Enabling Technologies and Cyber-Physical Systems for Mission-Critical Scenarios

Author: Paula Fraga Lamas

Doctoral Thesis UDC / 2017

Advisor: Luis Castedo Ribas

Programa de Doutoramento en Tecnoloxías da Información
e Comunicacións en Redes Móbiles

UNIVERSIDADE DA CORUÑA

March 22, 2017
Universidade da Coruña
Faculty of Computer Science
Campus de Elviña s/n
15071 - A Coruña (Spain)

Dr. Luis Castedo Ribas

CERTIFICA

Que a memoria titulada:
"Enabling Technologies and Cyber-Physical Systems for Mission-Critical Scenarios"
foi realizada por Dña. Paula Fraga Lamas baixo a miña dirección no Departamento de Electrónica e Sistemas (Enxeñería de Computadores dende Abril 2017) da Universidade da Coruña e remata a Tese que presenta para optar ó grao de Doctor.

A Coruña, 22 de Marzo de 2017.

Asdo.: Dr. Luis Castedo Ribas
Director da Tese Doutoral
Catedrático de Universidade
Departamento de Electrónica e Sistemas
Universidade da Coruña

Tese doutoral: Enabling Technologies and Cyber-Physical Systems for Mission-Critical Scenarios

Autor: Dña. Paula Fraga Lamas

Director: D. Luis Castedo Ribas

Data de defensa:

Tribunal

Presidente: D. Félix Pérez Martínez

Vogal: D. José María Pousada Carballo

Secretario: D. José Daniel Pena Agras

To the Xiamen tiger

Acknowledgements

One looks back with appreciation to the brilliant teachers,
but with gratitude to those who touched our human feelings.
The curriculum is so much necessary raw material,
but warmth is the vital element for the growing plant and for the soul of the child.

Carl Gustav Jung

Research: a detailed study of a subject, especially in order to discover new information or reach a new understanding. I consider myself a Researcher. I am willing to learn and change the world. Curious and observant about everything, the necessity of investigating arose to demonstrate that knowledge could be used to do great things and develop new ideas, products or technologies. Thus, research aims to solve specific problems to improve society. It was this passion for wisdom and innovation which encouraged me to start this journey. The path to become a doctor has been long and hard, but also full of adventures and people to acknowledge. This is my short way to thank all those people who, in one way or another, helped me to achieve it.

This thesis would not have been possible without the effort of my advisor Dr. Luis Castedo. I would like to thank him for the opportunity of being a part of the GTEC group, for giving me the freedom to pursue my own ideas, and for encouraging my professional growth and being always available to guide me. His invaluable trust has contributed to the success of this research.

My sincere thanks to professors Dr. Miguel González, Dr. Carlos J. Escudero and Dr. Adriana Dapena who have supported my work in different research projects, both scientifically and financially.

During this journey, Dr. Tiago Fernández helped me reviewing absolutely every detail of the performed work. He had faith in my ideas and he supported absolutely all of my proposals, even some that can be categorized as 'risky' (although I prefer to call them disruptive and brave). From the personal point of view, I recognize that he is one of the most talented, passionate, well-organized and efficient person I have ever met,

and it is a pleasure to work with him. Furthermore, his commitment with excellence, teaching and technology transfer is remarkable.

I would also like to thank the members of the dissertation committee, as well as the external reviewers, for devoting their time and effort to evaluate the contents of this thesis. A sincerely thank also to Prof. Wolfgang Utschick (Signal Processing Group Technische Universität München, Germany), Dr. Martin Taranetz (Technische Universität Wien, Austria) and, specially, Prof. Markus Rupp (Technische Universität Wien, Austria) for complementing my training with their intensive signal processing and wireless communications courses.

Another person that deserves mention is Dr. José A. García; from the beginning he was always providing support. I always remember him working at the CITIC whatever the hour. A special gratitude for my lab mates. Thank you for make the GTEC Lab a place to spend lots of hours and enjoy. Not only did you help me with everything I needed, but you became an important part of my daily life. Among them, special thanks go to the colleagues with whom I shared/share projects: Dr. Pedro Suárez, a book of wisdom (literally); Ángel Carro, who is an excellent person ready to help whenever you may need him; Manuel Suárez because hard work can be fun, and it is a pleasure to collaborate with such an enthusiastic person; Diego Noceda, who keeps calm under any circumstance, and Dr. José Rodríguez Piñeiro, who represents devotion for a job well-done. For instance, Dr. Óscar Fresnedo, although we did not collaborated yet in any project, he is sitting next to me, and has lost some of his personal space due to my belongings. I assume he does not care because he enjoys my conversation and we share a similar sense of humor.

I want to spread my gratefulness among the rest of the GTEC group. Hence, I give my very sincere thanks to Dr. Francisco J. Araújo, Dr. Julio C. Brégains, Dr. Paula Castro, Dr. Daniel I. Iglesia, Dr. José J. Lamas, Valentín Barral, Tomás Domínguez, Abraham Dopazo, Dr. José P. González and Adriano Todaro. I may also not forget to thank our former colleagues Dr. Josmary Labrador, Sonia Valiñas, Dr. Héctor Iglesias, Dr. Javier Rodas, Ismael Rozas, Néstor Coca, Belén Torrente, Santiago J. Barro and Fátima Armenteiros.

Moreover, I must express my appreciation to Cristina Ribao, whose help have been inestimable during the last years.

Likewise, I would not like to forget to mention my former colleagues of the CITIC (Lucía, Juan, Rubén, Sonia, Cris, Alberto, Jesús, Javi) and its staff. We always had interesting talks during lunch time and I really enjoyed trying to fix the world. Without forgetting to thank the cleaning ladies, Marisa (CITIC) and Miluca (AC), who were always taking care of me (and my plants).

Fortunately, the journey was full of distractions, and I want to acknowledge them. I owe a debt of gratitude to all the people that have walked with me during this period. Your encouraging and warm-hearted words were the best incentive to keep going. I am truly thankful to all my friends (Ana, Gabi, Noha, Leti, Mara, Fux, Maka...) for always bringing nothing but awesome moments to my life and their willingness to help me overcome difficult situations. Others who kept me out of the work, you have also done a good job.

All what I have done and all what I am would not be possible without all my family. They are absolutely essential in all the steps I followed. Specially, several are the reasons I want to express my gratitude to my parents: they raised me with love, taught me devotion, honesty, sense of responsibility, commitment, courage and perseverance, provided me with unfailing support throughout my years of study and through the process of writing this thesis, and they allowed me to be as ambitious as I wanted. They did not only encourage me to go along this path, but remained with me in tough moments. Moreover, they even did not complain much due to the amount of time that I did not visit them for being working.

A special mention goes to my sister. There is not a closer person than a sister. And there is no better sister than her. I trust her to make other's life better. Moreover, she just need to smile, because when she laughs is like sunshine, light comes out. She taught me that any project has to have a soul.

No one knows better than my boyfriend all the crazy ups and downs this journey has brought me. During these years, the best outcome was finding the best person to share my life with. Feelings are hardly described through words, I am grateful of his invaluable support and optimism and I am absolutely sure I could not have completed this work without him. Only one more thing to say to you: wanna bet? After this journey I will be looking for the next challenge. I hope we will enjoy it together.

Last, but not least, I would like to extend my gratitude to the many people who, although they are not cited, helped to bring this thesis to life.

Finally, the research work reported in this dissertation has been financed by the GTEC Group, the Department of Electronics and Systems; the human and material support of the University of A Coruña; grants by Xunta de Galicia (2007/000148-0, 2012/287, ED431C 2016-045 and CN 2012/211), project PRECODHARQ (09TIC008105PR) and the thematic network redTEIC (R2014/037); the Spanish Ministry of Industry, Tourism and Trade by the projects m:Vía 2009 (TSI-020301-2009-28) and PIRAmiDE (TSI-020301-2008-2); the Spanish Ministry of Science and Innovation by the projects COMONSENS (CSD2008-00010), COSIMA (TEC2010-19545-C04-01) and TECRAIL (IPT-2011-1034-370000); the Mixed Research Unit Navantia-UDC for the project 'The

Shipyard of the Future'; Ágata Technology S.L. for the project 'A Coruña's SmartPort: Monitoring subsystem and sustainable development', and 'Vigo's SmartPort: Monitoring subsystem and sustainable development'; Indra Sistemas, S. A. for the projects 'MoWi Phase III: Evolution and enhancements of the Mobile WiMAX (MoWi) interface' and 'MoWi Phase II: Evolution and enhancements of the Mobile WiMAX (MoWi) interface', and ATOS Origin for the project 'Ciudad2020: Towards a new model of sustainable smart city' (IPT-20111006).

Paula Fraga Lamas

Sometimes fate is like a small sandstorm that keeps changing directions.
You change direction but the sandstorm chases you.
You turn again, but the storm adjusts.
Over and over you play this out, like some ominous dance with death just before dawn.
Why? Because this storm isn't something that blew in from far away,
something that has nothing to do with you.
This storm is you. Something inside of you.
So all you can do is give in to it, step right inside the storm, closing your eyes and plugging up your ears so the sand doesn't get in, and walk through it, step by step.
There's no sun there, no moon, no direction, no sense of time.
Just fine white sand swirling up into the sky like pulverized bones.
That's the kind of sandstorm you need to imagine.
And you really will have to make it through that violent, metaphysical, symbolic storm.
No matter how metaphysical or symbolic it might be, make no mistake about it:
it will cut through flesh like a thousand razor blades.
People will bleed there, and you will bleed too. Hot, red blood.
You'll catch that blood in your hands, your own blood and the blood of others.
And once the storm is over you won't remember how you made it through,
how you managed to survive.
You won't even be sure, in fact, whether the storm is really over.
But one thing is certain.
When you come out of the storm you won't be the same person who walked in.
That's what this storm's all about.

Haruki Murakami, Kafka on the Shore

Abstract

Reliable transport systems, defense, public safety and quality assurance in the Industry 4.0 are essential in a modern society. In a mission-critical scenario, a mission failure would jeopardize human lives and put at risk some other assets whose impairment or loss would significantly harm society or business results. Even small degradations of the communications supporting the mission could have large and possibly dire consequences.

On the one hand, mission-critical organizations wish to utilize the most modern, disruptive and innovative communication systems and technologies, and yet, on the other hand, need to comply with strict requirements, which are very different to those of non critical scenarios. The aim of this thesis is to assess the feasibility of applying emerging technologies like Internet of Things (IoT), Cyber-Physical Systems (CPS) and 4G broadband communications in mission-critical scenarios along three key critical infrastructure sectors: transportation, defense and public safety, and shipbuilding.

Regarding the transport sector, this thesis provides an understanding of the progress of communications technologies used for railways since the implantation of Global System for Mobile communications-Railways (GSM-R). The aim of this work is to envision the potential contribution of Long Term Evolution (LTE) to provide additional features that GSM-R would never support. Furthermore, the ability of Industrial IoT for revolutionizing the railway industry and confront today's challenges is presented. Moreover, a detailed review of the most common flaws found in Radio Frequency IDentification (RFID) based IoT systems is presented, including the latest attacks described in the literature. As a result, a novel methodology for auditing security and reverse engineering RFID communications in transport applications is introduced.

The second sector selected is driven by new operational needs and the challenges that arise from modern military deployments. The strategic advantages of 4G broadband technologies massively deployed in civil scenarios are examined. Furthermore, this thesis analyzes the great potential for applying IoT technologies to revolutionize modern warfare and provide benefits similar to those in industry. It identifies scenarios where defense and public safety could leverage better commercial IoT capabilities to deliver

greater survivability to the warfighter or first responders, while reducing costs and increasing operation efficiency and effectiveness.

The last part is devoted to the shipbuilding industry. After defining the novel concept of Shipyard 4.0, how a shipyard pipe workshop works and what are the requirements for building a smart pipe system are described in detail. Furthermore, the foundations for enabling an affordable CPS for Shipyards 4.0 are presented. The CPS proposed consists of a network of beacons that continuously collect information about the location of the pipes. Its design allows shipyards to obtain more information on the pipes and to make better use of it. Moreover, it is indicated how to build a positioning system from scratch in an environment as harsh in terms of communications as a shipyard, showing an example of its architecture and implementation.

Resumen

En la sociedad moderna, los sistemas de transporte fiables, la defensa, la seguridad pública y el control de la calidad en la Industria 4.0 son esenciales. En un escenario de misión crítica, el fracaso de una misión pone en peligro vidas humanas y en riesgo otros activos cuyo deterioro o pérdida perjudicaría significativamente a la sociedad o a los resultados de una empresa. Incluso pequeñas degradaciones en las comunicaciones que apoyan la misión podrían tener importantes y posiblemente terribles consecuencias.

Por un lado, las organizaciones de misión crítica desean utilizar los sistemas y tecnologías de comunicación más modernos, disruptivos e innovadores y, sin embargo, deben cumplir requisitos estrictos que son muy diferentes a los relativos a escenarios no críticos. El objetivo principal de esta tesis es evaluar la viabilidad de aplicar tecnologías emergentes como *Internet of Things* (IoT), *Cyber-Physical Systems* (CPS) y comunicaciones de banda ancha 4G en escenarios de misión crítica en tres sectores clave de infraestructura crítica: transporte, defensa y seguridad pública, y construcción naval.

Respecto al sector del transporte, esta tesis permite comprender el progreso de las tecnologías de comunicación en el ámbito ferroviario desde la implantación de *Global System for Mobile communications-Railways* (GSM-R). El objetivo de este trabajo es analizar la contribución potencial de *Long Term Evolution* (LTE) para proporcionar características adicionales que GSM-R nunca podría soportar. Además, se presenta la capacidad de la IoT industrial para revolucionar la industria ferroviaria y afrontar los retos actuales. Asimismo, se estudian con detalle las vulnerabilidades más comunes de los sistemas IoT basados en *Radio Frequency IDentification* (RFID), incluyendo los últimos ataques descritos en la literatura. Como resultado, se presenta una metodología innovadora para realizar auditorías de seguridad e ingeniería inversa de las comunicaciones RFID en aplicaciones de transporte.

El segundo sector elegido viene impulsado por las nuevas necesidades operacionales y los desafíos que surgen de los despliegues militares modernos. Para afrontarlos, se analizan las ventajas estratégicas de las tecnologías de banda ancha 4G masivamente desplegadas en escenarios civiles. Asimismo, esta tesis analiza el gran potencial de aplicación de las tecnologías IoT para revolucionar la guerra moderna y proporcionar

beneficios similares a los alcanzados por la industria. Se identifican escenarios en los que la defensa y la seguridad pública podrían aprovechar mejor las capacidades comerciales de IoT para ofrecer una mayor capacidad de supervivencia al combatiente o a los servicios de emergencias, a la vez que reduce los costes y aumenta la eficiencia y efectividad de las operaciones.

La última parte se dedica a la industria de construcción naval. Después de definir el novedoso concepto de Astillero 4.0, se describe en detalle cómo funciona el taller de tubería de astillero y cuáles son los requisitos para construir un sistema de tuberías inteligentes. Además, se presentan los fundamentos para posibilitar un CPS asequible para Astilleros 4.0. El CPS propuesto consiste en una red de balizas que continuamente recogen información sobre la ubicación de las tuberías. Su diseño permite a los astilleros obtener más información sobre las tuberías y hacer un mejor uso de las mismas. Asimismo, se indica cómo construir un sistema de posicionamiento desde cero en un entorno tan hostil en términos de comunicaciones, mostrando un ejemplo de su arquitectura e implementación.

Resumo

Na sociedade moderna, os sistemas de transporte fiables, a defensa, a seguridade pública e o control da calidade na Industria 4.0 son esenciais. Nun escenario de misión crítica, o fracaso dunha misión poñería vidas humanas en perigo e en risco outros activos cuxa deterioración ou perda prexudicaría significativamente á sociedade ou aos resultados dunha empresa. Mesmo pequenas degradacións nas comunicacións que apoian a misión poderían ter importantes e posiblemente terribles consecuencias.

Por unha banda, as organizacións de misión crítica desexan empregar os sistemas e tecnoloxías de comunicación máis modernos, disruptivos e innovadores e, con todo, doutra banda, deben cumprir requisitos estritos que son moi diferentes aos relativos a escenarios non críticos. O obxectivo principal desta tese é avaliar a viabilidade de aplicar tecnoloxías emerxentes como *Internet of Things* (IoT), *Cyber-Physical Systems* (CPS) e comunicacións de banda ancha 4G en escenarios de misión crítica en tres sectores clave de infraestrutura crítica: transporte, defensa e seguridade pública, e construción naval.

Respecto ao sector do transporte, esta tese permite comprender o progreso das tecnoloxías de comunicación no ámbito ferroviario dende a implantación de *Global System for Mobile communications-Railways* (GSM-R). O obxectivo deste traballo é analizar a contribución potencial de *Long Term Evolution* (LTE) para proporcionar características adicionais que GSM-R nunca podería soportar. Ademais, preséntase a capacidade da IoT industrial para revolucionar a industria ferroviaria e afrontar os retos actuais. Asemade, estúdanse con detalle as vulnerabilidades máis comúns dos sistemas IoT baseados en *Radio Frequency IDentification* (RFID), incluíndo os últimos ataques descritos na literatura. Como resultado, preséntase unha metodoloxía innovadora para realizar auditorías de seguridade e enxeñería inversa das comunicacións RFID en aplicacións de transporte.

O segundo sector elixido vén impulsado polas novas necesidades operacionais e os desafíos que xorden dos despregamentos militares modernos. Para afrontalos, analízanse as vantaxes estratéxicas das tecnoloxías de banda ancha 4G masivamente despregadas en escenarios civís. Asemade, esta tese analiza o gran potencial de aplicación das tecnoloxías IoT para revolucionar a guerra moderna e proporcionar beneficios similares

aos alcanzados pola industria. Identifícanse escenarios nos que a defensa e a seguridade pública poderían aproveitar mellor as capacidades comerciais de IoT para ofrecer unha maior capacidade de supervivencia ao combatente ou aos servizos de emerxencias, á vez que reduce os custos e aumenta a eficiencia e efectividade das operacións.

A última parte dedícase á industria de construción naval. Despois de definir o novo concepto de Estaleiro 4.0, descríbese en detalle como funciona un taller de tubaxe dun estaleiro e cales son os requisitos para construír un sistema de tubaxes intelixentes. Ademais, preséntanse os fundamentos para posibilitar un CPS para Estaleiros 4.0. O CPS proposto consiste nunha rede de balizas que continuamente recollen información sobre a localización da tubaxe. O seu deseño permite aos estaleiros obter máis información sobre a tubaxe e facer un mellor uso da mesma. Ademais, indícase como construír un sistema de posicionamento dende cero nunha contorna tan hostil en termos de comunicacións, amosando un exemplo da súa arquitectura e implementación.

Index

List of Figures

List of Tables

Chapter 1

Introduction

Recent advances in communications and information technologies provide the possibility of developing tiny devices with sensing, actuating, communications and computing capabilities. Such a combination creates intelligent devices that are able not only to monitor but also to interact with the surrounding environment. Moreover, the Internet is increasingly ubiquitous, allowing users to connect anytime and from everywhere, not only to other people, but also to objects embedded in the physical world. The common vision of such systems is usually associated with the concept of Internet of Everything (IoE), where everything can be connected anywhere and anytime.

Currently, the industrial and business sectors are leading the adoption of the Internet of Things (IoT). Businesses will spend $3 billion in the IoT ecosystem and deploy 11.2 billion devices by 2020, while customers will invest up to $900 million [1]. Moreover, the public sector is estimated to increase significantly its adoption and spend up to $2.1 billion and install 7.7 billion devices, being the second-largest adopter of IoT ecosystems, particularly in areas like smart cities [2, 3], energy management [4] and transportation [5]. Overall, the potential economic impact will be from $3.9 trillion to $11.1 trillion per year by 2025 [6].

IoT is a distributed system for creating value out of data. It enables heterogeneous physical objects to share information and coordinate decisions. The impact of IoT in the commercial sector results in significant improvements in efficiency, productivity, profitability, decision-making and effectiveness. Specifically, industrial IoT is transforming how products and services are developed and distributed, and how infrastructures are managed and maintained. IoT is also redefining the interaction between people and machines. From energy monitoring on a factory to tracking supply chains, industrial IoT optimizes the equipment performance and enhances the workers safety.

Up to now, IoT allows for more effective monitoring and coordination of manufacturing, supply chains, transportation systems, healthcare, infrastructure, security, operations,

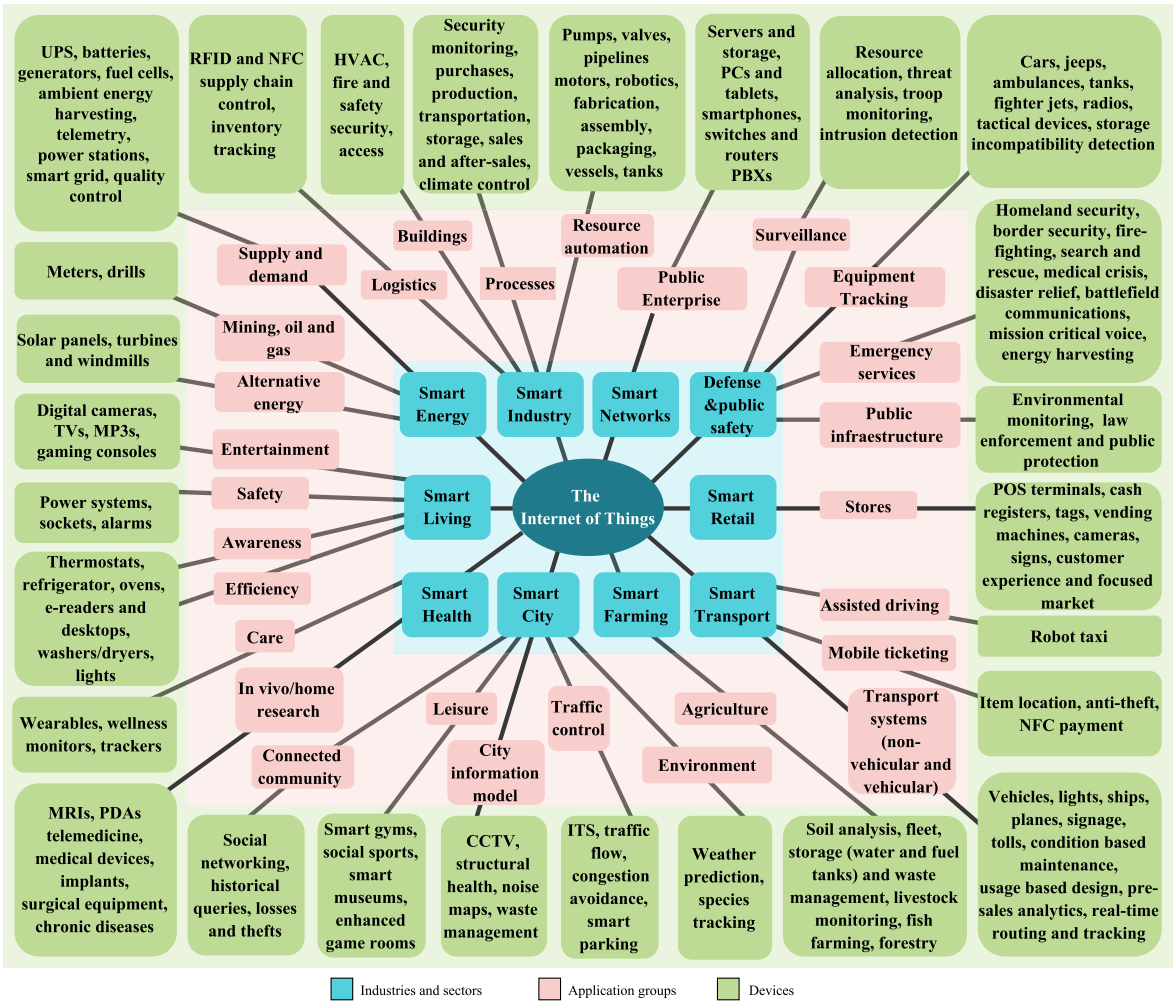


Figure 1.1: Proliferation of devices and applications in IoT.

and industrial automation, among other sectors and processes. In the near-future, IoT is expected to allow for the automation of everything around us. The proliferation of devices and its applications is illustrated in Figure 1.1. Regarding Machine-to-Machine (M2M) communications, traffic volume is expected to increase at an annual growth rate of 25 percent up to 2021. In total, in such a year there will be around 28 billion connected devices with more than 13.2 billion using M2M communications [7].

IoT represents the convergence of several interdisciplinary domains [8–12]: networking, embedded hardware, radio spectrum, mobile computing, communications technologies, software architectures, sensing technologies, energy efficiency, information management and data analytics. The rapid growth of IoT is driven by four key advances in digital technologies. The first one is the declining cost and miniaturization of ever more powerful microelectronic devices such as transducers (sensors and actuators), processing units (e.g., microcontrollers, microprocessors, SOCs (System-on-a-chip), FPGAs (Field-

Programmable Gate Array)) and receivers. The second factor is the fast pace and expansion of wireless connectivity. Furthermore, there is a need for radio technologies to comply with IoT device characteristics including suitability for deployment, battery-operated devices, form factors or coverage, among others. Furthermore, communications protocols need to adapt to IoT service requirements for real-time and mission-critical applications. As a consequence, there is a need for smart radio technologies that support low-power and ultra-low power operation, multiple communication ranges or diverse services ranging from telemetry to HD video streams for surveillance both in indoor and outdoor environments. It can be predicted that several wireless technologies like Bluetooth Low Energy (BLE), Zigbee, 6LowPAN, Z-Wave and Wi-Fi HaLow will continue to emerge as short range and low-power wireless communications technologies. For instance, with the fast pace of broadband networks like Worldwide Interoperability for Microwave Access (WiMAX), Long Term Evolution (LTE) and Wireless-Fidelity (Wi-Fi), IoT will be able to offer ubiquitous services.

The third is the expansion of data storage and the processing capacity of computational systems. Finally, the fourth one is the advent of innovative software applications and analytics, including advancements in machine-learning techniques for big data processing. These four drivers are present in the layers of the IoT technology stack. IoT devices transmit data over a wired or wireless communication network to servers and computers that store and process data using software applications and analytics. The knowledge gleaned from the analysis can be used for fault detection, control, prediction, monitoring, and optimization of processes and systems.

As demonstrated along this thesis, IoT technologies have the potential to increase tactical efficiency, effectiveness, safety and deliver immense cost savings in the long-term in mission-critical scenarios like transportation, defense and public safety, and the shipbuilding industry. For instance, these technologies can help the military to adapt to a modern world in which adversaries are located in more sophisticated and complex suburban scenarios (smart cities), or to equip the workforce of a Shipyard 4.0 to enhance their safety and productivity.

Cyber-physical Systems (CPSs) have emerged from the integration of embedded computing devices and smart physical environments deployed through a communication infrastructure. These include systems such as smart cities, factories or even defense. CPSs need to rely on IoT architectures and protocols that ease collecting and processing large data, and support complex processes to control such systems at different scales, from local to global. The large-scale nature of IoT-enabled CPSs create challenges ranging from management to security. Among the different technologies to perform identification in novel CPSs, RFID is currently one of the best positioned since it has been proven successful in multiple practical applications.

An important challenge for CPS is the availability of reliable communications system that fit with the different requirements of the different CPS applications. Hence, CPSs require communications networks characterized by bounded time delay and packet loss to perform its function properly. In this context, the LTE standard represents a promising enabler technology to realize CPS. IoT provides a basic platform for connecting all CPS, and CPS cooperate seamlessly with real and virtual spaces to make the paradigm of Industry 4.0 possible. Therefore, it can be definitely stated that there is no CPS without IoT, and no Industry 4.0 without CPS and IoT.

