assistance applications: Performance evaluation in the shipyard of the future," *Appl. Sci.*, vol. 10, no. 24, p. 9073, Dec. 2020.

[51] I. Froiz-Míguez, P. Fraga-Lamas, J. Varela-Barbeito, and T. M. Fernández-Caramés, "LoRaWAN and blockchain based safety and health monitoring system for Industry 4.0 operators," *Proceedings*, vol. 42, no. 1, p. 77, Nov. 2019.

[52] H. Kdouh, G. Zaharia, C. Brousseau, G. Grunfelder, H. Farhat, and G. E. Zein, "Wireless sensor network on board vessels," in *Proc. 19th Int. Conf. Telecommun. (ICT)*, Apr. 2012, pp. 1–6.

[53] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on human-centered IoT-connected smart labels for the Industry 4.0," *IEEE Access*, vol. 6, pp. 25939–25957, 2018.

[54] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas, and C. J. Escudero, "A plug-and-play human-centered virtual TEDS architecture for the web of things," *Sensors*, vol. 18, no. 7, p. 2052, 2018.

[55] M. Suárez-Albela, P. Fraga-Lamas, and T. M. Fernández-Caramés, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, Nov. 2018.

[56] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A practical performance comparison of ECC and RSA for resource-constrained IoT devices," in *Proc. Global Internet Things Summit (GIoTS)*, Bilbao, Spain, Jun. 2018, pp. 1–6.

[57] P. Stenumgaard, J. Chilo, J. Ferrer-Coll, and P. Ängskog, "Challenges and conditions for wireless machine-to-machine communications in industrial environments," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 187–192, Jun. 2013.

[58] R. Candell, C. Remley, J. Quimby, D. Novotny, A. Curtin, P. Papazian, G. Koepke, J. Diener, and M. Kashef, "Industrial wireless systems radio propagation measurements," NIST, Gaithersburg, MD, USA, NIST Tech. Note 1951, Jan. 2017. Accessed: Jul. 17, 2021, doi: 10.6028/NIST.TN.1951.

[59] *International Society of Automation (ISA) Standard. Wireless Systems for Industrial Automation: Process Control and Related Applications*, Standard ISA-100.11 A-2009, International Society of Automation (ISA), Research Triangle Park, NC, USA, 2009.

[60] M. Suárez-Albela, P. Fraga-Lamas, L. Castedo, and T. Fernández-Caramés, "Clock frequency impact on the performance of high-security cryptographic cipher suites for energy-efficient resource-constrained IoT devices," *Sensors*, vol. 19, no. 1, p. 15, Dec. 2018.

[61] P. O'Donovan, C. Gallagher, K. Bruton, and D. T. J. O'Sullivan, "A fog computing industrial cyber-physical system for embedded low-latency machine learning Industry 4.0 applications," *Manuf. Lett.*, vol. 15, pp. 139–142, Jan. 2018.

[62] Ó. Blanco-Novoa, P. Fraga-Lamas, M. A. Vilar-Montesinos, and T. M. Fernández-Caramés, "Creating the internet of augmented things: An open-source framework to make IoT devices and augmented and mixed reality systems talk to each other," *Sensors*, vol. 20, no. 11, p. 3328, Jun. 2020.

[63] E. Khorov, I. Levitsky, and I. F. Akyildiz, "Current status and directions of IEEE 802.11be, the future Wi-Fi 7," *IEEE Access*, vol. 8, pp. 88664–88688, 2020.

[64] *IEEE P802.11—TASK GROUP BF (WLAN SENSING) Official Web Page*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.ieee802.org/11/Reports/tgbf_update.htm

[65] B. S. Chaudhari, M. Zennaro, and S. Borkar, "LPWAN technologies: Emerging application characteristics, requirements, and design considerations," *Future Internet*, vol. 12, no. 3, p. 46, Mar. 2020.