1.1 Mission-critical scenarios

A mission-critical scenario refers to systems, infrastructures, assets, networks (whether physical or virtual) and operations that are absolutely necessary for an organization to achieve its mission. These resources constitute an essential part of the processes needed to perform their intended function. Because any of these elements can fail due to attacks, improper design, environmental factors, physical defects or operator errors, countermeasures should be devised to continue operation when key resources become unavailable. Each organization defines the meaning of mission-critical based on its needs. For a private enterprise, mission-critical may be synonymous of business goals where a failure might cause a very high cost loss. In the case of a public agency (governments and states), it may take various contexts but all of them might be associated with public safety goals, meaning that their incapability or destruction will have a weaken effect on security, society, economy, public health or safety, or any combination thereof. Therefore, the mission-critical definition can also differ in scope. For example, in a manufacturing operation, it might be associated with its production goals.

Surprisingly, the identification of organization mission-critical systems is not evident in some sectors. The complexity created by the interdependence of systems, can make it difficult to determine which systems and processes are actually critical to the mission. Defining mission criticality requires the identification of the impact that a particular system has on overall mission success, specifying the proper scenarios and the corresponding operational and technical requirements. The main system requirements analyzed in this dissertation can be seen in Figure 1.2.

Furthermore, mission resilience is defined as a multi-tiered, life-cycle focused methodology for understanding, anticipating and minimizing the effects of any disruption. This model focuses on the efficiency of a mission both during normal operations and disruptive events. Unlike disaster recovery planning, mission resilience is a proactive approach that systematically prepares a system for potential disruptions as opposed to waiting for a disruptive event to occur. Therefore, achieving mission assurance means

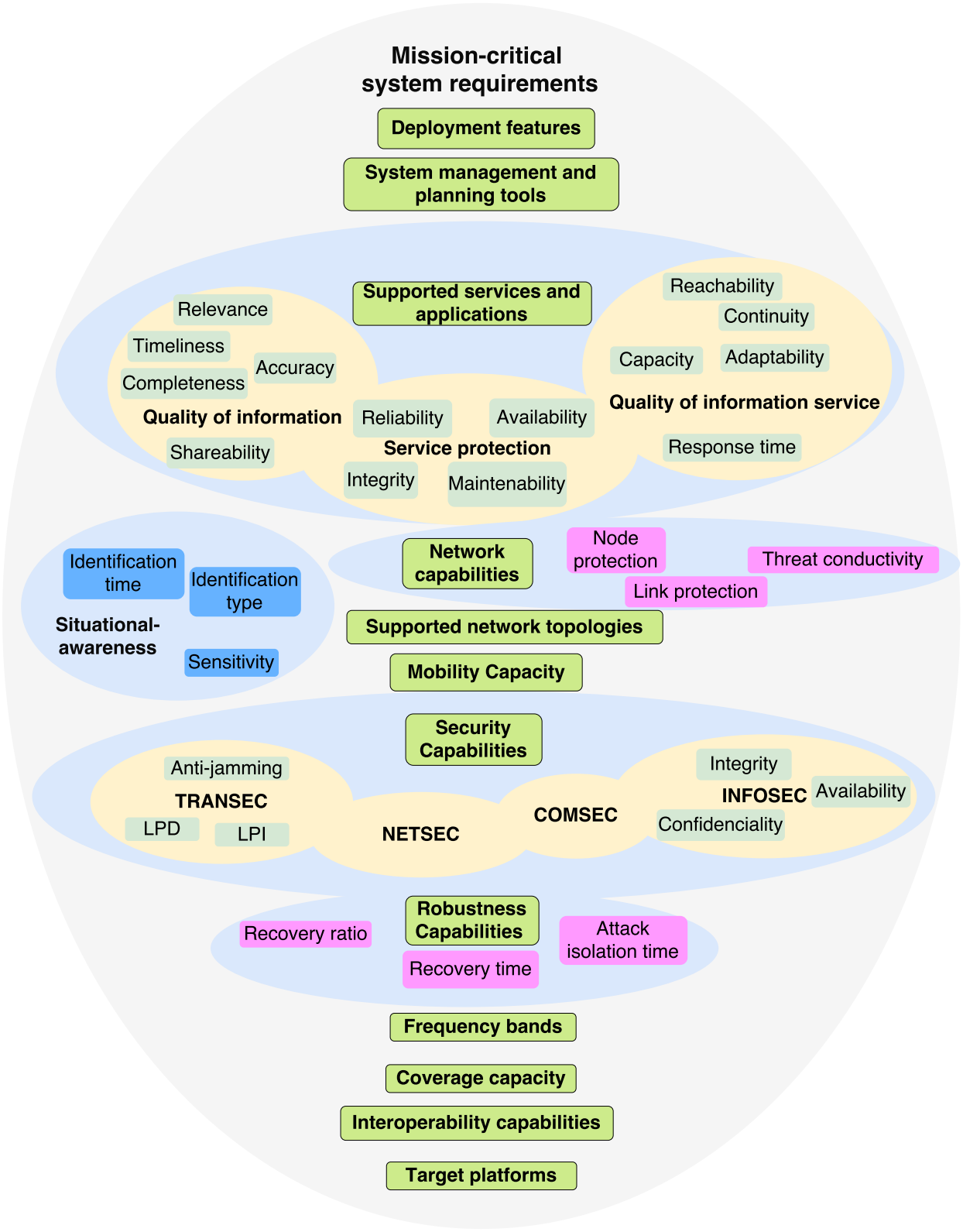


Figure 1.2: Mission-critical system requirements.

Figure 1.3: Navantia considers security and safety of all workers as the first criterion to take into account in the development of its activities.

that mission owners/operators have a degree of confidence that their mission-critical systems will be capable of sustaining necessary operational parameters despite any degradation. For example, a mission-critical system must operate despite sustained attacks throughout the mission cycle which, in the case of military systems, can range from hours to days.

Today, mission-critical scenarios play an increasingly important role in promoting social progress, greatly improving productivity whilst directly related to people's livelihood and national security. Due to their growing number and complexity, it is necessary to devote efforts to evaluate whether a mission-critical scenario can withstand attacks and keep its core missions working, and which is the best way to design and implement them. Furthermore, relying on the continuous development of information technologies, wireless communications, IoT and CPS systems, the constructing model of the mission-critical system is transforming from 'platform-centric, function-oriented' to 'network-centric, service-oriented', along with huge changes in technical systems.

Examples of known mission-critical systems are Supervisory Control and Data Acquisition (SCADA), air traffic control, and numerous systems that are widely used in military, energy, transportation and other national key areas. This dissertation provides notions to use enabling technologies for three mission-critical scenarios: transportation, defense and public safety, and the shipbuilding industry.

The railway sector is first analyzed, where communications are critical to the system operation and have stringent requirements for reliability and safety. Furthermore, rail networks have strict requirements for interoperability with legacy technology and long

life cycle support. Second, transportation cards are analyzed because they have a direct influence on the work of thousands of technicians and customers and, as a consequence, have strong requirements in terms of scalability, flexibility and security. Furthermore, among the major factors that influence the success of almost any smart card, in terms of being widely accepted, is the concept of trust. It is crucial that the card issuer is considered as a trusted entity to ensure that only trusted and authorized personnel have access to data.

Certainly, defense and public safety are the main critical sectors to be analyzed. Security and reliable communications are fundamentally important. Furthermore, one of the key factors for mission success within an emergency and crisis intervention, as well as in military operations, is the availability of a detailed Common Operational Picture (COP) at any point in time, also denoted by the term situational awareness. The essential benefits of a precise and reliable location have led to a significant demand for such CPS systems, among first responders, and also in the military domain.

These requirements can also be extended to the shipbuilding industry where business cannot afford significant operational downtime due to disruptions. The application of the principles of Industry 4.0 to shipyards is leading to the creation of Shipyards 4.0. Due to this, Navantia, one of the 10 largest shipbuilders in the world, is updating its whole inner workings to keep up with the near-future challenges that a Shipyard 4.0 will have to face. Such challenges can be divided into three groups: the vertical integration of production systems, the horizontal integration of a new generation of value creation networks, and the re-engineering of the entire production chain, making changes that affect the entire life cycle of each piece of a ship. Furthermore, its main concern is to consider the security and safety of all workers (Figure 1.3). One of Navantia's main business assets are pipes, which exist in a huge number and varied typology on a ship, and its monitoring constitutes a prospective CPS. Their improved identification, traceability and indoor location, from production and through their life, enhances shipyard productivity and safety.

1.2 Main contributions of this thesis

The main original contributions derived from this thesis can be summarized as follows:

- Analysis of the state-of-the-art regarding IoT, CPS and wireless communications in mission-critical environments like transportation, defense and shipbuilding industry.

- Study of the specific characteristics of railway communications. Both the operational requirements and the services needed are introduced. The feasibility of LTE and IoT to support such services is analyzed.

- Review of the most common flaws and latest attacks of RFID-based IoT systems. Formulation of a novel methodology to reverse engineer and audit security on commercial tags for RFID-based IoT applications. Security evaluation of a real-world transport tag using the latest RFID security tools (Proxmark 3) and the methodology proposed.

- Analysis and definition of a Military Broadband Wireless Communication Systems (MBWCS) based on 4G communication technologies.

- Survey of the potential of IoT technologies to revolutionize modern warfare. Identification of scenarios in which defense and public safety could leverage better commercial IoT capabilities to deliver greater survivability to the warfighter or first responders while reducing costs and increasing operation efficiency and effectiveness.

- Critical review of the most relevant operational capabilities (security, robustness, network topology, interoperability, among others), main tactical requirements and architectures, examining gaps and shortcomings in existing IoT systems across the military and the public safety fields.

- Definition of the novel concept of Shipyard 4.0. Description of how a shipyard pipe workshop works and the operational and technical requirements needed for building a smart pipe system.

- Development of a positioning system from scratch in an environment as harsh in terms of communications as a shipyard.

- Utilization of spatial diversity techniques to stabilize Received Signal Strength (RSS) values in RFID systems. Study on the performance of the real-time pipe monitoring CPS proposed by means of simulations and measurements.

1.3 Thesis overview

This thesis is structured in three parts around the key mission-critical infrastructure sectors selected: transportation, defense and public safety, and the shipbuilding industry. The first part of this thesis is devoted to analyzing transportation. It is covered by

Chapters 2-3. Chapter 2 provides first an understanding of the progress of communications technologies in the railway domain since the implantation of GSM-R. It describes the motivations for the different alternatives over time and the evolution of the railway requirements with their main specifications and recommendations. The aim of this work is to envision the potential contribution of LTE to provide additional features that GSM-R could never support. Furthermore, the ability of Industrial IoT for revolutionizing the industry and confront today's railway challenges is presented, jointly with the rise of the paradigm of Internet of Trains. For instance, current main industrial developments are described, exposing the main short and medium-term IoT-enabled services for smart railways.

Second, Chapter 3 focuses on evaluating the security of real-world transportation cards. It presents a detailed review of the most common flaws found in RFID-based IoT systems, including the latest attacks described in the literature. Next, a novel methodology that eases the detection and mitigation of such flaws is devised. Besides, after analyzing the latest RFID security tools, the methodology proposed is applied through one of them (Proxmark 3) to validate it.

The second part of this thesis analyzes the state-of-the-art of emerging technologies in defense and public safety. It is covered by Chapters 4-5. First, the strategic advantages of 4G broadband technologies massively deployed in civil scenarios are examined in Chapter 4. The analysis performed determines the technologies required in the middle and long term to comply with the operational requirements of the terrestrial army, and the state-of-the-art COTS military equipment that covers such needs. After the definition of the NATO scenarios, an analysis of the operational requirements is performed. In a second step, the technical requirements are derived and used as input for the applicability analysis of 4G WiMAX, LTE and Wi-Fi. Also, modifications and their related techniques are identified and evaluated for the three standards in order to design a novel Military Broadband Wireless Communication Systems (MBWCS).

Chapter 5 focuses on providing a holistic approach to IoT applied to defense and public safety. It presents a thorough study of the most relevant operational requirements for mission-critical operations, an overview of the key challenges, and the relationship between IoT and other emerging technologies. In order to perform the study, different relevant scenarios are proposed such as: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), fire-control systems, logistics (fleet management and individual supplies), smart city operations, personal sensing, soldier healthcare and workforce training, collaborative and crowd sensing, energy management, and surveillance. In addition to addressing various technical challenges, this work identifies vital areas of further research in the 2017-2020 timeframe.

The last part is devoted to shipbuilding industry. After defining the novel concept of Shipyard 4.0, Chapter 6 describes in detail how a shipyard pipe workshop works and what are the requirements for building a smart pipe system. Furthermore, it presents the foundations for enabling an affordable CPS for Shipyards 4.0. The CPS consists of a network of beacons that continuously collect information about the location of the pipes, its design allowed shipyards to have more information on the pipes and to make better use of it. Moreover, it indicates how to build a positioning system from scratch in an environment as harsh in terms of communications as a shipyard, showing an example of its implementation and the architecture that surrounds it.

Finally, Chapter 7 presents the main conclusions derived from this work and the proposed study lines to further continue it.

1.4 Participation in Research Projects

The research performed for this thesis has contributed to the following projects:

- Regional projects:
  - Grants awarded by Xunta de Galicia 2007/000148-0, 2012/287, ED431C 2016-045 and CN 2012/211.
  - PRECODHARQ project (09TIC008105PR).
  - redTEIC thematic network (R2014/037).
  - Mixed Research Unit Navantia-UDC with the project "The Shipyard of the Future" (IN853A 2015/01).
- National projects:
  - Ministry of Industry, Tourism and Trade: m:Vía 2009 (TSI-020301-2009-28) and PIRAmiDE (TSI-020301-2008-2).
  - Ministry of Science and Innovation: COMONSENS (CSD2008-00010), COSIMA (TEC2010-19545-C04-01) and TECRAIL (IPT-2011-1034-370000).
- Private collaborations:
  - Collaboration with Ágata Technology S.L. in the projects "A Coruña's SmartPort: Monitoring subsystem and sustainable development", and "Vigo's SmartPort: Monitoring subsystem and sustainable development".
  - Collaboration with Indra Sistemas, S. A. in the projects "MoWi Phase III: Evolution and enhancements of the Mobile WiMAX (MoWi) interface" and

"MoWi Phase II: Evolution and enhancements of the Mobile WiMAX (MoWi) interface".

– Collaboration with ATOS Origin in the project "Ciudad2020: Towards a new model of sustainable smart city" (IPT-20111006).

1.5 Authored publications

The contents of the thesis have been published in the following specialized journals and forums.

1.5.1 JCR Journals

1. Blanco-Novoa, O.; Fernández-Caramés, T. M.; Fraga-Lamas, P.; Castedo, L. An Electricity-Price Aware Open-Source Smart Socket for the Internet of Energy. *Accepted in Sensors.* **2017**. Impact factor 2015: 2.033 (Q1/T1 12/56 INSTRUMENTS & INSTRUMENTATION).

2. Fernández-Caramés, T. M.; Fraga-Lamas, P.; Suárez-Albela, M.; Castedo, L. Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications. *Sensors.* **2017**, *17*, 28. Impact factor 2015: 2.033 (Q1/T1 12/56 INSTRUMENTS & INSTRUMENTATION).

3. Pérez-Expósito, J. M.; Fernández-Caramés, T.M.; Fraga-Lamas, P.; Castedo, L. VineSens: An Eco-Smart Decision Support Viticulture System. *Sensors.* **2017**, *17*, 465. Impact factor 2015: 2.033 (Q1/T1 12/56 INSTRUMENTS & INSTRUMENTATION).

4. Fraga-Lamas, P.; Suárez-Albela, M.; Fernández-Caramés, T. M.; Castedo, L.; González-López, M. A Review on Internet of Things for Defense and Public Safety. *Sensors.* **2016**, *16*, 1644. Impact factor 2015: 2.033 (Q1/T1 12/56 INSTRUMENTS & INSTRUMENTATION).

5. Suárez-Albela, M.; Fraga-Lamas, P.; Fernández-Caramés, T.M.; Dapena, A.; González-López, M. Home Automation System Based on Intelligent Transducer Enablers. *Sensors.* **2016**, *16*, 1595. Impact factor 2015: 2.033 (Q1/T1 12/56 INSTRUMENTS & INSTRUMENTATION).

6. Fraga-Lamas, P.; Noceda-Davila, D.; Fernández-Caramés, T. M.; Díaz-Bouza, M.; Vilar-Montesinos, M. Smart Pipe System for a Shipyard 4.0. *Sensors.* **2016**, *12*, 2186. Impact factor 2015: 2.033 (Q1/T1 12/56 INSTRUMENTS & INSTRUMENTATION).

7. Suárez-Casal, P.; Carro-Lagoa, A.; García-Naya, J.A.; Fraga-Lamas, P.; Castedo, L.; Morales-Méndez, A. A Real-Time Implementation of the Mobile WiMAX ARQ and Physical Layer. *Journal of Signal Processing System.* **2015**, *78*, 283-297. Impact factor 2015: 0.508 (Q4/T3 212/255 ENGINEERING, ELECTRICAL & ELECTRONIC).

8. Carro-Lagoa, A.; Suárez-Casal, P.; García-Naya, J.A.; Fraga-Lamas, P.; Castedo, L.; Morales-Méndez, A. Design and Implementation of an OFDMA-TDD Physical Layer for WiMAX Applications. *EURASIP Journal on Wireless Communications and Networking.* **2013**, *2013*, 243. Impact factor 2013: 0.805. (Q3/T2 165/248 ENGINEERING, ELECTRICAL & ELECTRONIC).

1.5.2 SJR Journals

1. Fraga-Lamas, P.; Rodríguez-Piñeiro, J.; García-Naya, J.A.; Castedo, L. Unleashing the potential of LTE for next generation railway communications. In *Communication Technologies for Vehicles, Proceedings of the 8th International Workshop on Communication Technologies for Vehicles (Nets4Cars/Nets4Trains/Nets4Aircraft 2015))*, Sousse, Tunisia, 6–8 May 2015; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9066, pp. 153–164. Impact factor 2015: 0.252 (Q3/T2 COMPUTER SCIENCE (MISCELLANEOUS)).

1.5.3 International conferences

1. Fraga-Lamas, P.; Fernández-Caramés, Noceda-Davila, D.; Vilar-Montesinos, M. RSS Stabilization Techniques for a Real-Time Passive UHF RFID Pipe Monitoring System for Smart Shipyards. Accepted in 2017 IEEE International Conference on RFID (IEEE RFID 2017), Phoenix, AZ, USA, 9-11 May 2017.

2. Fraga-Lamas, P.; Fernández-Caramés, T. M. Reverse Engineering the Communications Protocol of an RFID Public Transportation Card. Accepted in 2017 IEEE International Conference on RFID (IEEE RFID 2017), Track: Protocols & Security, Phoenix, AZ, USA, 9-11 May 2017.

3. Fraga-Lamas, P.; Fernández-Caramés, Noceda-Davila, D.; Díaz-Bouza, M. A Real-Time Pipe Monitoring Cyber-Physical System for the Shipyard of the Future. Accepted in 2017 IEEE International Conference on RFID (IEEE RFID 2017), Phoenix, AZ, USA, 9-11 May 2017.

4. Fraga-Lamas, P.; Castedo-Ribas, L.; Morales-Méndez, A.; Camas-Albar, J.M. Evolving military broadband wireless communication systems: WiMAX, LTE and

WLAN. In Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 23–24 May 2016; pp. 1–8.

5. Carro-Lagoa, A.; Suárez-Casal, P.; Fraga-Lamas, P.; García-Naya, J.A.; Castedo, L.; Morales-Méndez, A. Real-time validation of a SDR implementation of TDD WiMAX standard. In Proceedings of the 2013 Wireless Innovation Forum European Conference on Communications Technologies and Software Defined Radio (SDR-WInnComm-Europe 2013), Munich, Germany, 11–13 June 2013.

6. Rodríguez-Piñeiro, J.; Fraga-Lamas, P.; García-Naya, J.A.; Castedo, L. Long term evolution security analysis for railway communications. In Proceedings of the IEEE Congreso de Ingeniería en Electro-Electrónica, Comunicaciones y Computación (ARANDUCON 2012), Asunción, Paraguay, 28–30 November 2012.

7. Fraga-Lamas, P.; Rodríguez-Piñeiro, J.; García-Naya, J.A.; Castedo, L. A survey on LTE networks for railway services. In Proceedings of the IEEE Congreso de Ingeniería en Electro-Electrónica, Comunicaciones y Computación (ARANDUCON 2012), Asunción, Paraguay, 28–30 November 2012.

1.5.4 National conferences

1. Suárez-Albela, M; Fraga-Lamas, P.; Fernández-Caramés, González-López, M. Sistema domótico con auto-configuración y auto-detección rápida de transductores. In Proceedings of the XXXI Simposium Nacional de la Unión Científica Internacional de Radio (URSI), Madrid, Spain, 5–7 September 2016.

2. Fraga-Lamas, P.; Castedo-Ribas, L.; Morales-Méndez, A.; Camas-Albar, J. M. Sistemas de comunicaciones militares de banda ancha basados en tecnologías inalámbricas 4G. In Proceedings of the DESEi+d 2015, III Congreso Nacional de I+D en Defensa y Seguridad, Pontevedra, Spain, 19–20 November 2015; pp. 925–932.

3. Fraga-Lamas, P.; Castedo-Ribas, L.; Morales-Méndez, A.; Camas-Albar, J.M. Estudio comparativo de aplicabilidad de tecnologías inalámbricas de banda ancha civiles en entornos militares. In Proceedings of the DESEi+d 2013, I Congreso Nacional de I+D en Defensa y Seguridad, Madrid, Spain, 6–7 November 2013; pp. 565–573.

4. Fraga-Lamas, P.; Camas, J.M.; Carro, A.; Suárez, P.; Castedo, L.; García-Naya, J.A.; Morales, A. Mobile WiMAX for next generation tactical wireless networks.

In Proceedings of the Information Systems Technology Panel Symposium on Emerged/Emerging 'Disruptive' Technologies (NATO IST-099 / RSY-024), Madrid, Spain, 9–10 May 2011.

1.5.5 Book chapters

1. Fernández-Caramés, T. M.; Fraga-Lamas, P.; Suárez-Albela, M.; Castedo, L. A methodology for evaluating security in commercial RFID systems. To be published in *Radio Frequency Identification*, 1st ed.; Crepaldi, P. C.; Pimenta, T. C.; INTECH: Rijeka, Croatia, 2017.

1.5.6 Technical reports

1. Camas-Albar, J.M.; Morales-Méndez, A.; Castedo-Ribas, L.; Fraga-Lamas, P.; Brown, C.; Tschauner, M.; Hayri-Kucuktabak, M. NATO Task Group ET-IST-068, IST (Information Systems Technology) panel of NATO STO (Science and Technology Organization). In *LTE vs. WiMAX for Military Applications*; Technical Report; North Atlantic Treaty Organization (NATO): Brussels, Belgium, 2015.

1.5.7 White papers

1. Fraga-Lamas, P.; Fernández-Caramés, T. M.; Carro-Lagoa, A.; Escudero-Cascón, C. J.; González-López, M. IPT-20111006, Project CIUDAD2020: A new smart city model that is ecologically and economically sustainable. *Estándares para interoperabilidad de redes de sensores: IEEE 1451 y Sensor Web Enablement (SWE)/ Standards towards interoperability of wireless sensor networks: IEEE 1451 and Sensor Web Enablement (SWE)*; White Paper; Innpronta Ciudad2020: Madrid, Spain, January 2014.

1.5.8 Patent applications

1. Suárez-Albela, M.; Fraga-Lamas, P.; Fernández-Caramés T.M., "Procedure, control system, node of transducers, computer program product to do, by a node transducers and/or part of a control system, that one or more transducers within the node accessible through a transducer network when the node is connected to the transducer network." Application number: P201300895, grant date: 4 May 2016. Spanish Patent and Trademark Office, National patent.

Chapter 2

Enabling Technologies for Smart Railways

2.1 Introduction

The future of railway industry is expected to rely upon smart transportation systems that leverage technologies over larger rail network infrastructure to reduce the life-cycle cost of the transport. New services, such as integrated security, asset management, and predictive maintenance, are expected to improve timely decision-making for issues like safety, optimal routes, scheduling, maintenance, and system capacity. Smart railways represent a combination of technological solutions, services, and components, as well as modern transportation infrastructure, such as automatic ticketing systems, digital displays, and smart meters. Likewise, these systems integrate software solutions to optimize the usage of assets, from tracks to trains, to meet the ever-growing demands for efficient, eco-friendly, and safer services.

The driving factors of the smart railways are expected to enforce the growth of the rail industry. These factors include the increasing importance of sustainability, government regulations, demographics (i.e., growing traffic of passengers and freight, aging population, and rapid urbanization), macroeconomics (i.e., limited public funding and governments' deficits, government initiatives and partnership models), microeconomics (i.e., price sensitivity, demands of an improved passenger experience, stakeholders interests), the growing interest in smart cities, the incredible pace of telecommunications and technological change, and the need for mobility.

The global smart railway market is estimated to grow from USD 10.50 bn in 2016 to USD 20.58 bn by 2021, at a Compound Annual Growth Rate (CAGR) of 14.4% [13]. Moreover, according to the International Transport Forum of the Organisation for Economic Co-operation and Development (OECD), by 2050, passenger mobility will

increase by 200-300% and freight activity by as much as 150-250% with respect to 2010 [14]. It is expected that these figures impact on each and every component of the value chain of the smart railway market, from passenger service to the back-end organization.

In addition, high-speed railway networks are extremely complex scenarios that have been promoted by many research initiatives, primarily aimed at fostering transportation quality. One of the strategic goals of high-speed rails focuses on the introduction of advanced broadband communications technologies that allow for improved services and that cope with market needs in a rapidly changing landscape.

Current railway communications technology was built in the beginning of the 90s, considering well-established mobile communication standards with potential to fulfill the requirements of railway services at that time [15]. After a preliminary study on the usability of Trans European Trunked RAdio (TETRA) and Global System for Mobile Communications (GSM), the latter was chosen because it was a proven technology in commercial use. Indeed, GSM Release 99 was standardized by European Telecommunications Standards Institute (ETSI) and it was well supported by its supplier association, the GSM Association (GSMA) Group. After extensive studies, Global System for Mobile Communications-Railways (GSM-R) was finally standardized by the Union Internationale des Chemins de Fer (UIC) and the European Railways. The European Integrated Railway Radio Enhanced NEtwork (EIRENE) project was launched in 1992 as an alliance between ETSI, railway operators, and telecommunications manufacturers. EIRENE's aim was to specify the functional and technical requirements for railway mobile networks. Two leading working groups were established within EIRENE for this task: a functional group and a project team. The functional group defined the Functional Requirements Specification (FRS), which mainly describes the mandatory features to ensure interoperability across borders. The project team determined the System Requirements Specification (SRS) based on the functional requirements. The SRS document defines the technical characteristics related to railway operation, thus identifying and specifying the additional Advanced Speech Call Items (ASCI) features [16].

A first draft of the EIRENE specifications was finalized in 1995, when the Mobile Radio for Railway Networks in Europe (MORANE) project was launched with the involvement of the UIC; the major railways in France, Italy and Germany; the European Commission, and a limited number of GSM suppliers. The objective of MORANE was to specify, develop, test, and validate prototypes of a new radio system, which should meet both functional and system requirement specifications. In 1997, the UIC prepared a Memorandum of Understanding (MoU) to enforce railway companies to only invest and cooperate in the implementation of GSM-R. This MoU was signed

in 1998 by 32 railways all over Europe, which increased up to 37 in 2009, including railways outside Europe. An Agreement on Implementation (AoI) came into effect in 2000 where the 17 signing railway companies stated their intention to begin national GSM-R implementation no later than 2003. From then on, GSM-R became the railway technology until now, when the rapid pace of commercial technologies are the driving force for further research on alternatives like Long Term Evolution (LTE).

The inception of smart railways began with the evolution of GSM-R, which is considered as the keystone of the rail industry transformation. Rail operators mainly use GSM-R for operational voice and data communications. Over a period of time, innovation in wireless communications technologies offered reliable transmission of video and data services for long distances. In the 2000s, the introduction of novel technological solutions and various digital devices projected new application areas, such as provision of information about the rails to passengers, the Communication-Based Trail Control (CBTC), rail traffic management systems, real-time passenger information systems, and Positive Train Control (PTC) solutions. However, the rail industry underwent a major revolution after 2005 with the introduction of Internet of Things (IoT) and the adoption of smart city projects, which led to the development of solutions such as smart ticketing, passenger infotainment, rail analytics, and dynamic route scheduling and planning. Industrial IoT-based solutions have eventually reinforced competitive advantages and have also uncovered new business models that are already impacting the global rail industry.

However, factors such as operational inefficiency, the lack of infrastructure and interoperability, high initial cost of deployment, and integration complexities over legacy systems and the network, may hinder the rail industry growth. Moreover, legacy infrastructure, aging communications systems, and the slow adoption of automation and protective technology in this mission-critical scenario pose enormous safety risks. Related with the issues of safety and connectivity is the matter of security. As rail systems rely more and more on wireless connectivity, they become more vulnerable to outside interference and intrusion. The consequences of even a small disruption become particularly severe as trains become more powerful, carry more passengers, and travel faster. Systems that are mission-critical for safe operation can be compromised by a simple electronic device or a small piece of malicious code. When passenger safety and lives are at stake, strong security becomes a fundamental requirement. Today, main challenges in enhancing rail transport can be summarized as:

- Increase efficiency and competitiveness: railways face ferocious competition from other modes (for example, the road sector offers attractive, cost-efficient, reliable, flexible, convenient door-to-door transport of freight and passengers across borders).

The challenge is further increased by a fragmented rail market, with numerous national systems for rail signaling and speed control operating in Europe. Thus, interoperability is a key challenge for free flow of rail traffic.

- Reduce rail noise and vibration, particularly in urban areas.

- Reduce greenhouse gas emissions. Although rail transport compares favorably to other transport means in terms of environmental impact, it can be further improved.

- Safety and security: rail safety in the European Union (EU) is among the highest in the world. Rail incidents (accidents, terrorism...) are not frequent and cause a relatively low share of deaths, but often involve a large number of people. To maintain and increase security, interoperable and harmonized safety standards for rolling stock and railways are required.

- Reduce operation and maintenance costs and increase the capacity of rail network.

This chapter provides an understanding of the progress of communications technologies in the railway domain since GSM-R. It describes the motivations for the different alternatives over time and the evolution of the railway requirements with its main specifications and recommendations. The aim of this work is to envision the potential contribution of LTE to provide additional features that GSM-R could never support, and the ability of Industrial IoT for revolutionizing the industry and confront today challenges.

This chapter is partly based on the publications [17–19] and is organized as follows. Section 2.2 provides a brief introduction of the main communications technologies used nowadays. Section 2.3 reviews GSM-R services in order to identify what is required to roll-out LTE to address specific requirements for railway communications services. The current status of LTE standardization is detailed in Section 2.4 in order to understand the evolution of the involved requirements and technologies. The advantages of the newest generation of communications systems for the railway environment are also explained. The strategic roadmap to ensure a smooth migration from GSM-R to LTE is described in Section 2.5. In Section 2.6, a formal analysis is introduced to study the feasibility of LTE for next generation railway networks. Section 2.7 describes the rise of industrial IoT and the paradigm of Internet of Trains. Furthermore, the main industrial developments are described. Section 2.8 reviews the main short and medium-term IoT-enabled services for smart railways. Finally, the last section is devoted to the conclusions and the future research lines.

2.2 Communications technologies for railways

Communications technologies in the railway sector are critical for the operation of the system and have strict requirements for reliability and safety [18]. This section reviews the main technologies that can be used to link the train to the Internet backbone and to provide Internet on-board.

Several technologies are embedded in the Train Access Terminal (TAT) to provide a continuous connection. The criteria to select a particular technology are typically the connection quality (i.e., the signal strength), delay, throughput, and cost. Two major families of technologies may be considered [20]:

- Satellite solutions. They can be based on different types of satellites (i.e., Geoestationary Orbit (GEO), Medium Earth Orbit (MEO), Low Earth Orbit (LEO)) with different frequency bands and that may provide unidirectional or bidirectional communications.

- Terrestrial. They can be divided into two main categories: (a) technologies that rely on existing networks (the so-called public cellular networks solutions), and (b) technologies that require the deployment of a specific ground infrastructure, dedicated train-to-infrastructure solutions: leaky coaxial cable, Wireless Fidelity (Wi-Fi), Worldwide Interoperability for Microwave Access (WiMAX), radio-over-Fiber, and optical solutions.

Nowadays, the most widely used communications system between trains and the elements involved in operation, control, and intercommunication within the railway infrastructure is GSM-R. It is in operation in 38 countries across the world, including all member states of the European Union and countries in Asia, America, and northern Africa. Two frequency bands were reserved by the ETSI for railway communications in Europe in 1995, which are 876-880 MHz (uplink) and 921-925 MHz (downlink). For each band, it is possible to allocate 19 subcarriers of 200 kHz, including a guard band. Each subcarrier supports 8 data or voice channels. The architecture of the GSM-R system is based on that of the GSM and can be subdivided into:

- Mobile Station (MS) subsystem: it enables the communication with the management team, the Radio Control Center (RCC), and between trains. It includes Mobile Radio Centers (MRCNs), which are basically the on-board radio equipments, as well as Portable Radio Centers (PRCNs), which are mobile devices.

- Base Station Subsystem (BSS): it is responsible for controlling the Base Transceiver Stations (BTSs).

- Network Switching Subsystem (NSS): it deals with tasks regarding call routing and control.
- The operation and management subsystem manages and controls the access to the resources and services provided by the network.

The GSM-R network is deployed forming elliptical cells along the tracks. BTS antennas are pointed to the tracks, where each cell is serviced by a single BTS with one antenna per direction. In case that stricter robustness requirements are imposed, a redundant strategy may be adopted. In such a situation, two independent layers of completely overlapped cells can be deployed. Generally, trains in one direction use one of the layers, whereas trains in the opposite direction use the other one. However, each layer is dimensioned to be able to transport all the traffic. Consequently, if there is a problem regarding one of the layers, the other one would be used. Coverage for tunnels whose length is smaller than 2 km is provided by external antennas, whereas radiating cable or repeaters are installed indoors for long tunnels.

There is a growing acknowledging that railway telecommunications will have to evolve to keep up with the rapid changes in technology. Hence, over the past few years, new technologies have been included by many railway operators, like WiMAX in Train-to-Wayside Communication (TWC) deployments, primarily as a means to deliver best-effort passenger Internet services [21]. In particular, the standard IEEE 802.16m has been backed up by market ecosystems. Wireless Local Area Network (WLAN)-based broadband capabilities have been used to deliver the most demanding train operation traffic but, until the IEEE 802.11ac amendment, the standard lacked Quality of Service (QoS) features such as end-to-end resource management, traffic admission, or traffic policy enforcement capabilities.

Several railway companies have established a quota system on the bandwidth used in order to limit the throughputs required. For instance, Amtrak has implemented a rate limiting on all US east coast and mid west services in March 2014: passengers are allowed for consuming up to 250 MB of data. Once exceeded, their data transfer rate is limited to 200 kbps to reduce data consumption. Such a quota system is also used in the Netherlands by limiting the speed per user to 150 kbps. Most solutions were first rolled out in the 2000s, and they have been upgraded with the possible usage of the Ka band for satellite solutions, and the deployment of the 4-th Generation (4G) cellular technologies.

Regarding on-board Internet, there are novel technological solutions that can be used to provide a broadband Internet access. The list of solutions presented in this chapter is not exhaustive, due to the constant evolution of the subject. For example, a wired Ethernet network could be considered, but it implies high installation costs. A WLAN

technology such as Wi-Fi is the most common deployment, and it is generally accepted that the replication concept of Wi-Fi access points within the train is the best technical solution to create connected trains with a client interface.

In the literature, authors like Fokum et al. [22] have already presented comprehensive surveys of approaches (e.g., TETRA, IEEE 802.11, satellite) that deliver broadband internet access on trains.

New technologies like Wireless Gigabit (WiGig) or Light-Fidelity (Li-Fi) will have to be considered in the medium-term [23]. WiGig (IEEE 802.11ad) is a new wireless technology under the Wi-Fi Alliance that operates at the unlicensed 60 GHz band (9 GHz bandwidth from 57 to 66 GHz in Europe). It offers high-speed, low latency, a throughput of up to 7 Gbps with a transmission distance of several tens of meters, and protected connectivity between nearby devices. Its Media access control (MAC) layer is extended and it is backward compatible with the IEEE 802.11 standard. When operating in the millimeter waves domain, beamforming techniques are needed to overcome the path loss from transmitter to receiver, what was not an issue for IEEE 802.11 a/b/g/n due to their use of omnidirectional antennas. On the other hand, Li-Fi (IEEE 802.15) is a 5-th Generation (5G) Visible Light Communication (VLC) system that uses light form diodes as a medium to deliver networked, mobile, and high-speed communications. It relies on data transmitted by amplitude modulation of light sources, according to a well-defined and standardized protocol. Its main drawbacks are that communications require obviously to switch on a light during transmissions and that mobility is not possible. For example, the French national state-owned railway company Société Nationale des Chemins de fer (SNCF) has been interested in Li-Fi during the last years. For instance, recent applications involving mass-market devices only have downlink communications implemented. A project between Lucioum Company and CEA-Leti is studying a bidirectional Li-Fi modem that allows for providing wireless Internet access of up to 20 Mbps. Furthermore, Oledcomm will provide Internet access via Li-Fi. On-board Internet by performing transmission via individual lights of the different passengers is a topic under research.

Surplus capacity could be leased by public mobile operators to trigger new customer services enabled by the usage of industrial IoT. 4G and 5G broadband will help to enhance smart railway attractiveness giving it an advantage over other competing transport means (i.e., excellent coverage, information provision with real-time updates, live-streaming video, mobile ticketing). Moreover, railway safety can be improved with train diagnostics and driver advisory systems (i.e., on-board CCTV recordings transferred to a control center).

2.3 Railway-specific services and requirements

It is publicly recognized that GSM-R is not well-suited for supporting advanced services such as automatic pilot applications or for provisioning broadband services to the train staff and passengers [24]. Based on GSM Phase 2 and Phase 2+ recommendations, GSM-R was analyzed to provide maximum redundancy and achieve maximum system availability. GSM-R provides two fundamental services: voice communications and the transmission of European Train Control System (ETCS) messages.

The definition of European Rail Traffic Management System (ERTMS) was the result of the European efforts to promote interoperability. ERTMS includes three levels. Among them, ERTMS levels 2 and 3 employ GSM-R as the basis that supports communications. In Europe, 4 MHz bandwidth is reserved for such communications. The main elements of ERTMS are:

- ETCS: it allows for automating train control. It consists of a Radio Block Center (RBC) and a Lineside Electronic Unit (LEU). ETCS can be divided into three levels, which are:
  - ETCS level 1: the location of the train is determined by traditional means (i.e., no beacons are used for locating the train), whereas communications between fixed safety infrastructure and trains are performed by means of *balises* (an electronic beacon or transponder placed between the rails of a railway track).
  - ETCS level 2: communications between trains and railway infrastructure is continuous and supported by the GSM-R technology. The location of the train is estimated by means of fixed *balises*.
  - ETCS level 3: the integrity of the train elements is checked at the train, thus no devices at the track are required. Fixed *balises* are used to locate the train.
- EURORADIO GSM-R: radio infrastructure.
- EUROBALISE: *balises* allowing for precisely locating the trains.
- EUROCAB: on-board management system that includes European Vital Computer (EVC), Driver-Machine Interface (DMI), and measurement devices such as odometers.

The UIC initiated the so-called ERTMS/GSM-R project to bring together existing and future developers. Furthermore, ERTMS/GSM-R manages the UIC roll-out plan aimed at updating the existing specifications of GSM-R. This common development has

continued until today, maintaining close cooperation with European Telecommunications Standards Institute (ETSI) and the GSM-R industry.

The FRS version 8.0.0 [25] and SRS version 16.0.0 [26], designated as European Railway Agency (ERA) GSM-R Baseline 1 Release 0, were published in December 2015 and represent the latest specifications. Such documents involve the description of mandatory requirements relevant to the interoperability of the rail system within the European Community, according to Directive 2008/57/EC [27], which incorporates requirements for a major milestone towards an IP-based core network architecture [28].

The areas covered by the EIRENE SRS can be outlined as follows:

- GSM-R network configuration, applicable to ER-GSM band frequencies, provides a guidance to meet performance levels, GSM-R coverage, speed limitations, handover and cell selection, and call set-up time requirements. Broadcast and group call areas are also defined.
- Mobile equipment specifications distinguish five types of mobile radios: cab radio and the Human-Machine Interface (HMI) for transmission of voice and non-safety data; EIRENE-compliant general purpose radio; EIRENE-compliant operational radio with functions to support railway operations; shunting radio; and ETCS data-only radios.
- EIRENE numbering plan requirements and constraints, call routing and structure of Functional Numbers.
- Subscription management, which handles the requirements for call priorities, encryption and authentication, broadcasts and Closed User Groups (CUGs).
- GSM-R operation modes: high-priority voice calls for operational emergencies (railway emergency calls); shunting mode, including the definition of user privileges; and an optional direct-mode communication providing short range fall-back communications between drivers and track-side personnel.

Some requirements are defined by individual railway companies [29]:

- Fixed network elements (e.g., links, switches, terminal equipment) and their specifications with respect to Reliability, Availability, Maintainability and Safety (RAMS) (EN50126, EN50128, EN50129), network interconnections and capacity. The fixed network must also support a specified set of services to provide end-to-end functionality. The inter-working between the fixed and the mobile side of the network must also be considered.
- Requirements for signaling systems to be used within the fixed network.

Table 2.1: Voice telephony services to be supported.

Voice-Call / Radio type	Cab	ETCS data only	General purpose	Operational	Shunting
Point-to-point	MI	NA	M	M	M
Public emergency	M	NA	M	M	M
Broadcast	M	NA	M	M	M
Group	MI	NA	M	M	M
Multi-party	MI	NA	O	O	M

Table 2.2: Data services to be supported.

Data / Radio type	Cab	ETCS data only	General purpose	Operational	Shunting
Text message	MI	NA	M	M	M
General data applications	M	O	O	O	O
Automatic fax	O	NA	O	O	O
ETCS train control	NA	MI	NA	NA	NA

- Non-mandatory specifications of controller equipment are provided by FRS, although details of such equipment, and the interface between the equipment and the GSM-R network are assigned to the railway operator.
- System management functionality and platforms; in particular, the specification of fault, configuration, accounting, performance, and security management requires various types of approvals to allow equipment to be connected to the network (i.e., it requires safety approvals for each railway).
- Roaming on a national public GSM network as part of a disaster recovery strategy in case of a loss of service.

According to the last EIRENE specifications, the railway integrated wireless network should meet the general and functional requirements under the categories: Mandatory for Interoperability (MI), Mandatory for the System (M), Optional (O) or Not Applicable (NA), depending on the type of radio. Specifically, the following are the general and functional requirements:

- Services: voice (Table 2.1), data (Table 2.2), and call related features. The call set-up required times are shown in Table 2.3, and should be achieved for interoperability (MI) in 95% of the cases. For 99% of the cases, the call set-up shall not be more than 1.5 times the call set-up required time.
- Railway EIRENE-specific applications are summarized in Table 2.4.
- Direct mode facility for local set-to-set operation without network infrastructure.
- Railway specific features: set-up of urgent or frequent calls through single keystroke or similar, display of functional identity of calling/called party, fast, and guaranteed

Table 2.3: GSM-R Call set-up time requirements.

Call type	Call set-up time
Railway emergency call	<4 s (M)
Group calls between drivers in the same area	<5 s (M)
All operational mobile-to-fixed calls not covered by the above	<5 s (O)
All operational fixed-to-mobile calls not covered by the above	<7 s (O)
All operational mobile-to-mobile calls not covered by the above	<10 s (O)
All low priority calls	<10 s (O)

Table 2.4: Specific features to be supported.

Feature / Radio type	Cab	ETCS data only	General purpose	Operational	Shunting
Functional addressing (FA)	MI	NA	M	M	M
Location dependent addressing (LDA)	MI	M	O	O	O
Direct mode	NA	NA	NA	NA	NA
Shunting mode	MI	NA	NA	NA	M
Multiple communications within the train	MI	NA	NA	NA	NA
Railway emergency calls	MI	NA	O	M	M

call set-up, seamless communication support for train speeds up to 500 km/h, automatic and manual test modes with fault indications, and control over mobile network selection and system configuration.

- Dedicated buttons that allow for quick access to emergency calls, Push-to-talk (PTT) and support for Link Assurance Signal (LAS) are required. Railway features such as Originator-To-Dispatcher-Information (OTDI), late entry, and frequency hopping in group calls should be considered. In addition, layouts for further features are presented: enhanced Presentation of Functional Number (ePFN), Driver's Safety Device alarms, Plain Text Messages, Presentation of the Functional Number (FN) of the initiator of a Railway Emergency Call (REC), and Alerting of a Controller.

A common minimum standard of performance is required to EIRENE-compliant mobile devices, although coverage and speed-limitation values are described in SRS. It should be noted that high-speed railway systems [30] (in operation, under construction and planned) have to cope with speeds of at least 250 km/h while enabling speeds over 300 km/h under appropriate circumstances. Generally, speeds around 200-220 km/h represent the threshold for upgraded conventional lines. Nevertheless, stable wireless connections have to be ensured at the moving speed of 500 km/h, or even more in the future [31].

Quality of Service (QoS) mechanisms shall ensure the priorization and pre-emption of critical services. Even though current wireless networks support various QoS policies depending on different traffic types, QoS for railway-critical communications and real-

Table 2.5: Summary of GSM-R QoS Requirements.

Requirements	Value
Connection establishment delay	$< 8.5\,s$ (95%),$\leq 10\,$s (100%)
Connection establishment error ratio	$< 10^{-2}$ (100%)
Connection loss rate	$< 10^{-2}/\,$h (100%)
Transfer delay of user data frame	$\leq 0.5\,$s (99%)
Transmission interference period	$< 0.8\,$s (95%), $< 1\,$s (99%)
Error-free period	$> 20\,$s (95%), $> 7\,$s (99%)
Network registration delay	$\leq$30 s (95%), $\leq$35 s (99%), $\leq$40 s (100%)
Call setup time	$\leq 10\,$s (100 %)
Emergency call setup time	$\leq 2\,$s (100 %)
Duration of transmission failures	$< 1\,$s (99%)

time applications shall be examined. QoS control is mandatory for resource management, safety, punctuality, efficiency, and accident prevention of trains, to ensure immediate reaction to emergencies and on-time operations. Strict latency requirements are needed for the seamless transmission/reception of data regarding the train position and status, and the Movement Authority (MA) permission between the in-service train and the control center (i.e., the transmission error probability over one train line should be less than 1% per hour and 99% of ETCS data should have a maximum latency of $<$ 0.5 s [32, 33]). QoS parameters with their percentage of availability are shown in Table 2.5.

2.4 LTE: one step ahead of broadband communication systems

The most important GSM-R shortcoming is the limited support for data services derived from the lack of packet-switched transmissions. For example, to deliver burst low-rate ETCS data messages, connections need to continuously take network resources despite they are not used. The maximum transmission rate per connection is limited to 9.6 kbps and the packet delay is about 400 ms, which is too high for real-time applications. Thus, GSM-R [24] cannot support modern data services. Another major problem is the limited capacity of ETCS using GSM-R circuit-switched data services in high traffic areas. This can be solved with an LTE micro-cell deployment or by using the ER-GSM band (includes standard and extended GSM 900 band) and changing to ETCS over packet-switched data using General Packet Radio Service (GPRS), Enhanced General Packet Radio Service (EGPRS) or Enhanced GPRS Phase 2 (EGPRS2) [34]. These shortcomings, together with the commitment of the GSM-R Industry Group [35] members to the long-term support of GSM-R until 2025, are encouraging the switch to a different system architecture as the new bearer network for railways.

The first major step in the evolution of LTE occurred in March 2011 when LTE-Advanced (LTE-A) was issued as part of 3rd Generation Partnership Project (3GPP) Rel-10, which made LTE formally compliant with the International Telecommunication Union - Telecommunication Standardization (ITU-T) 4G technology definition known as IMT-Advanced. LTE also met the requirements set by the mobile-operator-led alliance Next Generation Mobile Networks (NGMN). Rel-10 extended LTE radio access technology, including the possibility of using transmission bandwidths beyond 20 MHz, and improved spectrum flexibility by means of carrier aggregation.

Rel-11 includes basic functionality for Coordinated Multi-point (CoMP) transmission/reception, as well as enhanced support for heterogeneous deployments. Rel-12 (due out in December 2014) includes novel non-orthogonal waveforms to improve the performance of the Physical layer (PHY); sparse signal processing that can decode burst data traffic in an energy-efficient manner; robust systems that perform well under limited control channel bandwidth; and imperfect channel knowledge, hence reducing the end-to-end delay of wireless links from 10 ms to around 1 ms to meet the requirements of new machine-to-machine services.

2.4.1 Future communications networks

From the beginning of this thesis until now, the LTE standard evolved and new versions were released. Moreover, the new generation of communications systems, the so-called 5G has been defined. One of the most remarkable proposals for the definition of 5G is the utilization of Filter Bank Multicarrier (FBMC) modulations instead of the well-known Orthogonal Frequency-Division Multiplexing (OFDM). The next are the most important advantages offered by FBMC with respect to OFDM for the railway environment:

- FBMC offers higher bandwidth efficiency, which is very beneficial since the simultaneous communications between different trains can be more efficiently allocated into the scarce spectrum available in railway environments.
- Co-existence between the current GSM-R and the new broadband systems is a major concern in the railway industry. OFDM-based systems usually exhibit a high co-channel interference, leading to a potential performance impact on current GSM-R systems. FBMC-based systems are much more efficient, thus allowing for better co-existence with current systems.
- Improved multiple-access facilities in the uplink: due to the use of close-to-perfect subcarrier filters that ensure frequency localized subcarriers, FBMC does not require sophisticated synchronization methods for avoiding multiple-access

interference. Nevertheless, while OFDMA is adequate for allocating efficiently a subset of subcarriers per user in the downlink, the situation is different in the uplink, because user signals must arrive at the Evolved NodeB (eNodeB) synchronously, both in terms of symbol timing and carrier frequency. For a practical deployment, a close-to-perfect carrier synchronization is necessary, which is affordable in a stationary network, but becomes a very difficult task in a network that includes mobile nodes.

- Suitability for doubly dispersive channels: the waveforms used in FBMC can be optimized for doubly dispersive channels like the ones present in high-speed train communications, hence allowing for a compromise between time and frequency channel response.

However, there are some drawbacks. It must be noticed that channel estimation is more challenging in most FBMC schemes with respect to OFDM. Moreover, whereas OFDM offers full flexibility regarding Multiple-Input Multiple-Output (MIMO) structures, FBMC can only be used in certain MIMO schemes. Only schemes such as Filtered MultiTone (FMT) offer the same flexibility as OFDM, but FMT suffers from the same bandwidth loss as OFDM. Alternatives to FBMC such as Generalized FDM (GFDM) and Filtered OFDM (fOFDM) are also being considered as candidates for 5G systems.

2.5 Current status of standardization and migration roadmap

The UIC General Assembly held in Istanbul in 2008 announced that the advent of LTE was threatening the lifecycle of GSM technology. As a result, a technical report examining whether LTE communication systems would be applicable to the integrated railway wireless network [36] was published in 2009. The main conclusions were that LTE technology might be suitable for the future, but additional modifications would be required. Following this, a study on railways future mobile telecommunications systems was initiated.

In 2012, UIC envisioned the issue of next generation wireless communication standards at Paris World Conference. The Future Railway Mobile Telecommunication System (FRMTS) project was officially launched in 2013 in order to conduct research on the definition of a new wireless communications system, frequency redistribution, additional features, new structure of a network, efficient conversion from GSM-R, and railway signal transmission in a packet network. In particular, UIC has strengthen its cooperation with the 3GPP standard body to reflect the requirements of next-generation integrated wireless networks for railways in the LTE-based communication standards.

The American Research Innovation Technology Administration (RITA) envisions the future composite transportation network, taking as a whole the railway, the subway, and the road transportation. For instance, the next-generation of train-to-ground communications systems for this composite scenario will be based on Wi-Fi and LTE-A systems. In a European context, with the aim of overcoming the existing fragmentation, the strategic vision for the European Union's long-term transport policy includes the completion of the Single European Railway Area (Directive 2012/34/EU).

However LTE will be the baseline technology for the next generation of broadband public safety networks. Therefore, National Public Safety Telecommunications Council (NPSTC), TETRA + Critical Communications Association (TCCA), and Critical Communication Broadband Group (CCBG) are contributing to the standardization processes [37]. The current view is that this functionality could become available in products from circa 2016/17 onwards in LTE Rel-12 and 13. A new access technology might be defined in the Rel-14 and 15, while the time frame for a commercial deployment will be at the end of such a decade.

In recent years, UIC has started the migration from GSM Phase 2+ to LTE while ensuring that the life cycle of GSM-R will be extended with the unceasing progress of technologies. Authors emphasize the feasibility of a smooth evolution from GSM-R to LTE [24]. LTE migration of metro and railway is envisaged to move at different paces. In the absence of a global standard for Communications Based Train Control (CBTC), metro trains are likely to adopt LTE relatively quickly, in particular in new lines. Nonetheless, on mainline railways where international standards determine transmission networks for safety-critical systems, migration is likely to occur in two phases. In the early deployment stage, the non-safety-critical applications that require broadband will be carried out by the LTE network, whereas safety-critical applications will be carried out by the legacy networks. This requires the right mechanisms and architecture in radio and core networks to guarantee QoS and achieve a seamless service experience for all services. Following the maturity of LTE, all railway services will be then gradually transferred. When suppliers standardize ETCS on IP networks, LTE will replace GSM-R. Anyway, the coexistence of LTE and GSM-R will be required.

2.6 Assessing LTE potential for railway services

The maturity of LTE standards (up to Rel. 12) to address railway requirements is briefly summarized in the following paragraphs and in Table 2.6:

- **Point-to-point voice communications**: advanced voice communications are an essential functionality for railways. Different transmission strategies of voice

calls over the LTE architecture have been considered: Circuit Switched FallBack (CSFB), SMS over Serving Gateways (SGs), and Voice over LTE (VoLTE). The latter has emerged as the solution preferred by carriers and the GSMA has developed a profile [38] which defines the minimum set of features that a device and a network should implement to support a high quality IP Multimedia Subsystem (IMS)-based telephony service over LTE radio access.