[66] S. Farrell, *Low-Power Wide Area Network (LPWAN) Overview*, document RFC 8376, May 2018. Accessed: Jul. 17, 3032. [Online]. Available: https://rfc- editor.org/rfc/rfc8376.txt

[67] J. Sanchez-Gomez, D. G. Carrillo, R. Sanchez-Iborra, J. L. Hernandez-Ramos, J. Granjal, R. Marin-Perez, and M. A. Zamora-Izquierdo, "Integrating LPWAN technologies in the 5G ecosystem: A survey on security challenges and solutions," *IEEE Access*, vol. 8, pp. 216437–216460, 2020.

[68] S. S. Gornale and A. C. Nuthan, "QR code based randomized hybrid video encryption," in *Proc. Int. Conf. Energy, Commun., Data Anal. Soft Comput. (ICECDS)*, Aug. 2017, pp. 3104–3109.

[69] T. Ma, H. Zhang, J. Qian, X. Hu, and Y. Tian, "The design and implementation of an innovative mobile payment system based on QR bar code," in *Proc. Int. Conf. Netw. Inf. Syst. Comput.*, Jan. 2015, pp. 435–440.

[70] G.-J. Chou and R.-Z. Wang, "The nested QR code," *IEEE Signal Process. Lett.*, vol. 27, pp. 1230–1234, 2020.

[71] *ISO/IEC 18004:2015*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:18004:ed-3:v1:en

[72] V. Coksun, K. Ok, and B. Ozdenizci, *Near Field Communications: From Theory to Practice*, 1st ed. Hoboken, NJ, USA: Wiley, 2012.

[73] V. Gharat, E. Colin, G. Baudoin, and D. Richard, "Impact of ferromagnetic obstacles on LF-RFID based indoor positioning systems," in *Proc. IEEE Int. Conf. RFID Technol. Appl. (RFID-TA)*, Sep. 2017, pp. 284–289.

[74] *Information Technology—Radio Frequency Identification for Item Management—Part 2: Parameters for Air Interface Communications Below 135 kHz*, Standard ISO/IEC 18000-2:2009, 2009. Accessed: Jul. 17, 2021. [Online]. Available: https://www.iso.org/standard/46146.html

[75] X. Qing and Z. N. Chen, "Proximity effects of metallic environments on high frequency RFID reader antenna: Study and applications," *IEEE Trans. Antennas Propag.*, vol. 55, no. 11, pp. 3105–3111, Nov. 2007.

[76] *Information Technology—Radio Frequency Identification for Item Management—Part 3: Parameters for Air Interface Communications at 13,56 MHz*, Standard ISO/IEC 18000-3:2010, 2010. Accessed: Jul. 17, 2021. [Online]. Available: https://www.iso.org/standard/53424.html

[77] J. Virtanen, J. Virkki, L. Sydänheimo, M. Tentzeris, and L. Ukkonen, "Automated identification of plywood using embedded inkjet-printed passive UHF RFID tags," *IEEE Trans. Autom. Sci. Eng.*, vol. 10, no. 3, pp. 796–806, Jul. 2013.

[78] *Information Technology—Radio Frequency Identification for Item Management—Part 7: Parameters for Active Air Interface Communications at 433 MHz*, Standard ISO/IEC 18000-7:2014, 2014. [Online]. Available: https://www.iso.org/standard/57336.html

[79] V. Rajaram, Z. Qian, S. Kang, N. E. McGruer, and M. Rinaldi, "MEMS-based near-zero power infrared wireless sensor node," in *Proc. IEEE Micro Electro Mech. Syst. (MEMS)*, Jan. 2018, pp. 17–20.

[80] *IEEE Draft Standard for Health Informatics–Point-of-Care Medical Device Communications–Transport Profile–IrDA Based–Infrared Wireless*, document IEEE P1073.3.3/D8, Jul. 2003, pp. 1–74.

[81] J. Qi and G.-P. Liu, "A robust high-accuracy ultrasound indoor positioning system based on a wireless sensor network," *Sensors*, vol. 17, no. 11, p. 2554, Nov. 2017.

[82] C. Medina, J. C. Segura, and Á. D. la Torre, "Ultrasound indoor positioning system based on a low-power wireless sensor network providing sub-centimeter accuracy," *Sensors*, vol. 13, no. 3, pp. 3501–3526, Mar. 2013.

[83] S. Dantas, A. N. Barreto, L. Aguayo, A. J. Braga, L. S. Silva, and L. G. U. Garcia, "Simulation of IEEE 1902.1 (RuBee) protocol for communication with buried assets," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Oct. 2017, pp. 1–6.

[84] *IEEE Standard for Long Wavelength Wireless Network Protocol*, IEEE Standard 1902.1-2009, Mar. 31, 2009, pp. 1–35.

[85] L. Barbieri, M. Brambilla, A. Trabattoni, S. Mervic, and M. Nicoli, "UWB localization in a smart factory: Augmentation methods and experimental assessment," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–18, 2021.

[86] M. Li, H. Zhu, S. You, and C. Tang, "UWB-based localization system aided with inertial sensor for underground coal mine applications," *IEEE Sensors J.*, vol. 20, no. 12, pp. 6652–6669, Jun. 2020.

[87] *IEEE Standard for Information Technology–Local and Metropolitan Area Networks–Specific Requirements—Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN)*, IEEE Standard 802.15.3-2003, Sep. 29, 2003, pp. 1–360.

[88] *IEEE Draft Standard for Low-Rate Wireless Networks Amendment: Enhanced High Rate Pulse (HRP) and Low Rate Pulse (LRP) Ultra Wide-Band (UWB) Physical Layers (PHYs) and Associated Ranging Techniques*, Standard IEEE P802.15.4z/D07, Mar. 10, 2020, pp. 1–171.

[89] *UWB Alliance*. Accessed: Jul. 17, 2021. [Online]. Available: https://uwballiance.org

[90] J. Chen, B. Zhou, S. Bao, X. Liu, Z. Gu, L. Li, Y. Zhao, J. Zhu, and Q. Lia, "A data-driven inertial navigation/Bluetooth fusion algorithm for indoor localization," *IEEE Sensors J.*, early access, Jun. 15, 2021, doi: 10.1109/JSEN.2021.3089516.

[91] F. Demrozi, C. Turetta, F. Chiarani, P. H. Kindt, and G. Pravadelli, "Estimating indoor occupancy through low-cost BLE devices," *IEEE Sensors J.*, vol. 21, no. 15, pp. 17053–17063, Aug. 2021.

[92] G. Chen, X. Cao, L. Liu, C. Sun, and Y. Cheng, "Joint scheduling and channel allocation for end-to-end delay minimization in industrial WirelessHART networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2829–2842, Apr. 2019.

[93] D. Yang, J. Ma, Y. Xu, and M. Gidlund, "Safe-WirelessHART: A novel framework enabling safety-critical applications over industrial WSNs," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3513–3523, Aug. 2018.

[94] *Industrial Networks—Wireless Communication Network and Communication Profiles—WirelessHART*, document IEC 62591:2016, 2016. Accessed: Jul. 17, 2021. [Online]. Available: https://webstore.iec.ch/publication/24433

[95] Q. Han, P. Liu, H. Zhang, and Z. Cai, "A wireless sensor network for monitoring environmental quality in the manufacturing industry," *IEEE Access*, vol. 7, pp. 78108–78119, 2019.

[96] *IEEE Standard for Low-Rate Wireless Networks*, IEEE Standard 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015), Jul. 23, 2020, pp. 1–800.

[97] *Connectivity Standards Alliance (Previously ZigBee Alliance).* Accessed: Jul. 17, 2021. [Online]. Available: https://www.csa-iot.org

[98] E.-F. Luchian, A. Taut, I.-A. Ivanciu, G. Lazar, and V. Dobrota, "Z-wave-based vehicular blackbox with automatic emergency assistance," in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN)*, Jun. 2018, pp. 85–90.