- **Direct communication**: proximity Services (ProSe) are designed to address both critical and commercial requirements for direct mode or proximity, including discovery mechanisms and relay capabilities within and outside network coverage under continuous operator network control.

- **Location-based services**: in GSM-R, location services are used for addressing enhanced Location Dependent Addressing (eLDA) and for routing the call to the most appropriate Radio Block Centre (RBC). In LTE positioning, knowledge can be used in support of Radio Resource Management functions, as well as location-based services. ETSI TS 136.305 defines the E-UTRAN User Equipment (UE) entities and operations to support positioning methods. It provides support for downlink and uplink positioning, Enhanced Cell Id (ECID), and Assisted Global Navigation Satellite Systems (A-GNSS). LTE positioning services can be deployed through LTE Positioning Protocol (LPP). Furthermore, Open Mobile Alliance (OMA) LPP Extensions (LPPe) attempts to be bearer-independent as much as possible with respect to non-bearer associated position methods like A-GNSS and any terrestrial method applicable to a non-serving network. Although security, authentication, privacy, and charging are out of scope of LPPe.

- **Point-to-multipoint voice communications**: the Voice Broadcast Service (VBS) (3GPP TS 43.069) would be similar to Voice Group Call Service (VGCS) (3GPP TS 42.068) with the restriction that only the call originator is able to speak. LTE Rel-9 provides Evolved Multimedia Broadcast Multicast Service (eMBMS) as a bearer service to deliver PTT over LTE and allows for supporting Dynamic Adaptive Streaming over HTTP (DASH) over broadcast and unicast reception in Multicast and Broadcast over Single Frequency Networks (MBSFN) subframes. MBSFN implies several advantages such as the reduction of interferences at the receiver, the increase of the signal level received at the edges of the cells, and diversity in transmission. Rel-10 provides additional features such as Allocation and Retention Priority (ARP), which enables to establish priority between eMBMS sessions. Rel-11 includes enhanced support of service continuity with MBMS, content schedule information included in User Service Description (USD) to save

Table 2.6: LTE specifications to address service requirements.

Railway requirements	**LTE implementation**
Voice	• Point-to-point calls; VoLTE (GSMA IR. 92 v 7.0). • Proximity-based services (ProSe); Stage 2 (3GPP TS 23.303). • Service requirements for the Evolved Packet System (EPS) (3GPP TS 22.278). • Architecture enhancements to support ProSe (3GPP TS 23.703). • Security issues to support ProSe (3GPP TR 33.833). • LTE device to device proximity services; Radio aspects (3GPP TR 36.843). • 3GPP enablers for OMA; PoC services; Stage 2 (3GPP TR 23.979, OMA PoC V2.0 RD). • Emergency calls; MS emergency sessions (3GPP TS 23.167). • IP Multimedia Subsystem (IMS) emergency sessions (3GPP TS 23.167). • Support for IP based IMS Emergency calls over GPRS and EPS (3GPP TR23.869). • Group calls/Broadcast including emergency calls. • GCSE_LTE (3GPP TS 22.468); GCSE_LTE stage 2 (3GPP TS 23.468). • Mission Critical Voice Communications Requirements for Public Safety; NPSTC BBWG. • Public Safety Broadband High-Level Statement of Requirements for FirstNet Consideration, NPSTC Report Rev B. • Service aspects; Service principles (3GPP TS 22.101). • Architecture enhancements to support GCSE_LTE (3GPP TS 23.768). • Evolved Multimedia Broadcast Multicast Services (eMBMS) (3GPP TS 23.246); MBMS; Protocols and codecs (3GPP TS 26.346).
eMLPP	• QoS concept and architecture (3GPP TS 23.107). • Service-specific access control; Service accessibility (3GPP TS 22.011). • E-UTRA; RRC; Protocol specification (3GPP TS 36.331). • IMS multimedia telephony communications service and supplementary services (3GPP TS 24.173). • AT command set for User Equipment (UE) (3GPP TS 27.007). • Multimedia priority service (3GPP TS 22.153). • Enhancements for Multimedia Priority Service (3GPP TR 23.854).
Call related	• Call Forwarding supplementary services (3GPP TS 22.082). • Call Waiting (CW) and Call Hold (HOLD) supplementary services (3GPP TS 22.083). • Call Barring (CB) supplementary services (3GPP TS 22.088). • Numbering, addressing and identification (3GPP TS 23.003).
LDA	• LTE Positioning Protocol (LPP) (3GPP TS 36.355) and Annex (3GPP TS 36.455). • Functional stage-2 description of Location Services (LCS) (3GPP TS 23.271). • Serving Mobile Location Center (SMLC) Radio Resource LCS Protocol (RRLP) (3GPP TS 44.031).

Power, Quality of Experience (QoE) metrics reports to optimize Forward Error Correction (FEC) configuration of File Delivery over Unidirectional Transport (FLUTE), and location filtering to allow UE to selectively receive a service, among others. Group Communication System Enablers for LTE (3GPP TS 22.468, 3GPP TS 23.468, 3GPP TS 23.768) provides an efficient mechanism to distribute the same content to multiple users in a controlled manner with an end-to-end latency lower than 150 ms.

- **Push-to-talk over cellular**: VGCS systems will be expected to evolve into the Push-to-Talk over Cellular (PoC) system (OMA PoC V2.0 RD) to offer wide improvement in the voice quality and much faster call establishment. In Rel-13, PTT is revised to support the mission-critical operation in LTE networks (3GPP TS 22.179), Mission Critical Push To Talk over LTE (MCPTT).

- **Emergency calls**: Enhanced Railway Emergency Call (eREC) is an improvement over REC to subdivide the area of the call to set up only to the subscribers/lines that are directly affected, resulting in less production loss (e.g., parallel railway lines at a short geographical distance, dense station areas, level crossings, ...) while maintaining safety levels. IMS emergency calls (3GPP TS 23.167, 3GPP TR 23.869) represent the replacement of GSM-R point-to-point railway emergency calls.

- **Priority management**: the priority of a point-to-point, VBS, or VGCS call is assigned by the enhanced Multi-Level Precedence and Pre-emption (eMLPP) function. eNodeB's also play a key role in the policy management performing UL and DL rate policing and radio resource scheduling. ARP is used for call admission control and priorization of bearers during its establishment. The eNodeB Medium Access Control (MAC) scheduler is responsible for scheduling radio resources and supporting the concept of radio bearer QoS. Transport resources are managed by Evolved Packet Core (EPC).

- **Multi-service IP support**: the railway domain clearly distinguishes between non-critical and critical with the assignment of Safety Integrity Level (SIL). The features that IP transport networks must fulfill should be specified both at the level of communication standards and in their implementations in the upper functional layers. The migration to LTE technology implies the emergence of new security threats. As proposed by GSMA, Session Initiation Protocol (SIP) is the protocol used to register UE in the IMS server. Real-time Transport Protocol (RTP) and User Datagram Protocol (UDP) are the protocols recommended for voice transportation, and RTP Control Protocol (RTCP) for voice quality monitoring,

and providing link aliveness information while the media are on hold. The latter implies that the RTCP transmission must continue when the media are on hold.

- **Public Safety Networks Resiliency**: another important key technology is Self-Organizing Networks (SON), which allows for managing, configuring, maintaining, and optimizing the LTE communications networks (i.e., the optimization of the handover parameters in operations of heterogeneous networks).

2.7 The Internet of Trains: industrial IoT-connected railways

Long before IoT was coined, railway operators and infrastructure managers were actively using M2M technology and data analysis to improve the maintenance and performance of their assets. The Industrial IoT has had a major impact on the transportation industry, with the advent of autonomous vehicles and improved cargo management. Nevertheless, although they may have been pioneers, the reality is that the rail industry has barely scratched the surface of what is possible. As IoT continues to evolve, it is bringing greater standardization, openness, and scalability to the information provided to operators. They gain insight into how their assets are performing, which opens up many new possibilities to use big data in more creative and effective ways. Nonetheless, the fact that trains operate at such high speeds through tunnels and extreme weather conditions, presents real challenges when it comes to deploying IoT systems.

Regardless of the challenges, industrial IoT has the potential to revolutionize the railway industry. A rail network comprises thousands, if not millions of components, from rolling stocks to signals, rails, stations, and the staff who runs it all. All elements need to work cooperatively. The Internet of Trains holds the promise that rail systems can leapfrog interoperability, safety, and security issues, whilst modernizing rapidly. It refers to the use of networks of intelligent on-board devices connected to cloud-based applications to improve communications and control systems. The same network that strengthens safety has enough capacity to deliver data that serves a variety of applications across the rail system to reduce costs and improve operations. Using IoT is possible thanks to advances in the following underlying technologies:

- Telecommunications networks are becoming dedicated to industrial IoT applications and broadband communications are getting inexpensive, faster, and ubiquitous. Train companies run fiber along their tracks and have relationships with mobile operators to use such networks to maintain continuous mobile connectivity. Machine-to-Machine (M2M) technology can increase efficiency by using sensors embedded in a wide array of objects and systems to automate tasks and deliver real-time analysis and monitoring.

- Sensors for data acquisition are getting smaller, more affordable, and now consume less energy. In some cases, battery life can be extended up to five years, which is important, because it is not always possible to be close to an electrical supply.

- Cloud-based services have become more pervasive, fuelled both by smarter mobile devices and fast connectivity. They can be used to store sensor data and to provide the computation required for big data analytics.

- Big data and the Cyber-Physical System (CPS) enabled by IoT allow transportation modes to communicate with each other and with the environment, paving the way for truly integrated and inter-modal transport solutions.

2.7.1 Industrial IoT developments in the rail industry

This section briefly reviews recent industrial IoT developments in the rail industry. Regarding academic developments, there are just a few examples in the literature. A remarkable one is the design of an Electric Multiple Unit (EMU) IoT-system presented in [39]. It is oriented to the Maintenance, Repair and Operation (MRO) of high-speed trains in China. Massive seamless embedded RFID tags and sensors in train-ground transmission networks are able to perceive the status of high-speed trains in real-time, using holographic train visualization and delivering transit alerts. The use of multi-source and multi-level raw data in maintenance and repair processes, collecting various production aspects, such as trains flow, parts flow, labor flow, and equipments, helps to monitor productive processes and logistics during the whole life-cycle. This study is expected to increase the productive output of EMU maintenance 25% for the operation and 20% for the overhaul, respectively.

A different research area is studied in [40, 41], where authors examined a number of common rail-based planning and scheduling activities, and how they will benefit from the use of expert and decision-support systems.

Renowned commercial companies have been investing recently in Industrial IoT. Next paragraphs outline opportunities for the railway ecosystem (i.e., technology vendors and operators), including some initiatives that today are making the smart railway ecosystem vision a reality.

Trenitalia's Frecciarossa is working with SAP to develop a Dynamic Maintenance Management System (DMMS) [42]. The system presents cost savings between 8% to 10% of its maintenance bill. In this case, hundreds of sensors collect data in real time (from braking systems to the sliding doors), uploading them into SAPs cloud every ten minutes. Trenitalia runs 8,000 trains per day using a fleet of 30,000 locomotives, coaches, and freight cars. Once the data are in the cloud, they are analyzed using SAP

Predictive Maintenance and Service software and they are processed by the predictive analytics tool SAP HANA. Thus, Trenitalia can build predictive models using machine learning and also trigger actions (for example, when engine temperature hits a particular threshold, to help keeping trains running without delays). Key metrics, and diagnostic and management data are accessible by engineers and are visualized in real-time: the number of trains that are out of service, alerts that imply a maintenance action, the status of trains on the track, or the number of passengers. DMMS will be fully up and running across all Trenitalias rolling stock in 2018, and it will generate a full petabyte of data annually. Next, Trenitalia is hoping to automate the few remaining parts of diagnostics and maintenance that cannot be spotted by sensors, such as the roof and undercarriage of the trains, which still need a visual inspection. In the future, these tasks will be automated using cameras, instead of the visual inspection required today.

In 2013, VR Group [43], the state-owned railway in Finland, began fitting sensors on various systems and subsystems to monitor symptoms of failures to endure harsh weather conditions and ensure competitiveness. Traditionally, VR Group approached maintenance in two ways. Major systems, like wheels and bogies, were covered by scheduled maintenance. As a consequence, parts were replaced frequently when they still had a lot of life left. The other method was to fix things when they broke down. This type of maintenance was hard to forecast and could lead to missed routes and unhappy customers. Therefore, VR Group developed a predictive maintenance program that focused on monitoring the condition of elements at all times. Mathematical models predict when parts are likely to fail, so they can be replaced before they cause an unplanned downtime. The railway company goal is to change its maintenance approach, so eventually everything will be based on real-time fleet monitoring. By looking at new and historical data, Statistical Analysis System (SAS) helps VR Group to plan the maximum interval between certain maintenance events, like turning wheels (on a lathe) or replacing the wheel-and-axle sets on the trains. Each train has more than 30,000 of these sets. If the dates of turning are optimized, trains can be kept on the rails longer. They forecast a reduction of the amount of maintenance work by 35%. The failures causes can also be identified, which increases savings and improves the reliability of the trains. Additionally, effective insight enables VR Group to minimize stock levels of spare parts and materials, keeping only what is needed on hand.

Predictive maintenance is also encouraged by Siemens together with Teradata [44]. They expect predictive maintenance will evolve towards next-generation maintenance, creating a whole new business model to provide completely new services with up-time guarantees, risk-sharing models, and performance-based contracts for mobility systems.

Another example is represented by the french national state-owned railway company *Société Nationale des Chemins de Fer* (SNCF) [45], which is also using industrial IoT

powered by IBM Watson's deep learning analytics platform and SigFox's IoT network. These alliances are part of the company's 2020 strategy to become an industrial leader striving for operational excellence and optimum efficiency.

SNCF has developed a prototype where data acquisition devices are fitted to the transmission system on *Train à Grande Vitesse* (TGV). Data are transmitted over GSM and can be accessed remotely at the train depot, enabling technicians to see how well the gearbox is performing. SNCF also uses Sigfox communications devices to measure the water level tank in the TGV toilets, what speeds up the turnaround time when the train arrives at a depot.

Besides, engineers can connect to running trains in real-time, enabling SNCF to figure out whether a component is likely to fail, which could lead to the train being taken out of service. The cloud enables SNCF to run distributed calculations, the results of which can be reinjected into its train and rail maintenance processes.

2.8 IoT-enabled services: from more efficient operations to new business models

Legacy infrastructure is gradually being replaced by Train Management Systems (TMS) in which trains become communications hubs, transmitting data among them and to network control centers. M2M communications, centrally managed in a cloud-based architecture, enable operators to utilize equipment, tracks, and stations more efficiently, while dramatically reducing safety risks. The following sections are examples of Industrial IoT-enabled services (a general outlook is shown in Figure 2.1).

2.8.1 From reactive to predictive maintenance

Considering the expected growth in passenger and freight volume, and the aging of the existing infrastructure, maintenance costs are likely to increase significantly in the coming years. For instance, there is a high demand for maintenance operations based on frequent measurements of the different parts of the railway system.

The precise location of a heavy freight train, its speed and weight, correlated with data from vibration sensors located alongside the track, weather reports, and details of how long the power connector is disconnected from the catenary during operations, can improve maintenance decisions for critical items of infrastructures [46]. The fusion of this information with other meta-data, such as catenary dilation factors or track temperature, is an example that can further enhance the decision making process and help to create more sophisticated rail scheduling software.

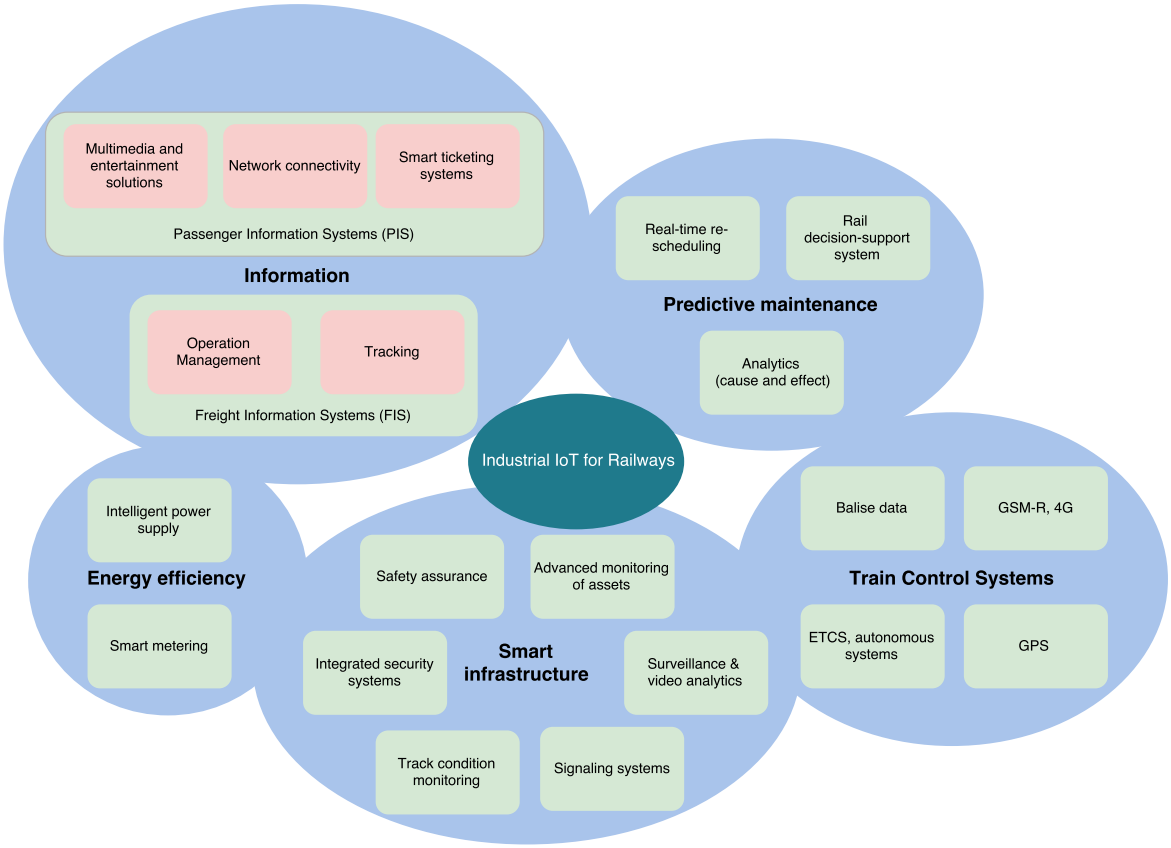


Figure 2.1: Industrial IoT-enabled services relevant to the rail industry.

Besides bringing greater safety and efficiency to the movement of rail traffic, IoT can also help to keep equipment to perform in a reliable way while maximizing time on the tracks with preventive maintenance. Costs can also be reduced by simplifying procedures and including better strategies based on analytics and data fusion, using train-borne, wayside and remote sensor technology to monitor the infrastructure condition.

Information concerning categorization of faults can be analyzed across multiple assets, even multiple operators, to spot trends and identify areas for preventative maintenance. Additionally, data analytics can speed up root-cause analyses, reducing labor time.

Automation for routine maintenance checks and repetitive tasks, such as ballast renewal, tamping, and track relaying, is needed. The amount of data that has to be collected from train-to-ground requires high-capacity wireless communications between train and wayside.

The following are a list of improvements that can be achieved:

- Increased up-time through a significant reduction of unplanned downtime.
- Extension and flexibility of maintenance intervals because the risk is understood.

- Improved utilization of assets (e.g., more mileage with fewer cars).
- Enhanced plan abilities, with streamlined Supply Chain Management (SCM).
- Maintenance can be performed at the least costly location.
- Uptime guarantees can be provided.
- Increased service contract capture rate, recurring revenues, and higher percentage of the total service revenue.

This matter has been studied in the literature. For example, different strategies for solving the railway preventive maintenance scheduling problem are examined in [47]. Furthermore, the applicability of big data techniques to facilitate maintenance decisions regarding railway tracks is discussed in [48].

2.8.2 Smart infrastructure

Infrastructure monitoring can provide significant benefits in different aspects like efficiency or safety. For example, data from sensors can improve driving performance. Adjusting the speed of the train according to its weight and length can extend the lifetime of brakes, while an enhanced understanding of the temperature of the engine and the brakes, the gradient of the railway, and traffic conditions, can help to decrease energy consumption significantly. For example, with 35% of train delays still caused by infrastructure or rolling stock failures, this is one obvious area where industrial IoT could offer vast improvements in performance.

Advanced monitoring of assets: sensors on trains and tracks help to reduce failures and improve the reliability of trains, signals, and tracks. On-board sensors monitor equipment and alert operators when critical parts are in need of attention. This cuts costs and helps to optimize asset utilization by reducing the need for taking trains out of service for routine inspection, for preventive maintenance, or for expensive repairs after a failure.

Remote monitoring helps to reduce maintenance time in the train depot. For example, train windshield water tanks can be equipped with a level sensor. Thus, a technician is then able to access this information via a web application on a tablet to see whether the water needs topping up.

A survey of Wireless Sensor Networks (WSN) for condition monitoring in the rail industry is presented in [49]. WSNs can be used for monitoring railway infrastructure like bridges, rail tracks, track beds, and track equipment along with vehicle health monitoring such as chassis, bogies, wheels, and wagons. The review studies which sensor

devices are used and what they are used for, and provides the identification of sensor configurations and network topologies including its main advantages and drawbacks.

Moreover, existing monitoring methods are studied in [50]. Authors integrate three methods to monitor rail damage in the turnout zone (i.e., fiber optic detection systems, optical imaging and Lamb guided wave detection systems).

In addition, Li et al. [51] propose models and algorithms that can effectively solve the physical topology optimization problem of the infrastructure health monitoring sensor network. Moreover, these methods can effectively reduce network costs and provide a theoretical basis for network communications link optimization.

Video surveillance systems: these systems visualize high-resolution images or videos within the train or station, where the system is installed [52]. The existence of a real-time viewing mode, a record mode, and a search/playback mode allows security managers to avoid threats. The surveillance camera supports video analytics, intelligent incident response, and emergency communication. These devices increase passenger safety and protect assets by integrating video surveillance systems across a network infrastructure. By integrating potentially thousands of cameras, a comprehensive view of the whole infrastructure (i.e., trains, tracks, depots, and stations) can be monitored by operators and management systems at the control center or by the staff operating in the field, with video analytics and real-world maps identifying, locating, and recording threats.

Intelligent Closed-Circuit Television (CCTV) cameras not only provide a record of events in case of an incident, but actively provide real-time alarms of the occurrence of potential problems, allowing for obtaining timely intervention responses and potentially reducing service outages. Moreover, when video recordings are requested by a law enforcement agency for an investigation of an incident, there is no need to send personnel on-board to pick up the hard drive manually.

In the railway domain, operators have expressed the lack of a surveillance on-board solution particularly because of the absence of broadband wireless communications systems between trains and the control center. Moreover, there are just a few examples in the literature that study video surveillance in railways. Numerous CCTV systems are deployed in metro because Wi-Fi networks are deployed easily in a tunnel environment. Nevertheless, there are few CCTV systems when considering conventional trains and none in the case of high-speed trains due to the absence of an efficient wireless transmission link train-to-ground.

Operations: once the infrastructure is in place to connect safety applications, it can also be used for non-safety-critical applications, enabling operators to leverage

their investment. By transmitting real-time, system-wide location data to control centers, on-board systems help operators optimize the deployment of equipment and the allocation of the track capacity to avoid bottlenecks and congestion.

Metro and commuter trains can utilize train data to relay departure, arrival, or train delay information to customers via mobile applications. Moreover, IoT has the potential to alter the prevailing business models used by rail system operators and their suppliers. Instead of selling equipment to operators, manufacturers or distributors can lease it based on usage metrics that remote sensors can track (for example, the weight of the cargo carried). This approach gives the manufacturer a regular source of revenue while turning the operator's cost from CAPital EXpenditure (CAPEX) to Operating Expenditure (OPEX).

2.8.3 Information

The worldwide railway industry faces pressure to improve the passenger and freight experience. To passengers, that might mean improved on-time performance, more on-board multimedia and entertainment, and more accurate information. To logistics companies, that might mean a cost-effective solution with total control of the freight. Taking the characteristics of the information into consideration, two types of targets have to be distinguished: passenger and freight.

Passenger Information System (PIS): is a key communications link between operators and passengers. PIS represents an electronic operating tool that provides, at any given time, visual and acoustic information to passengers on a route, both automatically or programmed manually. PIS includes real-time train tracking, route information and scheduling, travel planning, passenger infotainment, and online connectivity solutions. Along with system safety and reliability, the ability of the operators to provide accurate and useful information (i.e., departure/arrival times), and more comprehensive services, as well as a sense of control and participation, is a key component of passenger satisfaction.

PIS architecture spans across three different environments: rails, fixed installations such as stations and depots, and a centralized control center. This architecture is shared with the security, control and monitoring, and network functionalities. A wireless or wired connection is used for communication between the display device, the station computer, and the main server. The current position of trains is transferred to the relevant station computer through the main server, where the data are displayed, and new data for further stops can be calculated. The control center is used for controlling and monitoring the trains.

A journey planner application could recommend the fastest or most comfortable trip, allowing for live train times, available car parking, passenger loading, etc. Passengers will make informed choices about what option will provide them with the best experience according to their personal circumstances (i.e., whether it is more important to have the shortest journey time, or to be guaranteed a seat). The inclusion of historic data will enable the evaluation not only for a current trip, but also in a predictive way for a trip planned in the future.

The combination of passenger loading information from trains with social networking applications will help spread demand peaks. For example, offering the most efficient passenger exit considering the loadings of other inbound trains. In the case of interoperable tickets (valid for trains, metro, buses, and bicycles), intermodal travel could be encouraged by providing seamless connections to other modes.

Moreover, fusing status information from diverse on-board public-facing assets such as toilets, chillers and ovens, and presenting it to service organizations with current positional information, can improve the customer experience and reduce the penalty costs associated with having these assets out of service. The automation of toilets can significantly reduce the cost incurred by the train operator and, at the same time, provide a better service to passengers. Currently, most train operators are unable to determine the status of the on-board toilets in real-time and a significant amount of manual checking is required. Food and drinks can be easily refilled at the next station if data is available in real time regarding the items sold. Temperature can be remotely controlled to avoid issues with refrigerators that might not be working at all times.

Freight information system (FIS): rail freight generates a low level of external costs while reducing the environmental impact. Indeed, it represents the most eco-friendly land transport mode, with less energy consumption and CO_2 emissions than road, air or waterway transport. Today, legal barriers and operational and technical problems impact on the overall capacity and performance of the rail freight, and the reliability of freight services need to be improved. The modal share of rail transport is modest, with rail accounting for 11% transportation in Europe, and 6% of intra-european passenger transport according to reports of the European Commission in 2014. Two main challenges can be identified. First, a new service-oriented profile relying on on-time delivery. Second, an increase of productivity and cost competitiveness by addressing current issues, such as interoperability, the optimization of existing infrastructure, and the promotion of synergies from other sectors.

FIS delivers real-time information on freight traffic to provide a significant picture of freight transportation movements, effectiveness, and planning. FIS is subdivided into two solutions: operation management solutions for capacity and freight management,

which ranges from booking to rolling stock planning, and tracking solutions for real-time location information of cargo containers. A FIS helps freight operators to make infrastructure and planning decisions based on robust, reliable, and consistent data. The information also improves the labor utilization and productivity, and today is widely adopted by the logistics companies for better customer support and loyalty. The following represents the main advantages of FIS for railways:

- Improved dynamic train performances.
- Real-time information provision, which is specially important in the case of dangerous goods.
- It enables the interaction and exchange of information from train-to-ground.
- Remote real-time diagnosis with sensors embedded in wagons.

2.8.4 Train control systems

Autonomous systems: such systems may range from semi-automated to totally autonomous operation where no human intervention is needed. Semi-automated operation includes ETCS in-cab signaling and automated train braking systems. Autonomous examples include the fully automated operation of trains, where systems use complex control logic and incorporate computational intelligence techniques such as fuzzy logic and genetic algorithms. There are only limited investigations about full autonomous operation within the railway industry, usually focusing on automatic operation of metro/light rail systems [53]. Opportunities for research exist on maintenance planning and scheduling, among other activities, considering autonomous or semi-autonomous operation.

Safety assurance: safety is a primary requirement of IoT applications and solutions when it comes to train management. For example, one critical application is on-board train location and detection systems that enable train-awareness of the positions of other trains. This reduces the risk of collisions while allowing trains to operate safely in close proximity to one another, and making more efficient use of track capacity.

Speed monitoring and control is another important safety application. Systems have been developed that can display train velocity for drivers and report speeds back to central control systems. On-board monitoring systems are interconnected with wayside signaling systems that regulate train speed or even remotely command the train to stop based on track conditions, on the positions of switches, on the presence of other trains on the track, and other factors.

Signaling Systems: there are three major systems where automation and the IoT can bring significant benefits: signaling, interlocking, and level crossing control.

Signaling systems control the movement of a train by remotely adjusting train speed and braking. More traditional signaling systems are based on RFID along the train track, but wireless ground-to-train signaling is getting more and more common. Most of the new European lines are equipped with ETCS level 2 that requires constant radio communications between the train and the group.

Interlocking avoids conflicting movements on the tracks at junctions and crossings by using red and green light signals. The interlocking system works in conjunction with the signaling system to prevent a train from getting a signal to proceed if the route is proven to be unsafe. IoT can further improve the system level of automation and its integration with the signaling system.

Level crossing control has also a huge impact on safety. According to the European Railway Agency, 619 accidents occurred at level crossings in 2010, causing 359 fatalities in that year. Accidents related to level crossings represent 30% of all railway fatalities in the EU. IoT can help to decrease those statistics by deploying cameras and sensors for increased safety. One example in the literature relying on video is presented in [54]. Other alternatives use Ultra-Wide Band (UWB) technologies like authors in [55].

2.8.5 Energy efficiency

Energy efficiency can be determined throughout smart metering methods. With a knowledge of the different consumers it is possible to perform an efficient energy management. Smart metering also optimizes asset management and increases capacity. Such systems rely on three elements: sensors deployed in the railway system (at trackside and on-board), the communications between the different sensors, and the communications train-to-ground that require broadband links.

These examples are just the tip of the iceberg and many other areas that could offer potential benefits have probably not even been identified yet. Indeed, massive data aggregation, correlation, and analysis using highly-sophisticated algorithms have the potential to change operations, maintenance, yield management, and even passenger services in the future. As shown in this brief review, the industrial IoT is set to revolutionize train operations, enabling to improve customer service and the competitiveness of trains.

2.9 Conclusions

This chapter examined the role of enabling technologies to revolutionize the railway industry. Broadband technologies, like LTE, provide the capacity needed to create novel services. For instance, a formal study regarding GSM-R operational requirements and services was previously presented in order to provide an understanding of future customer needs. LTE Rel-11 adds the first feature for public safety (i.e., high-power UE). Nevertheless, starting from LTE Rel-12, the standard provides features for mission-critical communications such as IMS emergency calls, ProSe, GCSE, PoC, and eMBMS that will enable LTE to be used as part of a broadband public safety network. LTE Rel-13 introduces MCPTT, enhancements of ProSe and GCSE, and the isolated E-UTRAN operation. Although the feasibility of LTE in the railway environment is evaluated, developing the new ecosystem will also require the design of a thorough migration strategy.

Furthermore, the adoption of the Industrial IoT paradigm opens a wide area of potential applications. Examples like preventive maintenance, holistic freight management, and advanced monitoring of assets, were explained in order to expose the IoT capabilities to reinforce competitive advantages, create new business models, and change railways.

Chapter 3

Security Evaluation of Commercial Tags for RFID-Based Transportation Systems

3.1 Introduction

Nowadays, Radio Frequency IDentification (RFID) is part of many critical applications for tracking assets [56], and even people, as it was established in the previous chapters. In the transportation industry, RFID is used in road (e.g., tolls, identification of moving assets), air (e.g., baggage and boarding card handling), rail (e.g., monitoring tracks, identification of assets), and sea (e.g., controlling the check-in/out procedures in vessels transportation). Despite RFID's popularity, many applications developers have neglected its security: it is easy to find commercial systems that contain critical security vulnerabilities that allow for cloning tags or for straight signal replaying. Such vulnerabilities let attackers access certain services or facilities, get or alter personal information, and even track users. Additionally, many RFID systems are susceptible to reverse engineering. Thus, certain hardware and software components can be extracted and analyzed in order to reproduce them. For instance, multiple authors have been able to emulate communications protocols and reverse-engineer cryptographic algorithms using, in most cases, low-cost equipment.

Countermeasures can be taken to prevent attacks. The most common defenses include the use of cryptography, automatic malware detection, improving resistance to cloning, uncovering rogue devices, or secure authentication schemes. However, it is common to find commercial RFID systems that due to cost or speed have such security features disabled. Unfortunately, it is even more common to identify already-broken RFID security systems still in use in mission-critical scenarios.

To foster security, a methodology to reverse engineer and detect security flaws is put into practice in this chapter. Specifically, the communications protocol of an RFID public transportation card used by hundreds of thousands of people in Spain was analyzed. By applying the methodology and a few reverse engineering skills, it was possible to access private information (e.g., trips performed, buses taken, fares applied, ...) to capture tag-reader communications, and even emulate both tags and readers.

This chapter is based on the publications [57–59] and is organized as follows. Section 3.2 presents a brief overview of RFID security. Section 3.3 reviews the state-of-the-art of transportation cards and their main security issues. Section 3.4 proposes a step-by-step methodology for auditing RFID security and reverse engineering communications protocols. In Section 3.5 the methodology is applied through a RFID hardware security tool to a public transportation card. Finally, Section 3.6 is devoted to conclusions.

3.2 Fundamentals of RFID security

3.2.1 Types of RFID systems

The main types of RFID systems can be divided into the following categories according to their frequency band:

- LF (Low Frequency) RFID. According to the ITU (International Telecommunications Union), the LF band goes between 30 kHz and 300 kHz. Frequency and power in this band are not regulated globally in the same way: most systems operate at 125 kHz, but there are some at 134 kHz. The reading range provided is short (generally up to 10 cm), so, in practice, LF devices are not usually sensitive to radio interference. Its most popular applications are access control and animal identification (mainly for pets and livestock).
- HF (High Frequency) RFID. Although the HF band goes from 3 MHz to 30 MHz, most systems operate at 13.56 MHz. HF systems can reach a reading distance of up to 1 m, what can lead to interference and, therefore, MAC (Medium-Access Control) mechanisms have to be implemented. This sort of RFID systems is massively used in transportation, payment, ticketing, and access control.
- UHF (Ultra-High Frequency) RFID. The UHF band actually covers from 300 MHz to 3 GHz, but most systems operate in the ISM (Industrial-Scientific-Medical) bands around 860-960 MHz and 2.45 GHz. UHF tags can be easily read at 10 m, so they are ideal for inventory management and item tracking in logistics.

All these RFID systems can also be classified according to the way the tags are powered:

- Passive systems. They do not need internal batteries to operate, since they rectify the energy sent through the readers antenna. There are LF, HF, and UHF passive systems, which nowadays can be easily read at a 10 m distance.
- Active systems. They include batteries, what allows them to reach further distances (usually up to 100 m). Due to power regulations, almost all active systems operate in the UHF band.
- Semi-active, semi-passive or BAP (Battery-Assisted Passive) systems. They decrease power consumption by using batteries just for powering the tags for certain functionality. Commonly, batteries are used to power up the basic electronics, while the energy obtained from the reader is used for powering the communications interface.

A detailed description of the principles that regulate how RFID works is out of the scope of this chapter, but the interested reader can get a good overview of the technology and its basic security implications in [60].

3.2.2 Main attacks against RFID systems

3.2.2.1 Risks and Threats

Information security threats have been traditionally classified according to what is known as the CIA Triad:

- Confidentiality. It is related to the importance of protecting the most sensitive information from unauthorized access.
- Integrity. It consists in protecting data from modification or deletion by unauthorized parties, and ensuring that, when authorized people make changes, they can be undone if some damage occurs.
- Availability. It is the possibility of accessing the system data when needed.

If any of these three principles is not met, then security is said that it has been broken. Like other technologies, RFID is exposed to security threats and, specifically, to attacks on the confidentiality, integrity and availability of the data stored on the tags, or on the information exchanged between a reader and a tag. When these threats are associated with the probability of occurrence of an event that causes damage to an informational asset, they are known as risks. Two kinds of risks can be basically distinguished:

- Security risks. They are derived from actions able to damage, block or take advantage from a service in a malicious way. The action is usually carried out

with the objective of obtaining a profit or just to damage the access to certain service.

- Privacy risks. These risks affect the confidential information of the users. In some cases, when a user interacts constantly with the environment, objects and people around, an attacker would be even able to obtain extremely accurate information on the personal data, location, behavior and habits. In the case of RFID, there are mainly two privacy risks:
  - Unauthorized access to personal data. Many systems store private data on RFID tags, or transmit them when a tag and a reader exchange information.
  - Personal tracking. This is probably the most feared since an attacker might determine routes, purchases and habits of a specific person.

In real life, most risks are a mixture of both security and privacy risks: they threaten RFID security in order to get access to the information stored or to the data exchanged in a transaction.

3.2.2.2 Physical attacks

This type of threat consists in using some kind of physical medium to attack a tag or the RFID communications. There are mainly five basic attacks:

- Reverse engineering. Most tags are not tamper-proof and can be disassembled and analyzed.
- Signal blocking or jamming. It consists in blocking tag communications to avoid sending data to a reader.
- Tag removal. It consists in removing an RFID tag or replacing it with another one.
- Physical destruction. The attacker destroys the RFID tag by applying pressure, tension loads, or high/low temperatures; by exposing the tag to certain chemicals; or by just clipping the antenna off.
- Wireless zapping. RFID zappers are able to send energy remotely that, once rectified, is so high that certain components of the tag are burned.

3.2.2.3 Software attacks

These attacks are related to software bugs or vulnerabilities found in tags or in the RFID reader. The most common are:

- Remote switch off. Researchers have found that it is possible to misuse the kill password in some tags (EPC Class-1 Gen-2) with a passive eavesdropper and then disable the tags.
- Tag cloning. In this attack, the Unique Identifier (UID) and/or the content of the RFID is extracted and inserted into another tag.
- Command injection. Some readers are vulnerable to remote code execution by just reading the content of a tag.
- SQL injection. It has been found that some reader middleware is vulnerable to the injection of random SQL commands.
- Virus/Malware injection. Although difficult to perform in the vast majority of RFID tags, due to their low storage capacity, it is possible to insert malicious code in certain tags that is able to be transmitted to other tags.
- Network protocol attacks. Many systems integrate back-end databases and connect to networking devices, which are susceptible to the same vulnerabilities as any other general purpose networking device.

3.2.2.4 Channel attacks

Channel attacks refer to threats related to the lack of security in the communications between the reader and the tag. The following are the most popular attacks:

- Unauthorized reading. Most RFID tags can be easily read without leaving a trace, although readings are limited to relatively short distances. Some of the latest measures to prevent this kind of attacks make use of sophisticated techniques.
- Denial of Service (DoS) attacks. The channel is flooded with such a large amount of information that the reader cannot deal with the signals sent by real tags.
- Signal replaying. It consists in recording the RFID signal in certain time instants with the objective of replaying it later.
- Man-in-the-Middle (MitM) attacks. They consist in placing an active device between a tag and a reader in order to intercept and alter the communications between both elements.
- Relay/amplification attacks. They consist in amplifying the RFID signal using a relay, so the range of the RFID tag is extended beyond its intended use.

3.2.3 Countermeasures against the most common attacks

RFID systems can take one or more of the following measures against the attacks previously described:

- Reader-Tag authentication. Both devices should carry out a two-way authentication, so only legitimate devices can communicate. This mechanism prevents certain types of remote tag destruction (i.e., only an authorized user can send a kill command), unauthorized readings, and MitM attacks.
- Rogue device detection. If a reader is provided with the capacity of detecting abnormal tag behaviors, it might avoid DoS attacks, certain unauthorized readings, command/virus/malware injection, and network protocol attacks.
- Use of cryptography. Due to the limited power and performance of most RFID tags, complex cryptography is not usual in most reader-tag communications. However, a minimum level of communications confidentiality has to be provided by RFID systems, so the most relevant information should be encrypted. Basic cryptography can prevent eavesdropping, MitM attacks, and unauthorized readings.
- Data integrity verification. RFID systems should ensure that the data received has not been tampered or modified by an attacker. This verification is key in MitM attacks.

3.2.4 Reverse engineering attacks

There are different alternative attacks that researchers have tested over the last years:

- Communications protocol analysis. This is related to channel attacks: the communications between the reader and the tags are captured and analyzed. It is probably the most popular attack because it is non-intrusive and the cost of the hardware is relatively low in comparison to other attacks. For instance, an example of a communications protocol analysis is described in [61]: the authors detail how they reverse engineered and emulated an LF tag for sport events with the help of an Arduino board and a few electronic components. However, note that it is quite difficult to derive all of the functionality, specially in the case of encrypted and obfuscated communications. Although cryptography hinders communications protocols analysis, it is not actually implemented in many tags, since additional hardware (i.e., higher economic cost) and power are required, and communications latency is increased. The methodology proposed in this chapter is actually aimed at performing communications protocol analysis.

- Power analysis. It is a type of non-intrusive attack that assumes that power consumption (or the electromagnetic field) is related to the execution of certain instructions. A good description of how to carry out a power analysis is presented in [62, 63], where the authors attack different commercial HF and UHF RFID tags. A remarkable work is also [64], that describes what the author claims to be the first remote power analysis against a passive RFID tag. To prevent power analysis, the different protection functions must be designed to consume the same amount of power: although the algorithms may seem inefficient, the attacker would not distinguish between the different processes.

- Optical analysis. This attack is widely used for reverse-engineering microchips and, therefore, it can be used for studying the internal hardware of an RFID tag. Before performing such an analysis, the external enclosure has to be removed, which involves using acid and, less frequently, a laser beam. Then, an optical or electron microscope can be used to analyze the hardware. An excellent example of optical analysis is described in [65], where the authors detail how they reverse-engineered the security of MIFARE Classic cards (the authors first performed an optical analysis, and then a communications protocol analysis). To avoid reverse engineering through optical analysis, the designers of RFID tags can embed non-functional logic to misguide the attackers, re-position the internal hardware to make the analysis more difficult, or implement certain key functionality in software instead of hardware.

- Electronic analysis. It is usually performed in combination with optical analysis to get a better picture on how an RFID circuit works. It consists in applying really small probes to read or induce voltages in different parts of the chip when carrying out certain operations. Bus obfuscation and communications encryption are usually effective against this kind of analysis.

3.2.5 Hardware tools for auditing RFID security

In recent years, a number of projects have been developed with the aim of facilitating researchers low-level access to RFID communications. Some of them are just software tools that can be used with commercial RFID readers [66], while others involve specific hardware [67–72] or certain firmware [73]. Hardware developments are specially interesting: some devices can emulate readers [69, 70], others can emulate just tags [67, 71], and a few can emulate both kinds of devices [68, 72].

RFIDIOt [66] is a set of open-source software tools developed as python libraries aimed at analyzing RFID devices. These libraries are compatible with different HF and LF

readers (manufactured by ACG, Omnikey or Frosch Electronics), and support reading/writing to multiple tags (e.g., MIFARE, SLE, ISO/IEC 14443-A, ISO/IEC 14443-B, ISO/IEC 15693, ISO 18000-3, NFC, ICODE, EM 4x tags, Hitag, or TI-RFID).

Tastic [69] focuses on reading LF and HF tags at a long distance (up to one meter). It specifically targets badge systems like HID Prox, Indala Prox or HID ICLASS. It is based on an Arduino board that connects to standard DATA0/DATA1 Wiegand outputs.

OpenPCD [70] is an open-source and open-hardware system able to emulate and sniff data from HF RFID/NFC cards (e.g., ISO/IEC 14443, ISO/IEC 15690, MIFARE, ICLASS). It supports the libNFC library and has been designed around NXP's PN532, which is a transmission module that embeds a 80C51 microcontroller with 40 KB of ROM and 1 KB of RAM.

OpenPICC [71] is the counterpart of OpenPCD: it emulates HF tags like the ones compliant with ISO/IEC 14443 and ISO/IEC 15690. It is based on a 32-bit ARM microcontroller (AT91SAM7S256) with 128 KB of flash memory and 64 KB of SRAM.

There are not many academic platforms developed to test RFID security. One good example is described in [67]. Such a platform is composed by a microcontroller and an Field-Programmable Gate Array (FPGA). Its aim is to evaluate HF and UHF RFID tags. The latest academic development as of writing is the Chameleon Mini [72], which has been promoted by the Ruhr University (Bochum, Germany): it is a versatile RFID tag emulator compliant with ISO/IEC 14443 and ISO/IEC 15693 (for instance, it currently supports MIFARE Classic 1K/4K/Ultralight emulation).

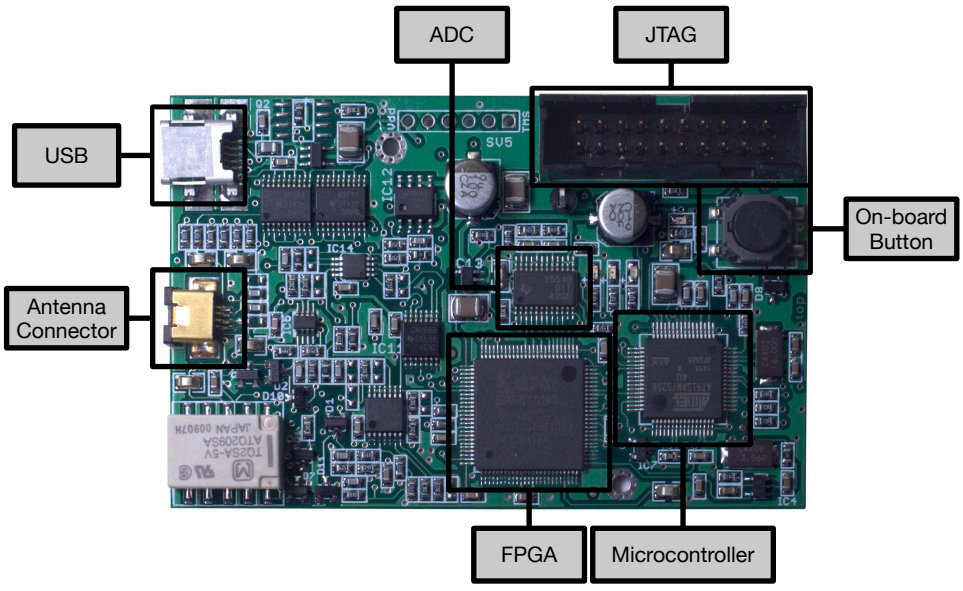


Figure 3.1: Main components of Proxmark 3.

The platform selected in this chapter to analyze RFID security is Proxmark 3 [68], which is an open-source system able to transmit at LF (125-134 kHz) and HF (13.56 MHz). The system contains an Atmel AT91SAM7S256 (256 KB of Flash and 64 KB of RAM), an FPGA (Xilinx Spartan-II) and an 8-bit Analog-to-Digital Converter (ADC). It is powered through an USB and has an SV2 connector for the antenna, which contains four pins: two are for the HF antenna, and the other two are for the LF antenna. All these components can be observed in Figure 3.1. The Proxmark 3 was our choice to test commercial RFID systems because of its main features:

- It operates in HF and LF, where most popular RFID applications work (e.g., identification tags, payment cards or passports). This is due to the hardware cost in such frequency bands and because the reading distance is enough for the applications. UHF is also heavily used in other fields, where more reading distance is required (e.g., logistics), and tags have become inexpensive, but the reading hardware (i.e., readers, antennas, muxes and amplifiers) is more expensive than most LF and HF devices.

- Its ability to sniff easily communications between a reader and different tags.

- The possibility of emulating diverse RFID communications protocols. The official firmware supports some basic protocols, but it is relatively easy to develop and upload new code to the embedded ARM microcontroller and to its FPGA.

- The community behind Proxmark 3, which has been extending the official firmware to add new features.

When the Proxmark 3 acts as an RFID receiver, the signal that comes from the antenna goes through the ADC and is converted from analog to digital. Then, the digital data are sent through an 8-bit bus to the FPGA, where they are demodulated. Finally, the signal is sent from the FPGA to the microcontroller through the SPI to deal with the RFID protocol. When the Proxmark acts as a transmitter, the same steps are performed but in reverse order. The FPGA modulators/demodulators are developed in Verilog, while the Atmel microcontroller is programmed in C. There is also a client application developed in C able to send remote commands to interact with the device. Different custom firmwares have been developed for Proxmark 3. An example is Proxbrute [73], created by McAffee in order to extend Proxmark functionalities to perform brute force attacks, mainly against access control systems.

3.3 Public transportation cards

Most modern public transportation services use contact, wireless, or hybrid systems to provide personal identification, data storage, and application processing. Although the primary function of such systems is to ease the payment for the different transportation means (i.e., train, subways, trams and buses) some have additional functionality related to tourism or citizen services.

Contact cards include traditional magnetic stripe and chip cards. The first ones are limited to providing a cheap and simple mean of identifying users. However, its security can be clearly improved and the magnetic stripe degradation forces them to be replaced after certain time or number of uses. Due to these facts, magnetic stripe cards are being replaced with chip cards. The first generation of chip cards still suffers from degradation during the reading process so, after a number of uses, the card starts to fail during transactions. The second generation opted for using wireless or hybrid (contact plus wireless) communications. Wireless cards communicate with the RFID reader at a short distance accelerating the payment process, and avoiding to take the card out of the wallet. In the case of hybrid cards, in addition to the wireless interface, the chip contact interface is maintained, therefore covering the services in which both types of RFID readers are used. There are also hybrid cards that include a magnetic stripe.

The advance of the identification technologies has allowed to increase the reading distance until several tens of meters. This has improved the level of automation and the possibility of offering new services, but it entails an increase in the card intelligence, which should add additional security to avoid unwanted readings or transactions. The vast majority of smart cards use the HF band, since it offers a good trade-off between reading distance, security, and cost. Examples of wireless smart cards are the MOBIB (Brussels), the Navigo Pass (Paris), the Octopus Card (Hong Kong), or the Troika Card (Moscow).

Regarding the operational frequency it must indicated that in 2011 the representatives of a consortium of the European Commission on smart cards, jointly with transport system managers from all over the world, concluded that the near-future technologies will be HF and Near Field Communication (NFC).

3.3.1 Privacy issues

Recently, different entities have reported that certain cards allow for obtaining data presumably anonymous. For example, two citizens' rights organizations complained that the card operated by the Brussels transport company (MOBIB card) violated the citizens' right to privacy, which is regulated by a law from 1992. Despite the company

claimed that the card complies with legality, researchers from the Catholic University of Louvain showed that the card could be read by anyone at relatively close distances, and obtained personal data and the trace of the last trips.

In France, the Navigo Pass suffered a similar situation. The National Committee for Informatics and Freedoms intervened, making the Parisian transport company to create an anonymous version of the card ("*Navigo Découverte*") which, although received some criticism for its non-anonymous acquisition system, it greatly guarantees the anonymity of the users by unlinking it from any data owned by the company.

Finally, it must be mentioned a report presented by a consortium of the European Commission [74], which indicated that smart card-based systems administrators can now monitor passenger behavior. This knowledge, although it can be used to improve safety, mobility and marketing strategies, requires the administrators to add security to protect the privacy and personal data of users. However, the general principles governing this aspect are common and are provided by regulations such as the Data Protection Directive of the European Union, the APEC Privacy Framework and the OECD (Organization for Economic Co-operation and Development) guidelines of 1980 about the protection of privacy and personal data in transboundary migratory flows.

3.3.2 Security issues

Several controversies related to the weakness of the security of transportation systems have arisen over the last years. The case that probably had the greatest impact was the access and handling of MIFARE Classic cards that controlled the transport systems of London (Oyster Card), the Netherlands (OV-chipkaart), the county of Miami-Dade in the United States (Easy Card), Istanbul (Istambulkart), Taiwan (EasyCard, Taipei Metro Rapid Transit) or Buenos Aires (SUBE card). In all these cases, it was possible to clone cards, obtain private data from other users and alter the credit available. The MIFARE Classic was attacked in 2008 in three ways. First, two hackers were able to remove the coating on the MIFARE Classic chip and, studying the circuitry, they were able to deduce the secret cryptographic algorithm used by the chip [75]. Second, it was shown how a single-use MIFARE Ultralight card could be reset to its original "unused" state [76]. Third, an engineer built an RFID tag emulator to perform a relay attack on the Ultralight card [77]. Besides, major security flaws were found in the Boston subway cards (Charlieticket and Charliecard). In 2010, researchers [78] detailed a side-channel attack on DESFire EV and EV1 cards. DESFire cards could be easily cloned by a hardware built for less than $25 in approximately 100 ms. In 2011, the same authors [79] demonstrated side-channel attacks on the MIFARE DESFire MF3ICD40. Additionally,

during 2012, MIFARE Ultralight cards of the New Jersey and San Francisco transit systems were manipulated using an Android application.

3.4 Methodology for security audit and reverse engineering communications protocols

3.4.1 Objectives of the methodology

The methodology presented in the next subsection was devised to automate the security audit and the reverse engineering process of commercial RFID systems. It is able to expose the internal structure of the communication protocol revealing possible vulnerabilities. These vulnerabilities include the existence of high-privilege modes, debugging functionality or backdoors implemented intentionally by the manufacturer.

Note that the knowledge obtained by applying the methodology proposed might also be used for other purposes: the gathering of information on poorly or non-documented RFID systems, the replication of software copyrighted without violating the law, or for espionage purposes. In this latter case, a company may reverse-engineer a competing product to study its inner workings and estimate the hardware cost in order to enhance its own products and determine if it is possible to offer better prices.

It must be indicated that we are only aware of one other methodology focused on reverse engineering RFID systems [80]: the one used by RIDAC [81], an open-source framework for auditing RFID security released by Oulu university (Finland) in 2009. The methodology has similar objectives, but it is structured in processes instead of steps, and is oriented towards the specific use of RIDAC software.

3.4.2 Basic steps

The methodology proposed first determines the most relevant parameters of a tag (i.e., operating frequency, coding scheme, and modulation), and then identifies its RFID standard (or tries to reverse engineer the communications protocol and the internal data structure).

The methodology flow diagram is depicted in Figure 3.2, where the following main steps can be observed:

- Visual inspection. Before analyzing the characteristics of a tag, it is first recommended to look for external signs that might indicate the manufacturer, the model or the RFID standard. If any of such data is recognized, it is usually straightforward to obtain the basic parameters and details on the communications protocol.