[99] *Z-Wave Alliance*. Accessed: Jul. 17, 2021. [Online]. Available: https://z-wavealliance.org

[100] S. Khssibi, H. Idoudi, A. Van den Bossche, T. Val, and L. A. Saidane, "Presentation and analysis of a new technology for low-power wireless sensor network," in *Proc. Int. J. Digit. Inf. Wireless Commun.*, vol. 3, no. 1, pp. 75–86, 2013.

[101] A. Aijaz, "High-performance industrial wireless: Achieving reliable and deterministic connectivity over IEEE 802.11 WLANs," *IEEE Open J. Ind. Electron. Soc.*, vol. 1, pp. 28–37, 2020.

[102] A. Willig, M. Kubisch, C. Hoene, and A. Wolisz, "Measurements of a wireless link in an industrial environment using an IEEE 802.11-compliant physical layer," *IEEE Trans. Ind. Electron.*, vol. 49, no. 6, pp. 1265–1282, Dec. 2002.

[103] F. Tramarin, S. Vitturi, M. Luvisotto, and A. Zanella, "On the use of IEEE 802.11n for industrial communications," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1877–1886, Oct. 2016.

[104] C.-C. Li, V. K. Ramanna, D. Webber, C. Hunter, T. Hack, and B. Dezfouli, "Sensifi: A wireless sensing system for ultra-high-rate applications," *IEEE Internet Things J.*, early access, Jun. 14, 2021, doi: 10.1109/JIOT.2021.3089159.

[105] E. Khorov, A. Krotov, A. Lyakhov, R. Yusupov, M. Condoluci, M. Dohler, and I. Akyildiz, "Enabling the Internet of Things with Wi-Fi HaLow—Performance evaluation of the restricted access window," *IEEE Access*, vol. 7, pp. 127402–127415, 2019.

[106] M. F. Khan, G. Wang, M. Z. A. Bhuiyan, and K. Yang, "Toward Wi-Fi halow signal coverage modeling in collapsed structures," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2181–2196, Mar. 2020.

[107] E. Khorov, A. Lyakhov, I. Nasedkin, R. Yusupov, J. Famaey, and I. F. Akyildiz, "Fast and reliable alert delivery in mission-critical Wi-Fi HaLow sensor networks," *IEEE Access*, vol. 8, pp. 14302–14313, 2020.

[108] *IEEE Recommended Practice for Local and Metropolitan Area Networks—Part 19: Coexistence Methods for IEEE 802.11 and IEEE 802.15.4 Based Systems Operating in the Sub-1 GHz Frequency Bands*, IEEE Standard 802.19.3-2021, Apr. 26, 2021, pp. 1–79.

[109] R. Maldonado, A. Karstensen, G. Pocovi, A. A. Esswie, C. Rosa, O. Alanen, M. Kasslin, and T. Kolding, "Comparing Wi-Fi 6 and 5G downlink performance for industrial IoT," *IEEE Access*, vol. 9, pp. 86928–86937, 2021.

[110] *IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*, IEEE Standard 802.11ax-2021 (Amendment to IEEE Std 802.11-2020), May 19, 2021, pp. 1–767.

[111] S. Barker, D. Irwin, and P. Shenoy, "Pervasive energy monitoring and control through low-bandwidth power line communication," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1349–1359, Oct. 2017.

[112] *Insteon Official Webpage*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.insteon.com

[113] M. Ruta, F. Scioscia, E. D. Sciascio, and G. Loseto, "Semantic-based enhancement of ISO/IEC 14543-3 EIB/KNX standard for building automation," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 731–739, Nov. 2011.

[114] *KNX Association*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.knx.org/

[115] *Information Technology—Home Electronic Systems (HES) Architecture—Part 3-10: Wireless Short-Packet (WSP) Protocol Optimized for Energy Harvesting—Architecture and Lower Layer Protocols*, Standard ISO/IEC 14543-3-10:2012, 2012. Accessed: Jul. 17, 2021. [Online]. Available: https://www.iso.org/standard/59865.html

[116] F. D. Arcari, C. Costa, C. E. Pereira, J. C. Netto, G. Torres, M. Souza, and I. Müller, "Development of a WirelessHART–EnOcean adapter for industrial applications," in *Proc. 7th Brazilian Symp. Comput. Syst. Eng. (SBESC)*, Nov. 2017, pp. 181–186.

[117] *EnOcean Alliance*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.enocean-alliance.org

[118] H.-S. Kim, S. Kumar, and D. E. Culler, "Thread/OpenThread: A compromise in low-power wireless multihop network architecture for the Internet of Things," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 55–61, Jul. 2019.

[119] *IEEE Standard for Low-Rate Wireless Networks*, IEEE Standard 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015), Jul. 23, 2020, pp. 1–800.

[120] *Thread Group Official Webpage*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.threadgroup.org

[121] *OpenThread by Google*. Accessed: Jul. 17, 2021. [Online]. Available: https://openthread.io

[122] F. Lurz, T. Ostertag, B. Scheiner, R. Weigel, and A. Koelpin, "Reader architectures for wireless surface acoustic wave sensors," *Sensors*, vol. 18, no. 6, p. 1734, May 2018.

[123] D. Malocha, M. Gallagher, B. Fisher, J. Humphries, D. Gallagher, and N. Kozlovski, "A passive wireless multi-sensor SAW technology device and system perspectives," *Sensors*, vol. 13, no. 5, pp. 5897–5922, May 2013.

[124] C. Campbell, *Surface Acoustic Wave Devices and Their Signal Processing Applications*. Amsterdam, The Netherlands: Elsevier, 2012.

[125] M. Bouzidi, Y. Dalveren, F. A. Cheikh, and M. Derawi, "Use of the IQRF technology in Internet-of-Things-based smart cities," *IEEE Access*, vol. 8, pp. 56615–56629, 2020.

[126] *IQRF Alliance*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.iqrfalliance.org/index.php

[127] B. Al Nahas, A. Escobar-Molero, J. Klaue, S. Duquennoy, and O. Landsiedel, "BlueFlood: Concurrent transmissions for multi-hop Bluetooth 5—Modeling and evaluation," 2020, *arXiv:2002.12906*. [Online]. Available: http://arxiv.org/abs/2002.12906

[128] M. U. Sheikh, B. Badihi, K. Ruttik, and R. Jäntti, "Adaptive physical layer selection for Bluetooth 5: Measurements and simulations," *Wireless Commun. Mobile Comput.*, vol. 2021, Jan. 2021, Art. no. 8842919.

[129] *Bluetooth Special Interest Group (SIG) Official Website*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.bluetooth.com

[130] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs standards and supported mobility," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1561–1581, 2nd Quart., 2019.

[131] *DASH7 Alliance Official Website*. Accessed: Jul. 17, 2021. [Online]. Available: https://dash7-alliance.org

[132] *Information Technology—Radio Frequency Identification for Item Management—Part 7: Parameters for Active Air Interface Communications at 433 MHz*, Standard ISO/IEC 18000-7:2014, 2014. Accessed: Jul. 17, 2021. [Online]. Available: https://www.iso.org/standard/57336.html

[133] A. Ikpehai, B. Adebisi, K. M. Rabie, K. Anoh, R. E. Ande, M. Hammoudeh, H. Gacanin, and U. M. Mbanaso, "Low-power wide area network technologies for Internet-of-Things: A comparative review," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2225–2240, Apr. 2019.

[134] *Ingenu Official Webpage*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.ingenu.com/technology/rpma/

[135] D. Magrin, M. Capuzzo, A. Zanella, L. Vangelista, and M. Zorzi, "Performance analysis of LoRaWAN in industrial scenarios," *IEEE Trans. Ind. Informat.*, vol. 17, no. 9, pp. 6241–6250, Sep. 2021.

[136] *Lora Alliance Official Webpage*. Accessed: Jul. 17, 2021. [Online]. Available: https://lora-alliance.org/

[137] R. Ratasuk, N. Mangalvedhe, D. Bhatoolaul, and A. Ghosh, "LTE-M evolution towards 5G massive MTC," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2017, pp. 1–6.