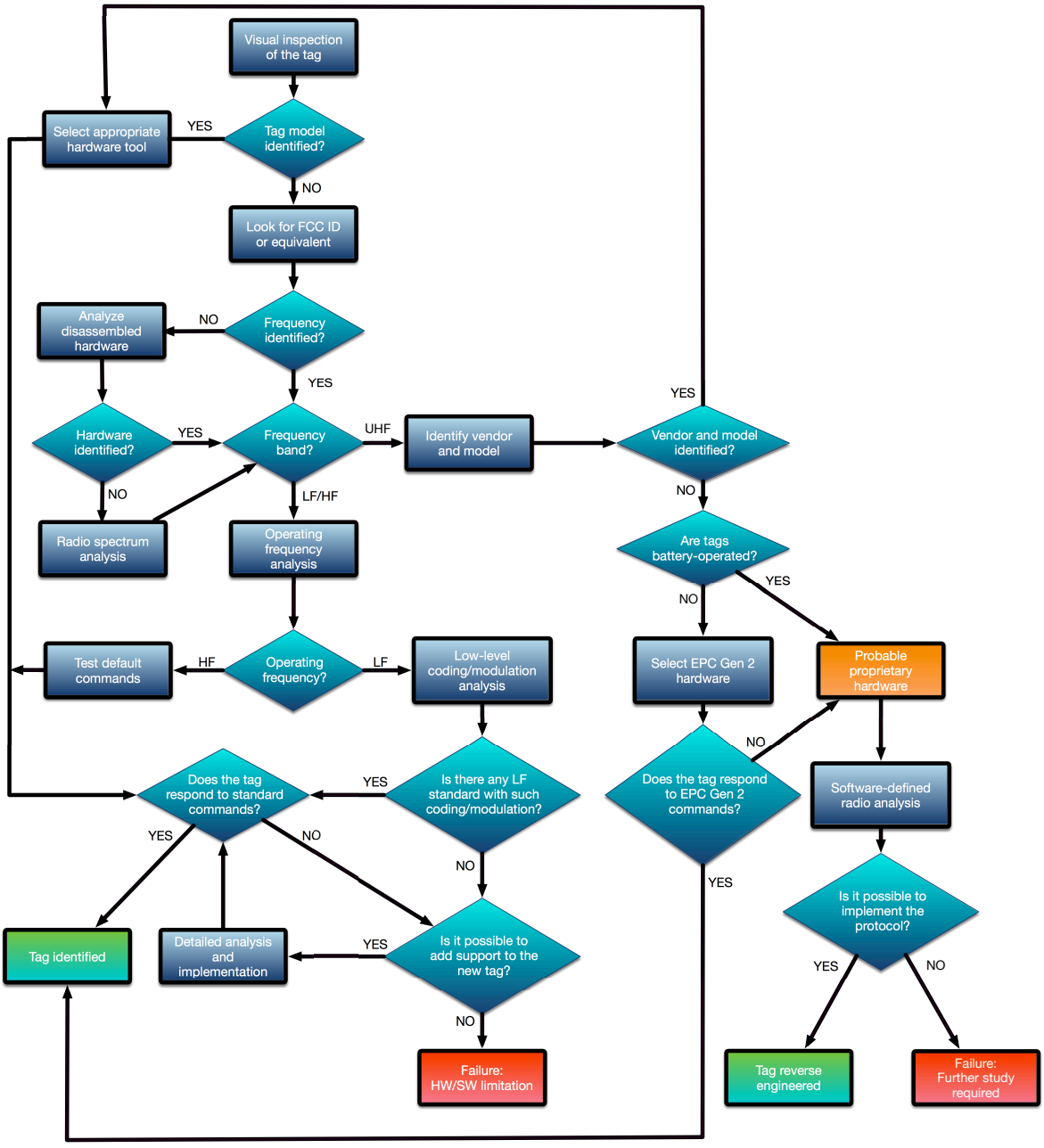


Figure 3.2: Flow diagram of the methodology.

- FCC (Federal Communications Commission) ID or equivalent. One of the most relevant external signs for determining the internal parameters of a tag is its FCC ID (or its equivalent in other parts of the world). The FCC is an agency of the United States that regulates radio communications. Each FCC-approved radio device receives a unique FCC ID that must be marked permanently and has to be visible to the buyer at the time of purchase. Such an FCC ID is composed by 4–17

alphanumeric characters. The first three characters are the Grantee Code, which identifies the company that asks for the authorization of the radio equipment. The rest of the characters (between 1 and 14) are the Product Code. If there is an FCC ID label on an RFID tag or on a reader, it is possible to obtain through the FCC ID search page [82] information like the name of the company that has applied for the authorization, the lower and upper operating frequencies, block diagrams, schematics, and even external/internal photos of the device.

- Frequency band detection. In most commercial systems it is not common to show external clues about the characteristics of a tag so, in these cases, a detailed analysis has to be carried out. The first parameter to be determined is the tag operation frequency. Most tags use LF, HF or UHF bands. If through the previous steps of the methodology it is not possible to determine the frequency, two additional processes can be performed:

  – Disassemble and analyze the hardware. This step aim is to study the internal components in order to determine the operation frequency. The most interesting elements are the ones related to the radio interface: transceivers, amplifiers, crystals and filters allow us to determine the operation band and then estimate the frequency. In this case, transceiver datasheets are the fastest way to obtain an accurate frequency value. RFID readers are usually really easy to disassemble, but RFID tags require more sophisticated tools and techniques.

  – Radio spectrum analysis. In this case, a spectrum or network analyzer, or an oscilloscope, is used to detect the operation frequency. The objective of such an analysis is to determine the resonant frequency of a passive RFID tag. The process models the RFID tag as a simple RLC parallel resonant circuit, what allows for obtaining the resonant frequency easily through Thomson equation:

$$f_r = \frac{1}{2\pi\sqrt{LC}}$$

    where L is the inductance and C is the capacitance. The key for measuring the resonant frequency is the fact that the impedance of the measuring antenna, the reflection coefficient (that measures how much of an electromagnetic wave is reflected by an impedance discontinuity) and the transmission coefficient (that measures how much of an electromagnetic wave passes through a surface) change significantly at frequencies in the vicinity of the RFID tag resonant frequency, f_r. Therefore, the resonant frequency can be determined by

scanning a frequency range and observing when these changes reach their peak. The whole process varies depending on the measurement equipment used, but some manufacturers ease it by offering step-by-step tutorials [83].

There is also a cheaper option for carrying out this analysis that involves working with SDR (Software-Defined Radio) tools like the ones cited in Section 3.2.5, which can be reprogrammed to be used as spectrum analyzers. For instance, the USRP platform [84] has been proposed recently for spectrum monitoring [85] and sensing in cognitive radio applications [86, 87], what can be re-purposed for RFID transmission frequency detection.

- LF/HF tag parameter analysis. If it is verified that the RFID system is LF or HF, the next step of the methodology requires determining the modulation and the coding scheme used by the tag. These tasks involve the use of the appropriate tool to perform a detailed analysis of the radio signals. Such a tool may be a bench oscilloscope with a measuring antenna or similar hardware (e.g., Proxmark 3) that allows for acquiring the RFID signals and then showing the wave received through a display. Thus, the identification is mainly visual, so the analysis becomes easier when the researcher has experience on recognizing the most common modulation and coding patterns. There also exists the possibility of using automatic recognition algorithms, which have been used for a long time (mainly in the military field) [88] but, they have been updated very recently and improved to detect RFID physical layer characteristics [89, 90].

- UHF tag parameter analysis. In the case of RFID UHF systems, the study becomes difficult because, although most passive tags are compliant with the EPC Gen 2 standard, there are a number of companies that make use of proprietary protocols. In such a case, reverse engineering may require using SDR platforms like USRP, MyriadRF or HackRF One to study and then emulate the RFID communications protocol. In the case of the USRP platform, several researchers have presented over the last years really good references on how to implement USRP-based systems for identifying UHF tags [91, 92].

- Standard analysis. Once the frequency, the modulation, and the coding scheme have been obtained, it is straightforward to determine whether there exists an RFID standard compliant with such a configuration. If there is no one, the research may involve reverse engineering a proprietary protocol.

Table 3.1: Physical layer characteristics of the most relevant RFID standards.

Standard	Mode/Type	Communications	Carrier Frequency	Modulations Supported	Coding Schemes	Main Applications
ISO/IEC 11785	FDX/FDX-B HDX	- -	134.2 kHz 134.2 kHz	ASK FSK	DBP NRZ	Animal identification
ISO/IEC 14223	FDX/HDX-ADV	-	134.2 kHz	ASK	PIE	Advanced animal tagging
ISO/IEC 18000-2	Type A Type B	Reader to Tag Tag to Reader Reader to Tag Tag to Reader	125 kHz 125 kHz 125 kHz or 134.2 kHz	ASK ASK ASK FSK	PIE Manchester, DP PIE NRZ	Smart cards, ticketing, animal identification, factory data collection
ISO 21007 (LF)	-	-	125 kHz	ASK	Manchester	Identification of gas cylinders
ISO/IEC 18000-3	Mode 1 Mode 2 Mode 3	Reader to Tag Tag to Reader Reader to Tag Tag to Reader Mandatory Mode Optional Mode	13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz	DBPSK DBPSK PJM BPSK ASK PJM	PPM Manchester MFM MFM PIE MFM	Smart cards, small item management, libraries, transportation, supply chain, passports, anti-theft
ISO/IEC 15693	- -	Reader to Tag Tag to Reader	13.56 MHz 13.56 MHz	ASK ASK or FSK	PPM Manchester	Vicinity cards and item management
ISO/IEC 14443	Type A Type B	Reader to Tag Tag to Reader Reader to Tag Tag to Reader	13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz	ASK OOK ASK BPSK	Modified Miller Manchester NRZ NRZ-L	Proximity cards, item management
ISO/IEC 18092 (NFC)	A B V	Reader to Tag Tag to Reader Reader to Tag Tag to Reader Reader to Tag Tag to Reader	13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz 13.56 MHz	ASK ASK, OOK ASK ASK, BPSK ASK ASK,OOK,FSK	Modified Miller Manchester NRZ NRZ PPM Manchester	Near-field communications
ISO 21007 (HF)	-	-	13.56 MHz	ASK	Miller	Identification of gas cylinders
ISO/IEC 18000-7	-	-	433.92 MHz	FSK	Manchester	Container/pallet tracking and security
ISO 18185-5	Type A Type B	Long-range Short-range Long-range Short-range	433 MHz 123–125 kHz 2.45 GHz 114–126 kHz	FSK OOK BPSK FSK	Manchester Manchester Differential Manchester	Electronic seals of freight containers and other supply chain applications
ISO/IEC 18000-6	Type A Type B	Reader to Tag Tag to Reader Reader to Tag Tag to Reader	860–960 MHz 860–960 MHz 860–960 MHz 860–960 MHz	ASK ASK ASK ASK	PIE FM0 Manchester FM0	Large item management, vehicle identification, supply chain, access/security
ISO 18000-6C (EPC Class 1 Gen 2)	-	Reader to Tag Tag to Reader	860–960 MHz 860–960 MHz	DSB/SSB/PR-ASK ASK or PSK	PIE FM0, Miller	Item management, vehicle identification, supply chain, access/security
ISO 10374	-	-	860–960 MHz, 2.45 GHz	FSK	Manchester	Identification of freight containers
ISO/IEC 18000-4	Mode 1 Mode 2	Reader to Tag Tag to Reader Reader to Tag Tag to Reader	2.45 GHz 2.45 GHz 2.45 GHz 2.45 GHz	ASK ASK GMSK DBPSK or OOK	Manchester FM0 None Manchester	Road tolls, large item management, supply chain, access/security

However, due to compatibility purposes, most massively commercialized LF, HF and UHF tags follow well-known RFID standards. Table 3.1 provides

a fast way to determine the RFID standard from the frequency, modulation and coding previously determined. Such a Table shows the wide variety of implementations, which include modulations like Amplitude-Shift Keying (ASK), Double-Sideband ASK (DSB-ASK), Single-Sideband ASK (SSB-ASK), Phase-Reversal ASK (PR-ASK), Frequency-Shift Keying (FSK), Binary-Phase Shift Keying (BPSK), Differential BPSK (DBPSK), Phase-Jitter Modulation (PJM), On-Off Keying (OOK) or Gaussian Minimum Shift Keying (GMSK); and coding schemes like Differential Bi-Phase (DBP), Dual Pattern (DP), Non-Return-to-Zero (NRZ), Non-Return-to-Zero-L (NRZ-L), Pulse-Interval Encoding (PIE), Manchester, Pulse-Position Modulation (PPM), Modified Frequency Modulation (MFM), modified Miller, or FM0.

- Sniff and emulate. The last step of the methodology is a trial and error process that requires to sniff and emulate communications to perform security tests. Sniffing is not only useful for reverse engineering a communications protocol, but also when trying to understand a well-documented standard protocol. Eventually, once the communications protocol is understood, it may be emulated with the appropriate hardware. For instance, Proxmark 3 official firmware offers off-the-shelf emulation of different standards (i.e., ISO/IEC 14443-A and 14443-B, ISO/IEC 15693) and specific tags (e.g., iClass, MIFARE, HID, Hitag, EM410x, Texas Instruments LF tags, or T55XX transponders). In the case of other platforms, an implementation of the reverse-engineered protocol may be necessary. For example, two cases of UHF RFID tag emulation using an USRP platform are presented in [91, 92].

3.5 Practical Evaluation

In this section, a public transportation card is analyzed. The alias 'T' was given in order to avoid legal issues since there are hundreds of thousands units still in use. It has been used over the last years by the city council of a relevant city in Spain for accessing and paying different services like public transportation, museum access or library loans. It must be noted that the research was conducted with some traces collected by the student Aitor Gaspar Romero in its M. Sc. degree thesis. Furthermore, the need for a scientific methodology arose in order to verify the security claims of one manufacturer of a commercial system used daily for transportation by more than 200,000 users, in the context of a Galician project coordinated by Dr. Tiago Fernández-Caramés.

3.5.1 Applying the methodology proposed

3.5.1.1 Visual Inspection and FCC ID

In plain sight, there are no signs that indicate the frequency band of the RFID cards. No FCC ID or other similar identifiers are included on the tags. It can be assumed that, by the reading range and the amount of information stored, they could be HF tags but a deeper analysis should be performed to verify it accurately.

3.5.1.2 Operating Frequency and Modulation

When using Proxmark 3, the operation frequency can be determined by first placing one of the antennas (LF or HF) far from the tag analyzed and then executing the command `hw tune`.

A sequence diagram that illustrates the inner workings of the Proxmark 3 when executing such a command is presented in Figure 3.3. The sequence begins with the execution of the command, which sends a request to the Proxmark 3 ARM microcontroller through the USB. Next, the microcontroller asks the FPGA for the ADC values when tuning the LF and HF antennas to different frequencies. Eventually, the voltages associated with such frequencies are obtained and presented to the user.

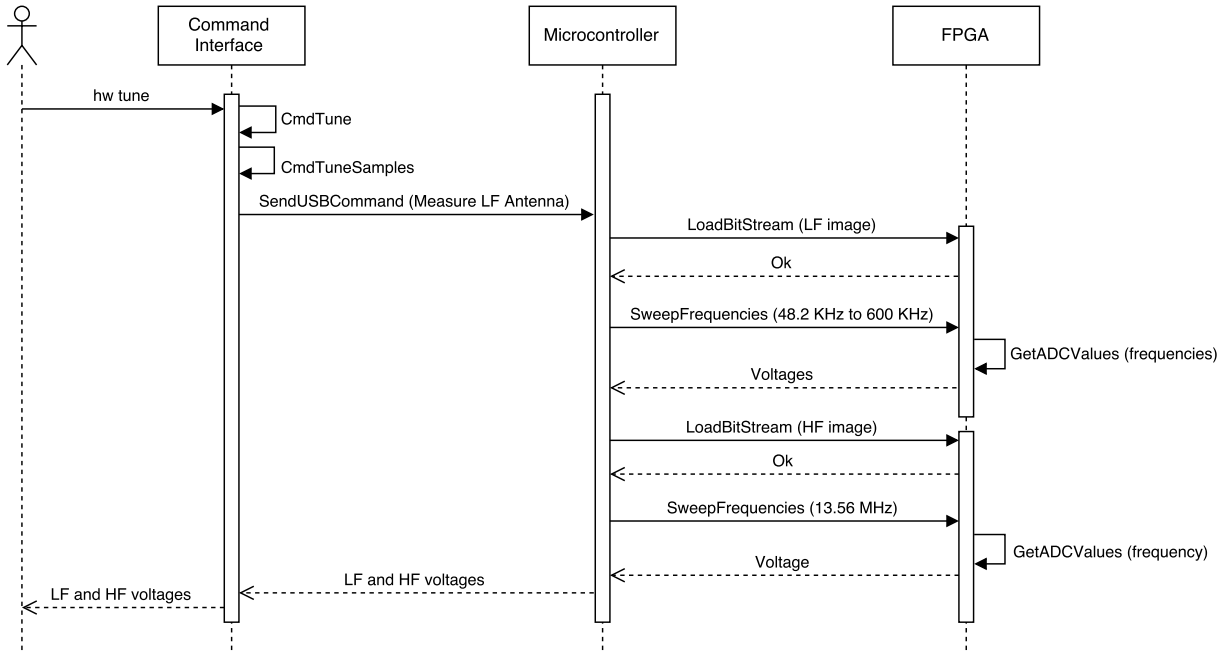


Figure 3.3: Sequence diagram of the command hw tune.

In order to determine the influence of the RFID tag analyzed on the reader (i.e., the Proxmark 3), the same operation has to be repeated next to such a tag: the operation

frequency will be the one where the Proxmark 3 indicates that the voltage has dropped remarkably. If one of the antennas (HF or LF) does not show any changes in voltage for all the frequencies, it must be replaced by the other one and the same steps previously described have to be carried out again. This process confirmed that the transportation card works in the HF band.

Once the radio frequency was obtained, the next step was to decide which of the possible standards the tags followed and then the modulation could be determined. Figure 3.4 illustrates the data of the RFID card decoded after trying one by one all the possible combinations defined by the most popular standards: first, ISO/IEC 15693 was tested, then ISO/IEC 14443-A and, finally, ISO/IEC 14443-B. In this last case, the command for reading tags [93] sends an ATQB command (0x05, 0x00, 0x08, 0x39, 0x73) and records the tag's answer. According to the standard, the second value of the output can be either 0x00000000 or 0x00000001. If it is "1", it means the reply from the tag was received properly. If it is "0", it means that not all bytes (or none) were received.

In the specific case of the previous tag, the answer was "3 1 e" so the second value ("1") means that the tag is actually compliant with ISO/IEC 14443-B. Figure 3.5 shows a simplified sequence diagram of the successful detection of an ISO/IEC 14443-B tag through Proxmark 3.

```
proxmark3> hf 15 reader
#db# 0 octects read from IDENTIFY request:
#db# 0 octects read from SELECT request:
#db# 0 octects read from XXX request:

proxmark3> hf 14a reader
iso14443a card select failed

proxmark3> hf 14b read
#db# 3 1 e
```

Figure 3.4: Determining the RFID standard of an HF tag.

Furthermore, Proxmark 3 is able to return the data after issuing the command hexsamples, thus showing the UID and additional control bytes (in Figure 3.6).

3.5.1.3 Determining the Underlying Protocols

ISO/IEC 14443 is a 13.56 MHz-based standard that defines proximity RFID systems usually related to payment cards. It consists of four parts: (1) physical characteristics, (2) RF power and signal interface, (3) initialization and anti-collision, and (4) transmission protocol. It also defines two kinds of tags (type A and type B) which differ in parts (2) and (3). Table 3.2 shows the differences in terms of modulation and coding between both types (in such a table the reader is called PCD, Proximity Coupling Device, and the tag is the PICC, Proximity Integrated Circuit Card).

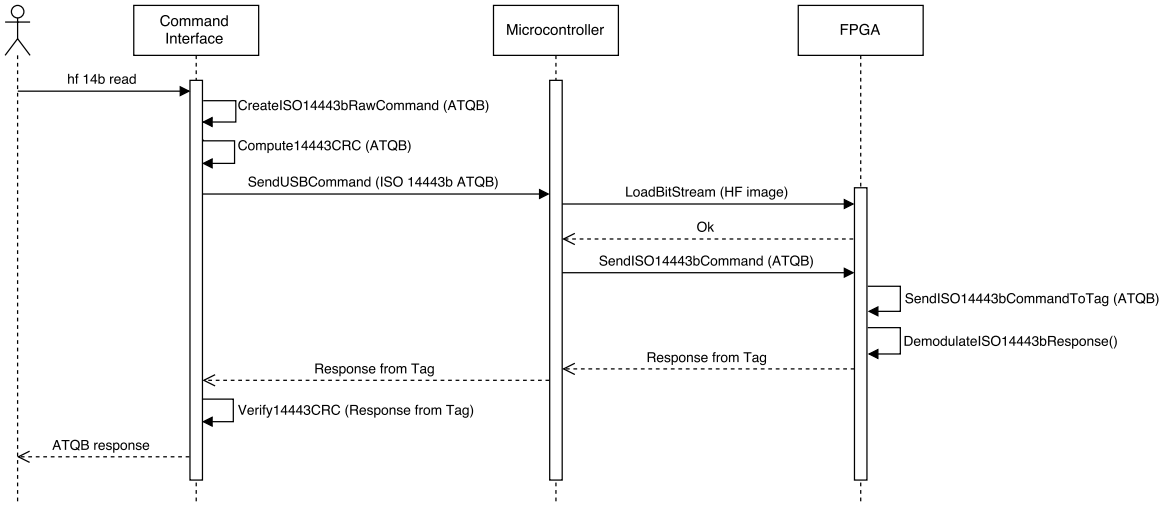


Figure 3.5: Simplified sequence diagram of the successful identification of an ISO/IEC 14443-B tag.

```
proxmark3> data hexsamples
50 08 5c XX 7e XX 4f 44
4b 33 22 XX 74 XX 44 44
```

Figure 3.6: UID and control bytes from an ISO/IEC 14443-B compliant card.

Table 3.2: Modulation and coding used by ISO/IECs 14443-A and 14443-B.

Technology	**Type A**	**Type B**
PCD to PICC	ASK 100% Modified Miller, 106 kbps	ASK 10% NRZ, 106 kbps
PICC to PCD	Load Modulation Subcarrier fc/16 OOK Manchester, 106 kbps	Load Modulation Subcarrier fc/16 BPSK NRZ-L, 106 kbps

3.5.1.4 Reverse-Engineering the Communications Protocol

The first step for reverse-engineering the communications protocol consisted in obtaining a good set of data samples of the communications carried out between each card and the reader. Data samples were taken during real trips in public transportation. A laptop with the Proxmark was carried in a backpack, while the RFID antenna cable was placed along the sleeve of a jacket until reaching the researcher's hand, where the antenna captured the dialog between the card and the reader. Once the radio signals were captured by the antenna, they were demodulated and decoded with Proxmark 3. The main problem with this setup was electric noise: many samples were lost because they became corrupted. None of the first ten capturing attempts was successful, and it was required to perform numerous tests and try three different 'T' cards to get a good data set. Eventually, a good set of traces was collected (one of them is shown in Table 3.3).

Table 3.3: Example of an M/T trace.

Timestamp	RSSI	Device	Payload	Additional information
0	142	TAG	50 08 10 2a 1d 53 4e 44 4b 33 81 93 bc 3f	
1398	112	TAG	00 78 f0	
854			05 00 00 71 ff	
11500			05 00 00 71 ff	
11478			06 00 97 5b	
46342			05 00 08 39 73	
1908			1d 08 10 2a 1d 00 08 01 00 94 60	
554	296	TAG	00 78 f0	
3566			02 80 26 4f 11 0a e7 de	
3146	116	TAG	02 00 14 98 70 10 01 01 76 55 72 90 00 73 65	
36188			03 80 32 00 00 18 ea 98	
1852			00 01 00 00 00 00 00 00	** Fail CRC **
480			00 90 00 1d fe	** Fail CRC **
3676			02 80 2e 01 00 20 43 2f	
2870	203	TAG	02 01 01 e0 f5 ff f5 ff 00 00 00 00 01 f4 07 06 a9 8c ff 00 11 03 e8 00 00 b9 0b ff 00 02 00 01 48 90 00 26 57	
48				(SHORT)
3798			03 80 30 00 00 1d 31 f6	
1580			03	(SHORT)
17462			02 80 28 00 00 04 75 39 34 0d 3a 07 d3	
5778				(SHORT)
34972			03 80 2a 01 00 24 00 15 00 4b 00 01 48 41 19 09 01 00 28 01 37 e5 8c 18 21 10 00 c2 01 01 09 23 00 10 01 00 00 4b d4 72 2b eb 04 ca 20	
14542	203	TAG	03 b3 56 ee 2c 90 00 e6 01	
197304			05 00 08 39 73	
804			33 81 93 bc 3f	**FAIL CRC**

In order to analyze the collected traces, it is needed to understand ISO/IEC 14443-B and to determine the meaning of the different messages, which were not encrypted. The following are the steps performed by a regular ISO/IEC 14443-B system:

1. The tag awaits for a REQB command.
2. The reader sends the REQB.
3. If the AFI (Application Family Identifier) of the REQB is the one expected, the tag answers with the ATQB and waits for an ATTRIB command.
4. The reader sends the ATTRIB command.

5. If the ATTRIB command is the one expected, the tag sends the ATA (also known as the ATATTRIB, Answer-to-ATTRIB).

6. Finally, the tag commutes to the active state, where it is able to exchange data commands with the reader until it receives a DESELECT and commutes to a HALT state.

Then, when the tag is in the active state, it can send three types of messages: i-block, s-block, or r-block. The first one is used for transmitting and asking for data from the application layer. The others are for protocol operations or are related to data from lower layers. Table 3.4 describes the structure of an i-block, which is the only block that appears in the traces of the 'T' cards.

Table 3.4: Structure of an i-block.

	PCB	**CID**	**NAD**	**Payload**	**CRC-B**
Length	1 byte	1 byte (optional)	1 byte (optional)	N bytes	2 bytes
Meaning	Protocol control	Card ID number	Node Address (for logic addresses)		Cyclic-Redundancy Check

Table 3.5: Structure of an ISO/IEC 7816 APDU command.

Field	**Description**	**Length (bytes)**
Header	CLA	1
	INS	1
	P1 and P2	2
Lc	Number of bytes transmitted	0, 1 or 3
Data	Payload	Lc
Le	Number of bytes of the response	0-3

After analyzing a number of traces, it was concluded that the information contained in the i-blocks was compliant with ISO/IEC 7816, whose typical APDU (Application Protocol Data Unit) follows the structure shown in Table 3.5. The CLA byte specifies the command class: if it is equal to 80, or greater (except for FF that is not a valid value), it means that proprietary commands are used. The same happens with the byte INS which identifies the type of command. The third field of the header are bytes P1 and P2 that, in general, refer to memory positions on the card, but may actually indicate any parameter of the command. Regarding the answers to ISO/IEC 7816 commands, they are conformed by two bytes (SW1 and SW2) which are encoded according to Table

Table 3.6: Common answers to ISO/IEC 7816 commands.