[138] J. S. E, A. Sikora, M. Schappacher, and Z. Amjad, "Test and measurement of LPWAN and cellular IoT networks in a unified testbed," in *Proc. IEEE 17th Int. Conf. Ind. Informat. (INDIN)*, Helsinki, Finland, Jul. 2019, pp. 1521–1527.

[139] *Mioty Alliance Official Webpage*. Accessed: Jul. 17, 2021. [Online]. Available: https://mioty-alliance.com/

[140] A. S. Petrenko, S. A. Petrenko, K. A. Makoveichuk, and P. V. Chetyrbok, "The IIoT/IoT device control model based on narrow-band IoT (NB-IoT)," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, Saint Petersburg, Russia, Jan. 2018, pp. 950–953.

[141] *Waviot Official Webpage. NB-Fi Specification*. Accessed: Jul. 17, 2021. [Online]. Available: https://waviot.com/technology/nb-fi-specification/

[142] M. Kanj, V. Savaux, and M. L. Guen, "A tutorial on NB-IoT physical layer design," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2408–2446, 4th Quart., 2020.

[143] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.

[144] A. Lavric, A. I. Petrariu, and V. Popa, "Long range SigFox communication protocol scalability analysis under large-scale, high-density conditions," *IEEE Access*, vol. 7, pp. 35816–35825, 2019.

[145] *Sigfox Official Webpage*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.sigfox.com/en

[146] B. Buurman, J. Kamruzzaman, G. Karmakar, and S. Islam, "Low-power wide-area networks: Design goals, architecture, suitability to use cases and research challenges," *IEEE Access*, vol. 8, pp. 17179–17220, 2020.

[147] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 34–40, Sep. 2017.

[148] *Weightless SIG Official Webpage*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.openweightless.org/

[149] R. A. Abbas, A. Al-Sherbaz, A. Bennecer, and P. Picton, "A new channel selection algorithm for the weightless-n frequency hopping with lower collision probability," in *Proc. 8th Int. Conf. Netw. Future (NOF)*, London, U.K., Nov. 2017, pp. 171–175.

[150] R. Abbas, A. Al-Sherbaz, A. Bennecer, and P. Picton, "Collision evaluation in low power wide area networks," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Leicester, U.K., Aug. 2019, pp. 1505–1512.

[151] A. Hoeller, R. D. Souza, H. Alves, O. L. A. López, S. Montejo-Sanchez, and M. E. Pellenz, "Optimum LoRaWAN configuration under Wi-SUN interference," *IEEE Access*, vol. 7, pp. 170936–170948, 2019.

[152] *Wi-Sun Official Webpage*. Accessed: Jul. 17, 2021. [Online]. Available: https://wi-sun.org/

[153] F. Wang, W. Liu, T. Wang, M. Zhao, M. Xie, H. Song, X. Li, and A. Liu, "To reduce delay, energy consumption and collision through optimization duty-cycle and size of forwarding node set in WSNs," *IEEE Access*, vol. 7, pp. 55983–56015, 2019.

[154] G. Nastasia, M. Falzarano, A. Corucci, P. Usai, and A. Monorchio, "Channel characterization of wireless systems on board of ships by using an efficient ray-tracing," in *Proc. IEEE Int. Symp. Antennas Propag.*, Chicago, IL, USA, Jul. 2012, pp. 1–2.

[155] M. Cheffena, "Propagation channel characteristics of industrial wireless sensor networks [wireless corner]," *IEEE Antennas Propag. Mag.*, vol. 58, no. 1, pp. 66–73, Feb. 2016.

[156] W. Tu, H. Xu, Y. Xu, Q. Ye, and M. Shen, "Research on 2.4 GHz wireless channel propagation characteristics in a steel ship cabin," *Int. J. Antennas Propag.*, vol. 2021, pp. 1–12, Jan. 2021.

[157] X. Jiang, Z. Pang, M. Luvisotto, R. Candell, D. Dzung, and C. Fischione, "Delay optimization for industrial wireless control systems based on channel characterization," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5855–5865, Sep. 2020.

[158] B. D. Beelde, E. Tanghe, M. Yusuf, D. Plets, and W. Joseph, "Radio channel modeling in a ship hull: Path loss at 868 MHz and 2.4, 5.25, and 60 GHz," *IEEE Antennas Wireless Propag. Lett.*, vol. 20, no. 4, pp. 597–601, Apr. 2021.

[159] H. Kdouh, C. Brousseau, G. Zaharia, G. Grunfelder, and G. E. Zein, "Measurements and path loss models for shipboard environments at 2.4 GHz," in *Proc. 41st Eur. Microw. Conf. (EuMC)*, pp. 408–411, 2011.

[160] A. Alarifi, A. Al-Salman, A. Alsaleh, A. Alnafessah, S. Al-Hadhrami, M. A. Al-Ammar, and H. S. Al-Khalifa, "Ultra wideband indoor positioning technologies: Analysis and recent advances," *Sensors*, vol. 16, no. 5, p. 707, 2016.

[161] I. P. Guembe, P. Lopez-Iturri, H. Klaina, G. G. Ezker, F. S. D. J. Urdanoz, J. L. Z. Cestau, L. Azpilicueta, and F. Falcone, "Wireless characterization and assessment of an UWB-based system in industrial environments," *IEEE Access*, vol. 9, pp. 107824–107841, 2021.

[162] M. Beyer and D. Markus, "Ignition of explosive atmospheres by small hot particles: Comparison of experiments and simulations," *Sci. Tech. Energetic Mater.*, vol. 73, no. 1, pp. 1–7, 2012.

[163] E. L. Mokole, M. Parent, T. T. Street, and E. Tomas, "RF propagation on ex-USS shadwell," in *Proc. IEEE-APS Conf. Antennas Propag. Wireless Commun.*, Nov. 2000, pp. 153–156.

[164] X. H. Mao and Y. H. Lee, "UHF propagation along a cargo hold on board a merchant ship," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 22–30, Jan. 2013.

[165] T. M. Fernández-Caramés, "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020.

[166] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A study of LoRa: Long range & low power networks for the Internet of Things," *Sensors*, vol. 16, no. 9, p. 1466, Sep. 2016.

[167] A. Seferagic, E. D. Poorter, and J. Hoebeke, "Enabling wireless closed loop communication: Optimal scheduling over IEEE 802.11ah networks," *IEEE Access*, vol. 9, pp. 9084–9100, 2021.

[168] *A6-UHFLongRange*. Accessed: Jul. 17, 2021. [Online]. Available: http://www.nextpoints.com/es/productos-rfid/item/196-rugged-pda-a6-rfid-uhf.html

[169] *Omni-ID Products*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.omni-id.com/industrial-rfid-tags

[170] *Omni-ID Fit 400 Datasheet*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.omni-id.com/pdfs/Omni-ID_Fit_400_datasheet.pdf

[171] *Omni-ID Exo 600 Datasheet*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.omni-id.com/pdfs/Omni-ID_Exo_600_datasheet.pdf

[172] *Omni-ID Exo 750 Datasheet*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.omni-id.com/pdfs/Omni-ID_Exo_750_datasheet.pdf

[173] *Omni-ID Exo 800 Datasheet*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.omni-id.com/pdfs/Omni-ID_Exo_800_datasheet.pdf

[174] *Omni-ID Dura 600 Datasheet*. Accessed: Jul. 17, 2021. [Online]. Available: http://www.omni-id.com/pdfs/Omni-ID_Dura_600_datasheet.pdf

[175] *Omni-ID Dura 1500 Datasheet*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.omni-id.com/pdfs/Omni-ID_Dura_1500_datasheet.pdf

[176] *Omni-ID Dura 3000 Datasheet*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.omni-id.com/pdfs/Omni-ID_Dura_3000_datasheet.pdf

[177] *Omni-ID Adapt 360° Datasheet*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.omni-id.com/pdfs/Omni-ID_Adept_360_datasheet.pdf