	SW1-SW2	Meaning
Normal processing	90 00	Ok
	61 XX	XX bytes are still pending to be sent
Warning processing	62 XX	State of non-volatile memory is unchanged
	63 XX	State of non-volatile memory has changed
	64 XX	State of non-volatile memory is unchanged
Execution error	65 XX	State of non-volatile memory has changed
	66 XX	Security-related issues
	67 00	Wrong length
	68 XX	Not supported functions in CLA
	69 XX	Command not allowed
	6A XX	Wrong P1-P2 parameters
Checking error	6B 00	Wrong P1-P2 parameters
	6C XX	Wrong LE field. There are XX bytes available
	6D 00	Instruction code not supported or invalid
	6E 00	Class not supported
	6F 00	No precise diagnosis

3.6. The most common answer during a correct sequence of commands is 90-00 but the execution of the sequence can be successful and return a different response.

Once the basics of ISO/IECs 14443-B and 7816 were understood, it was then possible to process the traces generated by the public transportation system. First, it must be noted that commands of Table 3.3 that include messages like "**FAIL CRC**" and "(SHORT)" must be excluded from the analysis, since they are corrupted. In the same way, a good trace should have alternating messages from the tag and the reader, instead of containing two consecutive messages from the same device (except from the case when the reader is looking for tags). Taking these facts into account, Table 3.7 indicates the relationship between the standard commands and the trace shown in Table 3.3. As it can be observed, the sequence of messages is not correct: some are missing, others have not been received in the correct order.

After analyzing a great deal of traces of the 'T' system, it was found that a sequence of six pairs of commands was repeated constantly. For the sake of brevity, and due to legal issues, only the first two pairs of commands will be detailed.

The first command is always the same: '02 80 26 4f 11 0a e7 de'. The standard ISO/IEC 14443-B indicates that it is an i-block whose first byte means that it is block number 0 and that it does not contain CID or NAD. The last two bytes of the message are the CRC-B so the transmitted data are composed by five bytes (80 26 4f 11 0a). These bytes follow ISO/IEC 7816: the first one is the CLA byte (80, proprietary command), the second one is the field INS (26), the third and the four (4f 11) are P1

Table 3.7: M/T trace messages analyzed.

Timestamp	RSSI	Device	Payload	Additional information	Message
0	142	TAG	50 08 10 2a 1d 53 4e 44 4b 33 81 93 bc 3f		ATQB
1398	112	TAG	00 78 f0		ATATTRIB
854			05 00 00 71 ff		REQB
11500			05 00 00 71 ff		REQB
11478			06 00 97 5b		
46342			05 00 08 39 73		REQB
1908			1d 08 10 2a 1d 00 08 01 00 94 60		ATTRIB
554	296	TAG	00 78 f0		ATATTRIB
3566			02 80 26 4f 11 0a e7 de		
3146	116	TAG	02 00 14 98 70 10 01 01 76 55 72 90 00 73 65		
36188			03 80 32 00 00 18 ea 98		
1852			00 01 00 00 00 00 00 00	** Fail CRC **	i-Block
480			00 90 00 1d fe	** Fail CRC **	
3676			02 80 2e 01 00 20 43 2f		
2870	203	TAG	02 01 01 e0 f5 ff f5 ff 00 00 00 00 01 f4 07 06 a9 8c ff 00 11 03 e8 00 00 b9 0b ff 00 02 00 01 48 90 00 26 57		
48				(SHORT)	
3798			03 80 30 00 00 1d 31 f6		
1580			03	(SHORT)	
17462			02 80 28 00 00 04 75 39 34 0d 3a 07 d3		
5778				(SHORT)	
34972			03 80 2a 01 00 24 00 15 00 4b 00 01 48 41 19 09 01 00 28 01 37 e5 8c 18 21 10 00 c2 01 01 09 23 00 10 01 00 00 4b d4 72 2b eb 04 ca 20		
14542	203	TAG	03 b3 56 ee 2c 90 00 e6 01		
197304			05 00 08 39 73		REQB
804			33 81 93 bc 3f	**FAIL CRC**	

Table 3.8: Responses collected for the first command

Trace\#Byte	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Card 1-Trace 1	02	00	14	98	70	10	01	01	76	55	72	90	00	73	65
Card 1-Trace 2	02	00	15	98	70	10	01	01	76	55	72	90	00	e2	30
Card 1-Trace 3	02	00	17	98	70	10	01	01	76	55	72	90	00	c0	9b
Card 2-Trace 1	02	01	40	98	70	10	01	02	07	90	31	90	00	65	ac
Card 2-Trace 2	02	01	42	98	70	10	01	02	07	90	31	90	00	47	07
Card 3-Trace 1	02	00	0c	98	70	20	01	01	69	87	97	90	00	ba	6a

Table 3.9: Responses to the second command.

Trace\#Byte	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Card 1-Trace 1	3	0b	89	87	0	0	10	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	90	0	1d	ce
Card 1-Trace 2	3	0b	89	87	0	0	10	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	90	0	1d	ce
Card 2-Trace 1	3	0b	89	87	0	0	10	0	0	0	3	b5	8c	f5	8d	0	10	30	0	0	0	0	0	0	0	90	0	a8	0c
Card 3-Trace 1	3	0b	89	87	0	0	20	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	90	0	8	7d

and P2 (parameters of the command), and the fifth (0a) is the field LE which indicates the number of expected bytes to be received from the tag (i.e., 10 bytes are expected). This first command is followed by the first response of the tag. As it can be observed in Table 3.8, it is almost the same for every tag. Its structure is as follows:

- Byte 1 (02): it indicates that it is an i-block 0.
- Bytes 2-13: ISO/IEC 7816 data. For instance, bytes 2-3 indicate the total number of trips carried out with the card.
- Bytes 12-13 contain the state of the execution of the command (90-00, successful execution).
- Bytes 14-15: CRC-B.

The second request is also always the same: '03 80 32 00 00 18 ea 98'. Byte 1 (03) means that it is i-block 1. Bytes 2-6 are ISO/IEC 7816 data. Since CLA is 80, the command is proprietary. INS is equal to 32, P1 and P2 are 00 and 00, and LE (expected length of the answer) is 24 bytes. Finally, bytes 7-8 are the CRC-B.
The second answer is related to the use of special fares during a trip. Table 3.9 show examples of traces for different cards that have diverse fares. The data are structured as follows:

- Byte 1 (03) indicates that it is i-block 1.
- Bytes 2-27: ISO/IEC 7816 data. For instance, bytes 12-13 and 14-15 indicate the activation and expiration dates of a special fare, and byte 11, the type of fare (e.g., 1 for standard, 3 for reduced fare).
- Bytes 28-29: CRC-B.

The rest of the pairs answer-response contain other interesting information like the balance of the card, the place where the card was recharged (e.g., ATM, bank) or the data about each trip performed (i.e., cost, date, time, line and vehicle number).

3.5.1.5 Security Evaluation

After all the analysis, it was not found a severe security threat in the system but there are several issues regarding data privacy that developers should consider. The main problem is that the RFID communications are performed in plain text, without any kind of ciphering, what leads to the possibility of snooping and emulating them. Thanks to that, an attacker can emulate an unauthorized reader and obtain private

data like the credit balance or the specific characteristics of the trips of a user. Note also that many smartphones currently support NFC, which is partially compatible with ISO/IEC 14443-B tags, and it is straightforward to develop an Android application to read the data (there have already been attacks to ISO/IEC 14443-A tags using mobile phones [94]). The complete disassembling of the protocol also opens the possibility to perform Man-in-the-Middle (MitM) attacks, where a third device might alter the data on the RFID transactions in order to get certain benefits (e.g., to avoid discounting credit on the card).

3.6 Conclusions

RFID is one of the key technologies for the development of IoT applications, specifically public transport ones, but it is important to take security into consideration to avoid privacy and security risks. This chapter included two main contributions aimed at fostering security in RFID-based IoT applications. First, due to the lack of a step-by-step methodology for auditing RFID communications security, a novel approach was presented. Second, the application of such a methodology was illustrated through a real-world application where flaws were detected. The tests performed have shown that, by using a device like Proxmark 3 and a minimum of reverse engineering skills, it is possible to extract private information from the cards evaluated, to capture tag-reader communications to perform MitM attacks, and to emulate both readers and tags.

The final conclusion is that, although many applications can make use of advanced security RFID measures, certain developers have adopted the technology without taking such mechanisms into account. In the case of the transportation tag analyzed, its security can be improved by adding a higher security layer (e.g., encrypting internal data), enabling some of the already existing security protocols, or simply replacing the tag with a more secure version.

To sum up, a methodology like the one proposed can help IoT application developers to perform audits and determine the security level of an RFID system before taking it from a test environment to a mission-critical scenario.

Chapter 4

Military Broadband Wireless Communication Systems

4.1 Introduction

The motivation to develop military disruptive technologies is driven by new operational needs and the challenges arising from modern military deployments. The fast evolution of Commercial Off-The-Shelf (COTS) technologies is one of the primary reasons to analyze the usage of these up-to-date technologies to fulfill current tactical deployment necessities.

The context of this chapter is framed within the Exploratory Team (ET) of the Information Systems Technology (IST) panel of North Atlantic Treaty Organization (NATO) Science and Technology Organization (STO). The ET known as IST-ET-068: 'LTE vs. WiMAX for Military Applications' was launched in 2012 to analyze the applicability of the 4G wireless standards deployed in a tactical environment. Its main objective was to assess whether it is worth adapting high-performance 4G standards or if it is better to develop a new system from scratch in order to cover imminent demands in the tactical domain. Previous and on-going NATO research was examined: Cognitive Radio (I and II: IST-104-RTG-035 & RTG-055, SDR (IST-080), Military Communications and Networks (IST-092), Tactical Communications in Urban Operations (IST-067), Emerging Wireless Technologies (IST-070) and Next Generation Communications (IST-105), among others; including also trends on this field. Furthermore, the background of the different partners in national and international initiatives was essential: the Communications Research Centre (CRC) in Canada, the Fraunhofer institute (FKIE) in Germany, the Havelsan company in Turkey, and Indra Sistemas S.A. in Spain. Moreover, it was also important the experience acquired with

the design and implementation of the Mobile WiMAX standard using a Software Defined Radio (SDR) architecture.

The strategic advantages of broadband technologies massively deployed in civil scenarios, such as 4G Worldwide Interoperability for Microwave Access (WiMAX), LTE and WLAN are examined. The military Data Distribution Subsystems (DSS) represents the scenario with the greatest similarity with commercial wireless technologies in terms of communication range, requested services and network capabilities support. Nevertheless, it is not possible to straight use these technologies due to the specific characteristics of tactical environments. The scenario-based approach proposed together with a deep analysis of modern civilian waveforms is a guarantee to minimize the impact and cost of a new Military Broadband Wireless Communication System (MBWCS) development. Furthermore, current market COTS 4G-based tactical products and on-going international waveform development initiatives, such as COALWNW, ESSOR, NATO Narrowband WF and other MANET/Ad-Hoc were also examined to confirm that a 4G-based MBWCS can coexist, and that it makes sense to devote effort to its definition and development.

The analysis proposed is able to determine the technologies required in the middle and long term to comply with the operational requirements, and the state-of-the-art COTS military equipment that covers such needs. After the definition of the NATO scenarios, an analysis of the operational requirements is performed. In a second step, the technical requirements are derived and used as input for the applicability analysis. For this work, it was necessary to characterize the technical implementation requirements of 4G standards, and analyze capabilities, aptitudes and challenges when deploying a tactical network. Also, modifications and their related techniques are identified and evaluated for the three standards.

This chapter is based on the following publications [95–102] and is structured as follows. Section 4.2 provides a brief overview of the state-of-the-art of WiMAX, LTE and WLAN broadband wireless standards. Section 4.3 characterizes the relevant scenarios in which these technologies may be applicable within NATO countries tactical deployments. The operational requirements and end-users needs that will drive the technical analysis are explained in Section 4.4. The methodology and the applicability analysis results are reflected in Section 4.5. Finally, Section 4.6 is devoted to the conclusions.

4.2 4G commercial broadband technologies

Commercial broadband cellular technologies provide high value for situation awareness, monitoring and intervention, distributed command and control, and public participation in crisis management. Taking into account their features, research efforts from industry

Table 4.1: Comparison between WiMAX, LTE and Wi-Fi.

Metric	**WiMAX 2 (IEEE 802.16m)**	**LTE-A (3GPP Rel-10)**	**Wi-Fi (IEEE 802.11n)**
Technology orientation	Flat All-IP architecture initially born as Fixed WiMAX. Data-oriented evolved to support voice.	Focused in voice, progress gradually for data services (GSM/GPRS/EGPRS/UMTS/HSPA).	
Frequency bands	LOS: 10-66 GHz NLOS: 2-11 GHz licensed and unlicensed bands	700; 1,700; 1,900; 2,100; 2,500 and 2,600 MHz	2.4 and 5 GHz
FFT Size	1.25 MHz to 28 MHz / 128 - 2,048	128 - 2,048	20 MHz or 40/64 or 128
Physical layer	DL/UL: OFDMA	DL: OFDMA, UL: SCFDMA	OFDM (200 channels)
Duplex mode	TDD, FDD and H-FDD	TDD, FDD (originally more interested in FDD)	TDD
Modulations	QPSK, 16-QAM and 64-QAM	QPSK, 16-QAM and 64-QAM	BPSK, QPSK, 16-QAM and 64-QAM
Mobility	Max. 350 km/h	Max. 350 km/h	200 km/h (IEEE 802.11p)
Coverage	Up to 50 km	Up to 100 km	> 200 m
Operating bandwidth	5, 7, 8.75, 10, 20, and 40 MHz (up to 100 MHz with carrier aggregation).	Up to 100 MHz	5, 10, 20 and 40 MHz
Peak data rate	DL: >350 Mbps (MIMO 4×4), UL: >200 Mbps (MIMO 2×4) with 20 MHz and FDD	DL: 1 Gbps, UL: 500 Mbps	6-600 Mbps (MIMO 4×4)
Average cell spectral efficiency	DL: >2.6 bps /Hz (MIMO 2x2), UL: >1.3 bps/Hz (MIMO 1x2)	DL: >1.6-2.1 bps /Hz, UL:> 0.66-1 bps/Hz	>3 bps/Hz
Latency	Link layer < 10 ms, Handover < 30 ms	Link layer < 5 ms, Handover < 50 ms	Handover < 50 ms (IEEE 802.11f and 802.11r)
Security	WPA2	WPA2	WPA2 (802.11i)
VoIP capacity	>30 users per sector / MHz (TDD)	>80 users per sector / MHz (FDD)	12 active calls IEEE 802.11 a/b/g/n
Additional features	QoS	QoS	QoS (IEEE 802.11e), Dynamic Frequency Selection and Transmit Power Control (IEEE 802.11h)
Roadmap	• IEEE 802.16-2012 (Revision of IEEE 802.16 including Std 802.16h, IEEE Std 802.16j and IEEE Std 802.16m WirelessMAN-Advanced is part of IEEE Std 802.16.1). • IEEE 802.16p-2012 (First Amendment to IEEE 802.16-2012), M2M applications. • IEEE 802.16n-2013 (Second Amendment to IEEE Std 802.16-2012), Higher Reliability Networks. • IEEE 802.16q-2015 (Third Amendment to IEEE Std 802.16-2012), Multi-tier Networks.	• Rel-12, 2015 (new type of subcarrier, active antenna systems, ProSe, PTT, eMBMS). • Rel-13, 2016 (LTE in unlicensed spectrum with Licensed-Assisted Access (LAA), Carrier Aggregation up to 32 component carriers as well as flexibility to aggregate large numbers of carriers in different bands, enhancements for MTC, full-dimension MIMO, indoor positioning ··· • Rel-14, 2017 (5G requirements, Multimedia Broadcast Supplement for Public Warning System, User Control over spoofed callS, Location services, Mission Critical Video over LTE, UICC power optimization for MTC···	• IEEE 802.11aa-2012 (MAC Enhancements for Robust Audio Video Streaming). • IEEE 802.11ad-2012 (Enhancements for Very High Throughput in the 60 GHz Band). • IEEE 802.11ae-2012 (Prioritization of Management Frames). • IEEE 802.11ac-2013 (Enhancements for Very High Throughput for Operation in Bands below 6 GHz). • IEEE 802.11af-2013 (Television White Spaces (TVWS) Operation). • IEEE 802.11ad-2014 (transfer rate up to 7 Gbps).

have recently been focused on Machine Type Communications (MTC), as they are a key enabler for large-scale distributed Cyber-Physical Systems (CPSs).

WiMAX [103], LTE [104] and WLAN [105] are representative although competing technologies. Hence, there is a WiMAX-versus-LTE-versus-WLAN controversy to

declare which one is the best. From a military point of view, there is a need to address which one, or which parts of them, best fits the operational requirements and target tactical deployments, but ignoring business related issues. These mainstream technologies resemble each other in some key aspects including scalable bandwidth, seamless mobility, operating in licensed spectrum bands, strong QoS mechanisms, and pure IP architecture. However, these technologies have evolved from different origins and differ from each other in certain aspects such as design choices, architecture, protocol stacks, air interface and security, as it can be seen in Table 4.1.

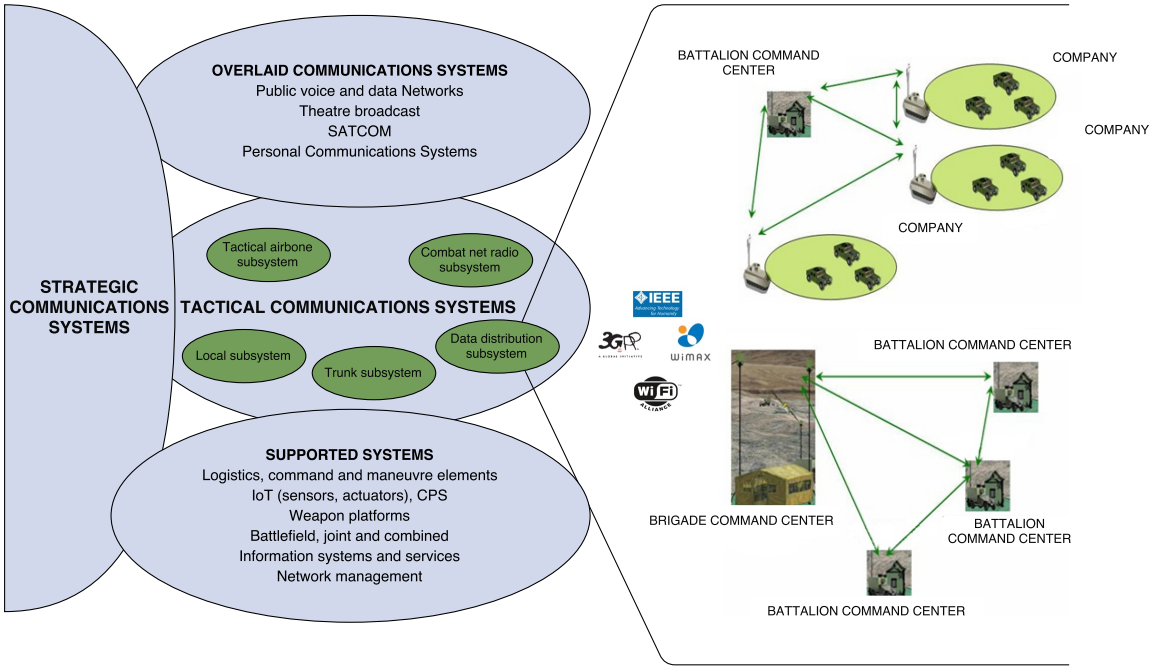


Figure 4.1: Architectural framework for the tactical communications system.

4.3 Definition of target scenarios

The objective of the approach followed to Network Centric Warfare (NCW)/Network-Enabled Capability (NEC) is to increase interoperability among networks compliant with the NATO NEC Feasibility Study recommendations, national operational needs and the proposed 'scenario based' methodology. Five main target scenarios were identified within the land army to develop the MBWCS (Figure 4.1):

Type A: Battalion & Brigade level communication.

This scenario can be defined as wireless communications between several Command and Control (C2) centers at battalion level and a C2 at Brigade level (also between two Brigade C2s or even division). The Battalions radius of action is around 60 km,

while the Brigades radius of action will be approximately 150 km. Brigades can be composed of 4-20 battalions. Maximum distance in just one hop between Command Centers (CCs) is approximately 50 km. It is a Line-Of-Sight (LOS) environment with no mobility and no need for Mobile Ad hoc Network (MANET) functionality on one side, and a 100-150 Km single-hop range with mobility and a mesh scheme on the other one.

Type B: Company & Battalion level communication.

This scenario considers the provision of wireless communications between several C2 centers at Company and Battalion level. The environment fits in a typical rural environment with no significant obstacles and almost LOS between the different elements of the communication network. The maximum range of a Company is about 20 km, while at Battalion level is 60 Km. Battalions may be composed of 3-15 companies and the maximum distance in a single hop between C2 will be around 20 km. Mobility will be considered at both hierarchy levels. A mesh communication scheme would be adequate, i.e., a CC at Company level may contact with battalion level through other Company CCs within the range limit of communication.

Type C: Wireless communication infrastructure at Battalion or Command HQ.

This scenario covers a wireless communication infrastructure inside a Command Post (CP) to substitute traditional optical fiber deployments. It is typically a rapid deployment at Battalion HQ or CP, equivalent to NATO Battalion CC. Hence, MBWCS technology can be deployed with fixed infrastructure allowing coverage within a radius of 2 km. The level of deployment risk and subsequent enhancements to existing COTS technologies will be negligible.

Type D: Company level communications with limited mobility.

This scenario can be defined as wireless communications to support Company CP communications (equivalent to a forward operating base). Fixed infrastructure with no or limited mobility is supported either via vehicles serving as a central access point to the network with antenna masts that can be elevated to maximize coverage, or through a deployable aerostat with a COTS access point. Typical coverage will be around 5 km. It is expected that the deployment risk will be increased to accommodate enhanced security and robustness.

Type E: Full mobility Company level communications.

This scenario considers wireless communications with platoon deployments or Company/coalition dividing forces. In this scheme, a group can leave a fixed infrastructure network and form an ad-hoc MANET. In addition, robustness to interference and security issues will be key requirements. It is expected that this type of network will

require a significant deployment risk while allowing the most flexible configuration of existing COTS products.

4.4 Operational requirements

A given set of operational requirements grouped by capabilities were analyzed in order to cover the previous scenarios.

4.4.1 Deployment features

The MBWCS shall be a part of a military data network which enables integration of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems. The deployment will depend largely on the hierarchy of the unit. Large units shall have a semi-static or static character with non-restrictive time deployment (in an order of magnitude of hours). Small units will contemplate full mobility with rapid deployment (less than 10 minutes). Regarding the intrinsic features, MBWCS will be within determined ranges in terms of dimension, weight, heat dissipation and power consumption. In scenarios C, D and E, MBWCS target platforms will be portable, easily installable and dismountable. Except for C, hostile environments will be expected.

4.4.2 System management and planning

The MBWCS will provide a simple GUI to enable easy network planning. It will include various user profiles to offer a selection of deployment features adapted to the user requirements. System management will be configured at Brigade level with the option of limited configuration at lower levels. MBWCS will support the ability to decentralize system management functions, plug and play capabilities with autoconfiguration, and local and remote network management (in scenarios similar to Type E, where MANET functionality is required). System management will allow an ad-hoc network to form and separate from the existing network and rejoin an existing fixed infrastructure network, i.e., Type D scenario.

4.4.3 Supported services and applications

The most critical and priority service is voice communication. In this way, Companies and Brigade and Battalion CCs will provide at least a low bandwidth verbal communication and services like PTT. Voice will take always priority over any other type of traffic; instant messaging, critical data and C2 messages, i.e., Blue Force Tracking (BFT).

On the other hand, some important tactical data services, such as operation orders, fire support plans, logistics reports, cryptographic keys, configuration files, as well as e-mails, are also transferred between Brigade and Battalion CCs as well as between Battalion CCs and Companies. Nodes will be able to use IP based military applications such as C2, Combat Management System applications, ILS, surveillance and intelligence applications (map based applications, database lookup, etc). Some rules and parameters will be defined by the state-of-the-art QoS policies, as well as by service prioritization mechanisms.

4.4.4 Network capabilities

NATO Network Enabled Capability (NNEC) allows to exchange timely and secure information between users from different NATO nations. NNEC is implemented over the Network Information Infrastructure (NII). The MBWCS shall support soft handover network mechanisms to support reliable communication in Type B, C and E scenarios where mobility is assumed. For scenarios A and D, no handover is needed.

The MBWCS will forward information through the network, even when the range between communication nodes exceeds the coverage range. The network will adapt the transmission delay for optimization of QoS support.

4.4.5 Supported network topologies

Military networks meet Command, Control, Communications, Computers, and Intelligence (C4I) system requirements facing the moves of users from one network to another or from one access interface to another. This implies the adaptation of the routing and maybe of the addressing. Back-up networks and reconfiguration functions will keep a maximum level of connectivity with adequate QoS. An IP-based, high-speed, extensible and reliable wireless tactical network will be established among land platforms. Nodes connectivity requirements can be categorized as vertical communications up and down the command chain, horizontal between each level, horizontal at each level between adjacent formations, and horizontal and vertical outside the chain of command.

Network architecture primarily addresses Point-To-Multipoint (PMP) or Point-to-Point (PtP) links. These topologies are required in some of the scenarios identified above. Nevertheless, most platforms are mobile, and there is no chance of providing a communication infrastructure among them during the military operations. Therefore, MBWCS should be capable of establishing high-throughput ad-hoc networking for specific scenarios, i.e., MANET is required for small units (Type C, D and E). The mobile ad-hoc network is specially useful in rapid deployments. In PMP deployments suitable for small and big units, it is usual to require equipment that can aggregate

four links. Fully mesh capabilities with network auto discovery and efficient automatic routing are critical at the small units. Relaying capacities can be used for range extension at the same hierarchical level, and between hierarchical levels operating at different frequency bands, i.e., between Brigade and Companies. Network topology sizing will depend on the scenario and the hierarchy level of the unit deployed. A reasonable assumption is 23 users per base station for the specific scenarios A and B, while a lower number, from 5-15 users, will be necessary in scenarios C, D and E. When operating under Emissions Control (EMCON) restrictions, cooperative communications will not be possible.

4.4.6 Mobility capabilities

Brigade typically lacks mobility and presents a fixed infrastructure. On the other hand, Battalion and Company are mobile communication nodes. Land vehicles speed can change from 65 to 150 km/h. For Battalion CCs, the maximum speed to be considered is around 100 km/h and the Armored Combat Vehicles (ACV) used for Company CCs around 150 km/h. A hand-held system can be used by a Company soldier to join the network in the field at speeds up to 5 km/h. Close helicopter support shall be considered at an estimated speed up to 400 km/h.

4.4.7 Security capabilities

Security is a wide and complex field, crucial to support communication between NATO coalition partners, as well as national solutions. The following issues shall be considered:

- **Information Security (INFOSEC)**: the MBWCS will support up to NATO security classification level 3 (NATO SECRET or national equivalent) for big units deployments, and up to level 2 (NATO CONFIDENTIAL or national equivalent) for small units. NATO coalition partners, as well as national security systems with different security levels, will get connected to the networks. Additionally, MBWCS will be able to switch between software or hardware-based ciphering systems.
- **Communications Security (COMSEC)**: the MBWCS shall adapt or use several security mechanisms based on national and coalition specific cryptographic solutions, hence supporting key management features including: Generation, Activation, Deactivation, Reactivation and Destruction of Keys and the Accounting Authentication and Authorization (AAA) concept. Even when critical information is secured (ciphered), the unauthorized user can act as an eavesdropper and start simple communication behavior analysis. Depending on the level of signal

knowledge, the unauthorized user may act as a communication participant while attacking. To prevent the influence of such attacks, several protection mechanisms and Electronic Protection Measures (EPM) features have been identified within Transmission Security (TRANSEC) capabilities: Low Probability of Interception (LPI), Low Probability of Detection (LPD) and Anti-Jamming (AJ).