[178] *Omni-ID Adapt 850 Datasheet*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.omni-id.com/pdfs/Omni-ID_Adept_850_datasheet.pdf

[179] *NPR ActiveTrack-2 New Edition*. Accessed: Jul. 17, 2021. [Online]. Available: http://www.nextpoints.com/es/productos-rfid/item/187-npr-active-track-2-new-edition.html

[180] *Active RuggedTag-175S*. Accessed: Jul. 17, 2021. [Online]. Available: http://www.nextpoints.com/es/productos-rfid/item/319-tag-rfid-activo-active-rugged-tag-175s.html

[181] *Navantia's Offshore Patrol Vessels*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.navantia.es/en/products-and-services/patrol-vessels/

[182] R. Candell, Y. Liu, M. Hany, and K. Montgomery, "Industrial wireless deployments in the navy shipyard," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Adv. Manuf. 300-9, Aug. 2020.

[183] H. Rong and M.-R. Chen, "Influence and countermeasures on the ship-borne communication equipment of naval field complex electromagnetic environment," in *Proc. 11th Int. Symp. Distrib. Comput. Appl. Bus., Eng. Sci.*, Oct. 2012, pp. 345–347.

[184] G. B. Tait and M. B. Slocum, "Electromagnetic environment characterization of below-deck spaces in ships," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 2008, pp. 1–6.

PAULA FRAGA-LAMAS (Senior Member, IEEE) received the M.Sc. degree in computer engineering from the University of A Coruña (UDC), in 2009, and the M.Sc. and Ph.D. degrees in the joint Mobile Network Information and Communication Technologies Program from five Spanish universities, University of the Basque Country, University of Cantabria, University of Zaragoza, University of Oviedo, and UDC, in 2011 and 2017, respectively, and the M.B.A. and master's degrees in business innovation management (Jean Monnet Chair in European Industrial Economics, UDC), and Corporate Social Responsibility (CSR) and social innovation (Inditex-UDC Chair of Sustainability). Since 2009, she has been with the Group of Electronic Technology and Communications (GTEC), Department of Computer Engineering, UDC. She has over 90 contributions in indexed international journals, conferences, and book chapters, and holds three patents. She has also been participating in over 30 research projects funded by the regional and national government as well as research and development contracts with private companies. She is actively involved in many professional and editorial activities, acting as a reviewer of more than 35 international journals, an advisory board member, a topic/guest editor of top-ranked journals, and a TPC member of international conferences. Her current research interests include mission-critical scenarios, Industry 5.0, the Internet of Things (IoT), cyber-physical systems (CPS), augmented reality (AR), fog and edge computing, blockchain and distributed ledger technology (DLT), and cybersecurity.

JOSÉ VARELA-BARBEITO received the M.Sc. degree in electrical engineering from the University Alfonso X El Sabio, in 2005. He started his professional career as an Electrical Engineer at Everis and then worked as a SAP Consultant for companies, such as Tecnocom and Altia. He currently works with the Department of Information Technologies, Navantia S. A., where he is also the Head Researcher of the Joint Research Unit Navantia-UDC in the line of Auto-ID for Intelligent Products, working in topics like the Internet of Things and RFID traceability systems. He is also the Co-ordinator of the Department of Systems Maintenance and he is responsible for the development of the control and communications architecture of the new plant of the shipyard.

TIAGO M. FERNÁNDEZ-CARAMÉS (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science from the University of A Coruña (UDC), Spain, in 2005 and 2011, respectively. Since 2005, he has been working with the Department of Computer Engineering, UDC: from 2005 to 2009, through different predoctoral scholarships and, in parallel, since 2007, as a Professor. He currently works as an Associate Professor of electronic technology with the UDC. In such fields, he has contributed to more than 100 papers for conferences, high-impact journals and books, as well as to six patents. His current research interests include the IoT/IIoT systems, RFID, wireless sensor networks, augmented reality, embedded systems, and blockchain, as well as the different technologies involved in the Industry 4.0 and 5.0 paradigms.