- **Network Security (NETSEC)**: the MBWCS shall support protection mechanisms including incorrect traffic generation such as denial-of-service attacks (e.g., cache poisoning, message bombing), incorrect traffic relaying (e.g., blackhole, replay, wormhole and rushing attacks, as well as message tampering) and error correction capabilities.

4.4.8 Robustness capabilities

The MBWCS will provide robustness to signal interference and/or loss of network operation. When deployed in locations with other tactical networks, i.e., vehicular deployment, it will provide adequate measures to avoid interference from adjacent users in the same frequency band. For mesh or PMP modes, the network will provide redundancy and be robust to a single point of failure. This may be of the form of a link failure or the failure of a radio, without unduly affecting the overall network performance. Systems will be robust to jamming signals in the form of noise, barrage, and sweep/chirp jamming, supporting techniques to actively track jamming signals and applying automatic jamming avoidance measures. The MBWCS should include cognitive radio and dynamic spectrum management techniques to automatically overcome bad conditions in the communications environment.

The operational requirements for robustness also include the physical attributes of the radio. Generally, this is addressed by the target platform requirements which in turn is dependent on the deployment scenario. Equipment will be physically robust to environmental damage, i.e., shock- and water-proof. The MBWCS will provide the mechanisms to allow fast switching between the technology chosen and back-up/legacy communications in the event of failure. The MBWCS will support an uninterrupted power supply to ensure that a back-up power supply can support around 1-2 hours for big units and a minimum of 15 minutes for small units; maintaining the continuous usage of the radio platform for a minimum of 3 months without interruption for big units; and in the order of magnitude of days for small units. When deployed in a hand-held or man-pack radio configuration, the MBWCS will have power requirements compatible with existing battery capabilities.

4.4.9 Target frequency bands

NATO Band IV, from 4.4 to 5 GHz, allows high throughputs enabling the usage of advanced services with smaller coverage than in HF, VHF or UHF bands. Operational concepts for NATO III+ and IV frequency bands will cover a wideband PtP and PMP radio-link at the higher level of the military echelons with no or limited mobility, hence addressing scenarios Type A and B. Typical channel bandwidth is among 10-20 MHz providing a high data rate backbone. NATO Band I, from 225 MHz to 400 MHz, and its potential migration to 1-2 GHz frequency band (part of the NATO III frequency band) is used between Battalion and Brigade level. This is still the target band for the systems that are currently being developed. This band has restrictions such as the reduction of the channelization bandwidth. Nevertheless, it offers the possibility of a significant increase in the range of communications. Operational concepts for NATO Band I frequency band are mainly addressing scenarios with full mobility and MANET capabilities, at Company level or below (Type D and E), with a typical channel bandwidth of 1.25 MHz and are able to provide data services up to 1 Mbps together with voice services.

4.4.10 Coverage capabilities

In order to increase coverage and allow for higher performances, Brigade Command Center (CC) and its Battalion CCs, as well as Companies, will provide relay functionality in Non Line-Of-Sight (NLOS) conditions either in suburban or in rural areas (including coastal scenarios). Mesh will be considered at least inside Company deployments. Brigade CC and its Battalion CCs will communicate with each other considering that the maximum distance of one hop among them is maximum 60 km for LOS conditions (maybe with degraded performances). The distance is similar in the communication among Battalion CCs. In the case of Battalion CC and its Companies, they will communicate at a maximum distance of 20 km.

4.4.11 Interoperability capabilities

MBWCS will be fully compliant with NATO Reference Architecture and national-wide standards. MBWCS will be compact, reprogrammable and multi-mode, thus providing interoperability on the air by the usage of common waveforms.

4.4.12 Target platforms

According to the scenarios' definition, several objective platforms will be considered. Target vehicle platform will support operations on land vehicles, war ships or helicopters

acting as support of the network. Nevertheless, specific platforms could operate as fixed installations like headquarters in certain scenarios (mainly Battalion, Brigade or upper levels), or hand-held or man-pack platforms at a lower tactical level (mainly companies and platoons). Deployment features and environmental conditions previously explained will be considered.

4.5 Applicability analysis

This research was conducted following a scenario-based layerized approach allocating technical requirements in the involved OSI layers. Cross-layering (CL) is used when several layers are affected simultaneously. Standards compliance and modifications' identification were assessed for each of these layers considering both waveform (WF) and platform (PTF) requirements; concluding whether the functionality can be directly derived from the standards as they are or if, at a high level, modifications are needed. This structure optimizes the comparison between different standards, helping in the definition of the final MBWCS proposal. A cost-benefit analysis of the implementation of the modifications of each one of the standards was performed. The aim is to provide some qualitative metrics about the effort needed for conducting these modifications against the benefits/impact achieved in terms of compliance. In summary, a compliance matrix for technical requirements shows the analysis result with the criteria fully or partially compliant or not. This matrix is essential as guidance for the specification of the ideal MBWCS. The cost-benefit analysis of the implementation of the modifications of WiMAX, LTE and WLAN, and the specifics of scenarios A, B, C, D and E are also considered to structure analysis' outcomes. For the sake of simplicity, this thesis does not go into detail of each one of the scenarios' issues. The aim of this section is to shortly describe the applicability analysis of the targeted standards confronting the identified technical requirements.

4.5.1 Platform requirements

Following, some of the PTF-only requirements are cited: reduced weight and dimension equipment, with the highest level of integration, ease of installation and plug and play (Portable platforms: man-pack with size 257 cu. in. (438 cu. in. with battery), maximum 3" H × 10" W × 9" D (without battery bucket), 3" H × 10" W × 14" D (with battery bucket), weight 9 lbs. (14 lbs. with battery) and hand-held with size 28 cu. in. and weight 1.7 lbs with battery and antenna; Vehicular platforms: 5.472" / 7.67" H × 11.4" / 15.74" W × 12.59" / 13.38" D). Antennas shall be carefully chosen considering deployment type scenario: fixed/vehicular/man-pack/hand-held, external/internal

location and height consistent with coverage range (according to free Fresnel zone), polarization, beamwidth, gain ... Omnidirectional antennas shall be chosen when high mobility is required (scenarios Type C, D and E) along with the incorporation of features like auto-acquisition, optimum orientation, tracking ...

The MBWCS shall provide 28.8-87.2 kbps data bandwidth depending on chosen codec, for narrowband voice, wideband voice or VoIP service. For example, a default codec for narrowband voice (such as G.711, G.726, G.729AB and G.723.1), a default codec for wideband voice (such as G.722, G.722.2) and a default codec for fax (such as G.711).

A Simple Network Management Protocol (SNMP)/Hyper Text Transfer Protocol (HTTP) based network management is needed to support remote network management. The network shall be configured in all the elements of the architecture (BS, CPE and backbone) to provide redundancy in such a way that any loss of a node will not result in the degradation of services or loss in communications. ARP protocol for connections with external networks (Ethernet) and special mechanisms, e.g., gratuitous ARP, are needed together with systems for avoiding intrusion and/or tampering, e.g., firewalls, anti-virus software or malware scanners.

Procedures, design values and equipment shall be compliant with the considerations from military standards: MIL-STD 810G, MIL-STD 461F, MIL-STD-1275 ...

The MBWCS shall supply a common interface (connectors to radios and software) to support possible external crypto modules and a FILL interface for security material handling. Tunable hardware filters at the receiver front-end with variable bandwidths will be needed to accommodate the various modes of operation to avoid co-site interference. The MBWCS shall provide a GPS antenna interface and embedded GPS receiver to support synchronization capabilities.

The platform shall provide specific physical interfaces. For example, for control purposes, control interfaces can be mapped on a RS-232 or Ethernet interface. For payload transmission and reception, interfaces can be mapped on an Ethernet interface. For voice communications, interfaces can be mapped on a PTT interface, Ethernet or any other specific interface.

4.5.2 Waveform requirements

The set of 4G standards, as can be seen in the compliance matrix in Table 4.2, covers the main necessities identified in terms of advanced services support with enough QoS and mobility support, mainly having gaps in their adaptation to specific military frequency bands, security, and robustness.

Table 4.2: Compliance Matrix of WiMAX, LTE and WLAN.

C	Requirements	WiMAX	LTE	WLAN
Deployment	**PHY**: Power efficient modulations.	PC	PC	NC
	PHY: Efficient coding schemes.	C	C	C
	CL: Power management with different operation modes and fast-switching technologies.	C	C	C
Management	**MGT**: Specific APIs based on the POSIX standard to allow the waveform to be fully reconfigured. This includes, but not limited to, the ability to change the transmission frequency, modulation and coding and network QoS.	NC	NC	NC
	MGT: An interactive system architecture, i.e., modular-view-controller architecture patterns, to reconfigure the waveform via a specific Application Programming Interface (API).	NC	NC	NC
	MGT: A collection of pre-defined parameters in an user profile to allow easy configuration and deployment based on operational scenarios.	NC	NC	NC
	PHY: Spectrum sensing or the utilization of a sensor network at physical layer as additional features to provide feedback for the system planners.	PC	PC	PC
Services and Applications	**CL**: The MAC layer shall support burst data traffic with high peak rate demand, simultaneously supporting streaming video and latency-sensitive voice traffic as well as other data/Web services like e-mail, chat, file/tactical data transfer over the same channel.	C	C	C
	NET: Developed for the delivery of IP-based broadband services.	C	C	C
	MAC: The transmission time interval used by MBWCS as well as MAC Layer/Scheduler shall be able to provide real-time requirements.	C	C	PC
	CL: VOIP connections.	C	PC	PC
	CL: MBWCS shall provide data latency for voice data transfer less than 300 ms, for video data transfer, at least 1 Mbps data rate and data latency less than 200 ms for the low criticality data transfer at least 9.6 Kbps data rate and data latency less than 1s for the critical data transfer at least 384 Kbps data rate and less than 200 ms data latency.	C	C	C
	MAC: A specific scheduling algorithm in order to provide the necessary QoS for time-sensitive traffic such as voice and video according to the previous technical requirements.	PC	PC	PC
	NET: Networking QoS features include: bandwidth, delay, error, availability, Security.	PC	PC	PC
	CL: Congestion management, traffic shaping and packet classification features.	C	C	C
	NET: Routing information shall take priority over any other traffic.	PC	NC	C
Network	**NET**: MBWCS shall support IP protocols (IPv4 / IPv6) to enable IP based NNEC concept with broadcast, multicast and unicast capabilities.	C	C	C
	NET: Connection oriented (e.g., TCP) and connectionless (e.g., UDP) services as well as applications like SIP or the IMS architecture.	C	C	C
	NET: Efficient IP services including several compression techniques.	C	C	NC
	MAC: Automatic Repeat Request (ARQ) techniques (fast retransmissions).	C	C	PC
	MAC: Relay capabilities (extended range, backbone connections) to avoid communication gaps.	C	C	C
	CL: Cross-layering techniques in order to support several basic capabilities like or QoS management, shall be considered.	C	C	PC
	NET: Mobility management in the network layer (e.g., scenario Type B, C and E) supporting mobile IP protocols like mobile IPv6, hierarchical mobile IPv6, fast mobile IPv6 or Proxy Mobile IPv6 (at network side).	C	C	PC
Topology	**CL**: MBWCS with MANET topology shall support dynamic network environments between vehicle convoys or groups of dismounted personnel where nodes may regularly join or leave the network and the connectivity between nodes may change frequently.	PC	NC	NC
	CL: Network protocols with ad-hoc, self-healing, self-forming and path optimizing capabilities.	PC	PC	C
	NET: Network Layer MANET routing protocol shall consider the following features in order to maximize network efficiency; distributed operating; loop-freedom (open, closed); proactive operation in case of enough bandwidth and energy supply permission, i.e., QOLSR, Fast-OLSR, TBRPF, OSPF, OLSRv2 $\cdots$, hybrid Operation and security.	NC	NC	PC

C	Requirements	WiMAX	LTE	WLAN
	MAC: Mechanisms for bandwidth request and assignment.	C	C	PC
	CL: Power control and Adaptive Modulation Control (AMC) mechanisms.	C	C	C
	CL: The MAC layer shall support network entry, ranging, key management, multicast...according to the network topology.	C	PC	C
Mobility	**PHY**: Physical layer of MBWCS shall have an appropriate frame structure and parameters.	C	C	NC
Mobility	**MAC**: MBWCS MAC layer shall be able to establish different links at the same time for handover.	NC	NC	NC
Mobility	**PHY**: MBWCS PHY Layer shall be able to provide metrics, such as SINR and RSSI, to measure the link quality.	C	C	PC
Mobility	**MAC**: MBWCS MAC Layer shall use the provided metrics to take handover decisions.	C	C	C
Mobility	**CL**: MBWCS ecosystem shall provide a backbone infrastructure for mobility management signaling exchange in order to perform handover mechanisms.	C	C	U
Security	**SEC, TRANSEC**: Frequency hopping and spread-spectrum techniques (LPD).	NC	PC	NC
Security	**PHY, TRANSEC**: MIMO and/or smart antennas due to Direction Of Arrival (DOA) (LPD).	C	C	NC
Security	**TRANSEC**: secure PN-sequence generators to prevent easy sequence estimation (LPI).	PC	C	NC
Security	**TRANSEC**: scrambling of transmission data and control information (LPI).	PC	C	C
Security	**CRYPTOSEC**: ciphering, authentication and key management algorithms adaptable to national or coalition needs, support for NATO Suite B.	PC	U	PC
Security	**CRYPTOSEC**: mutual authentication even for non-equal treated stations, i.e., BS and SS.	C	C	PC
Security	**CRYPTOSEC**: internal and external security devices for ciphering (IPSEC: IP ciphering), digital signatures and the possibility to volatile store critical material (keys, policies, algorithms).	PC	C	NC
Security	**MGT**: MBWCS shall support Over-The-Air (OTA) operations, e.g., transmission of security material using Over-The-Air Rekeying (OTAR).	C	NC	PC
Security	**INFOSEC**: NATO Level 3 security including IP security protocols (IPSec/HAIPE) as well as IP tunneling protocols (NAT, IPv4/IPv6-Transition).	C	C	C
Robustness	**MAC**: Adaptive modulation and coding and/or HARQ or ARQ strategies to offer robustness to interference.	C	C	PC
Robustness	**PHY**: Depending on the deployment, the system shall be compliant with spectral emission masks to avoid co-site interference.	C	C	C
Robustness	**PHY**: The MBCWS shall employ interference cancellation techniques to mitigate the effects of jamming signals.	PC	PC	NC
Robustness	**CL**: Algorithms and signal processing techniques to actively track jamming signals and instantiate algorithms in both the physical and network layer, to allow the radio to signal and change certain transmission profiles such as transmission frequency.	NC	C	PC
Robustness	**CL**: MAC or Network layer signaling algorithms to provide sufficient channel quality indicators, thus allowing the fast adaptation of the network to interference signals.	C	C	C
Robustness	**NET**: In the case of a loss in an external synchronization signal i.e., GPS/GNSS, the system shall be designed to self-configure and maintain network connectivity.	C	C	C
Robustness	**PHY**: MIMO and/or beam-forming techniques shall be required to improve the link performance.	C	C	C
Robustness	**CL**: Dependent on the deployment scenario, power control algorithms and sleep and idle modes shall be provided to conserve power consumption.	C	C	C
Robustness	**CL**: Network self-healing and recovery, the loss of a single radio or link can not affect network performance.	C	PC	C
Robustness	**PHY**: Channel coding in the form of forward error correction codes shall be designed in order to increase the robustness offered by these techniques.	C	C	C
Bands	**PHY**: A specific profile designed for NATO I target frequency band, based on limited bandwidths (i.e., 1.25 MHz) and single carrier modulations.	NC	NC	NC
Bands	**PHY**: A specific profile designed for NATO IV target frequency band, based on large bandwidths (i.e., 20 MHz or higher) and multicarrier modulations.	PC	NC	NC

C	Requirements	WiMAX	LTE	WLAN
Coverage	**PHY**: MBWCS shall be able to establish links in both LOS and NLOS.	C	C	PC
	CL: MBWCS shall support Layer 2 or Layer 3 Relay technology in order to extend coverage.	C	C	C
	CL: The Physical Layer as well as MAC layer of MBWCS shall be in accordance with Relay Technology used.	C	C	C
	CL: Mesh Networking for Company Level communication being capable to route or switch through the traffic of other nodes in order to extend coverage.	C	PC	C
	PHY: MBWCS shall be able to assign a lower frequency channel with low data rate option (changing to a more robust modulation scheme) in order to increase coverage between two nodes without using intermediate network nodes.	NC	NC	PC
	PHY: MBWCS shall be tested according to ITU (International Telecommunication Union) Channel Models (ITU-R recommendation M.1225 and IMT-Advanced M.2135-1 (2009)) for suburban, rural and costal scenarios.	NC	NC	NC
Interoperability	**CL**: MBWCS shall support interoperability due to waveform concept and definition of PHY, MAC and NET functionality.	C	C	C
	NET: MBWCS shall support IP protocols (IPv4/IPv6) to enable NNEC concept, upper layer protocols and applications.	C	C	C
Target	**PHY**: RF front-ends of the fixed, vehicular and man-pack platforms shall support MIMO technology. Hand-held configurations can consider as optional the support of MIMO technology.	C	C	C

Specifically, WiMAX, LTE and WLAN are compliant with WF or WF/PTF requirements such as: efficient coding schemes, power management with different operation modes and fast-switching technologies, congestion management, traffic shaping and packet classification features, power control, AMC mechanisms and relay capabilities, and MIMO and/or beam-forming techniques.

Their MAC layer supports burst data traffic with high peak rate demand, simultaneously supporting streaming video and latency-sensitive voice traffic, as well as other data/Web services. The 4G MBWCS provides data latency for voice data transfer less than 300 ms; for video data transfer, at least 1 Mbps data rate and data latency less than 200 ms; for the low criticality data transfer, at least 9.6 kbps data rate and data latency less than 1s; for the critical data transfer, at least 384 kbps data rate and data latency less than 200 ms.

The standards support IPv4 / IPv6 to enable IP based NNEC concept with broadcast, multicast and unicast capabilities, connection oriented (TCP) and connectionless (UDP) services, as well as applications like Session Initiation Protocol (SIP) or the IP Multimedia Subsystem (IMS) architecture. NATO Level 3 security including IP security protocols (IPSec/HAIPE), as well as IP tunneling protocols (NAT, IPv4/IPv6-Transition) are supported.

In other requirements WiMAX, LTE and WLAN just partially comply, for example in spectrum sensing or the utilization of a sensor network at physical layer, as additional features to provide feedback to the system planners. The standards also do not present

the ideal scheduling algorithm in order to provide the necessary QoS for time-sensitive traffic such as voice.

WLAN is the only standard that is partially or non-compliant with the transmission time interval as well as MAC Layer/Scheduler real-time requirements. It does not provide efficient IP services including several compression techniques: Packet Header Suppression (PHS), Robust Header Compression (ROHC) or Enhanced Compressed Real Time Protocol (ECRTP), adaptive modulation and coding and/or HARQ or ARQ strategies to offer robustness to interference. Furthermore, WLAN does not use cross-layering techniques in order to support several basic capabilities like or QoS management, mobility management in the network layer by supporting mobile IP protocols like mobile IPv6, hierarchical mobile IPv6, fast mobile IPv6 or Proxy Mobile IPv6 (at network side), among others.

Nevertheless, none of the standards completely fulfill the following requirements: an interactive system architecture, like modular-view-controller architecture patterns, which allow for reconfigurability of the waveform via a specific API. These standards do not consider a collection of pre-defined parameters in a user profile to allow easy configuration and deployment based on operational scenarios, and a MAC layer able to establish different links at the same time for handover.

The interoperability due to waveform concept and definition means a clarified definition of PHY, MAC and NET functionality and behavior, and additional physical issues considerations e.g., propagation towards routing or a definition of a common set of transmission protocols.

The PHY layer design is clearly driven by TRANSEC features, and is significantly different that of an OFDM-based system with high bandwidth efficient modulation. This implies the implementation of power efficient modulations, or frequency hopping and spread-spectrum techniques. Physical layer of MBWCS shall have an appropriate frame structure and parameters (such as reference signals, cyclic prefix, sub-carrier spacing ($\triangle$f), time delay imposed, and so on) in order to mitigate the errors to be formed due to the Doppler Effect, and efficient techniques and/or algorithms in order to reduce PAPR in downlink path.

Only LTE offers secure PN-sequence generators to prevent easy sequence estimation, scrambling of information and support for CRYPTOSEC capabilities: internal and external security devices for ciphering (IPSEC: IP ciphering), digital signatures and the possibility to volatile store critical material (keys, policies, algorithms). Nevertheless, WiMAX is the only technology that gives support to Over-The-Air (OTA) operations, e.g., transmission of security material using OTA Rekeying (OTAR), and is capable to offload traffic to other nodes in order to extend coverage.

None of them have specific profiles designed for NATO I and IV, and they need improved protocol stacks for supporting MANET topologies considering hybrid operation and security.

The definition of MBWCS merges the most promising and compliant components or blocks according to these outcomes to reach its full potential.

4.6 Conclusions

In this chapter it was confirmed that the development of an innovative MBWCS would be clearly optimized if 4G standards are taken as basis. Once the feasibility has been confirmed, and after a cost-benefit analysis of the implementation of a 4G scenario-based MBWCS, the way-ahead would be setting up of a specific Research Task Group (RTG) for NATO IST-ET-068. This RTG shall cover two approaches. The first one will create a MBWCS relaxing to some extent the requirements, identifying what can be included with a positive cost-benefit trade-off, i.e., adding a crypto device. The main objective will be to minimize modifications in the hardware, in the firmware of the wireless transceivers, or in the backbone network. The second one will evolve the high-level assessment into the quantitative domain, thus performing a detailed design of the envisaged MBWCS, conducting exhaustive simulations and prototyping activities with the WiMAX, LTE and WLAN promising features and modules concerning the specified requirements' compliance. Conclusions state that today standards only imply a partial compliance of some of the requirements identified and none of them are able to comply with the full specification. Moreover, 5G systems shall be examined to assess the compliance of the requirements proposed in order to design a disruptive MBWCS. Nevertheless, this summary gives an overall view of the most efficient and timely way to design a MBWCS for the near future warfare.

Chapter 5

Internet of Things for Defense and Public Safety

5.1 Introduction

The Internet of Things (IoT) is undeniably transforming the way that organizations communicate and organize everyday businesses and industrial procedures. Its adoption has proven well suited for mission-critical sectors that manage a large number of assets and coordinate complex and distributed processes. This chapter analyzes the great potential for applying IoT technologies (i.e., data-driven applications or embedded automation and intelligent adaptive systems) to revolutionize modern warfare and provide benefits similar to those in industry. It identifies scenarios where defense and public safety could leverage better commercial IoT capabilities to deliver greater survivability to the warfighter or first responders, while reducing costs and increasing operation efficiency and effectiveness. These technologies can help the military and first responders to adapt to a modern world in which adversaries are located in more sophisticated and complex suburban scenarios (smart cities) while budgets are shrinking.

Defense and public safety organizations play a critical societal role ensuring national security and responding to emergency events and catastrophic disasters. Instead of public safety, some authors use the term Public Protection Disaster Relief (PPDR) [106] radio communications, defined in ITU-R Resolution 646 (WRC-12) as a combination of two key areas in emergency response:

- Public protection (PP) radio communication: communications used by agencies and organizations responsible for dealing with the maintenance of law and order, protection of life and property, and emergency situations.

- Disaster relief (DR) radio communication: communications used by agencies and organizations dealing with a serious disruption in the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether they happen suddenly or as a result of complex, long-term processes.

Nowadays, the challenge of crisis management is in reducing the impact and injury to individuals and assets. This task demands a set of capabilities previously indicated by European TETRA [107], TCCA [108], and ETSI [109] standardization bodies and American APCO Project-25 [110], which includes resource and supply chain management, access to a wider range of information and secure communications. Military and first responders should be able to exchange information in a timely manner to coordinate the relief efforts and to develop situational awareness. FY 2016 SAFECOM Guidance [111] provides an overview of emergency communications systems and technical standards. Communication capabilities need to be provided in very challenging environments where critical infrastructures are often degraded or destroyed. Furthermore, catastrophes, natural disasters or other emergencies are usually unplanned events, causing panic conditions in the civilian population and affecting existing resources. In large-scale natural disasters, many different public safety organizations (military organizations, volunteer groups, non-government organizations and other local and national organizations) may be involved. At the same time, commercial communication infrastructure and resources must also be functional in order to alert and communicate with the civilian population. In addition, specific security requirements including communication and information protection can also exacerbate the lack of interoperability. In order to establish and maintain a Common Operational Picture (COP), it is necessary to share various types of data between agencies and between field and central command staff.

Typically, first responders include police officers, firefighters, border guards, coastal guards, road and railway agents, custom guards, airport security, emergency medical personnel, non-governmental organizations (NGOs), and other organizations among the first on the scene of a critical situation. These organizations can provide one or more of the functions described above. The relationships between them may depend on the national legislation or the context.

Over the last years, some research papers focused on evolving public safety organizations have been published [112]. As introduced previously in Chapter 4, some of these articles have particular interest in the challenges to evolve the LTE network architecture toward 5G in order to support emerging public safety networks [113]. With respect to IoT, there are several published papers that cover different aspects of the IoT technology

applied to defense and public safety. For example, Chudzikiewicz et al. [114] propose a fault detection method based on a network partitioned into clusters for the military domain. Yushi et al. [115] introduce a layer architecture and review some application modes. They also include the example of a weapon control application. Butun et al. [116] propose a lightweight, cloud-centric, multi-level authentication as a service approach that addresses scalability and time constraints for IoT devices surrounding public safety responders. References [8, 117] contain short surveys for leveraging the IoT for a more efficient military. The authors of [118, 119] focus on security challenges, while TCG drafts a guideline for securing IoT networks [120].

Unlike recent literature, the contribution of this chapter focuses on providing a holistic approach to IoT applied to defense and public safety with a deeper study of the most relevant operational requirements for mission-critical operations and defense, an overview of the key challenges, and the relationship between IoT and other emerging technologies. Besides, the chapter presents a research roadmap for enabling an affordable IoT for defense and public safety.

For the sake of simplicity, the rest of the chapter will focus on the military side, since it covers most of the significant scenarios and functions, and represents the most challenging cases.

This chapter is based on the following publications [121–126]. Furthermore, a patent application was filled after the work on the development of smart cities concerning the standard IEEE 1451 [126]. The remainder of this chapter is organized as follows. Section 5.2 presents some promising scenarios for mission-critical IoT. Section 5.3 introduces the main operative requirements and capabilities, and analyzes their applicability to defense and public safety. Section 5.4 reviews the basics of the IoT architecture for tactical and emergency environments. Section 5.5 describes the main shortcomings and outlines the primary technical and cultural challenges that stand in the way of leveraging IoT technologies at a broader scale. It also identifies further research areas to enable COTS IoT for tactical and emergency environments. Finally, Section 5.6 is devoted to conclusions.

5.2 Target scenarios for mission-critical IoT

An overview of the most promising IoT scenarios is depicted in Figure 5.1. Until now, the deployment of IoT-related technologies for defense and public safety has been essentially focused on applications for C4ISR, and fire-control systems. This is driven by a predominant view that sensors serve foremost as tools to gather and share data, and create a more effective Command and Control (C2) of assets. IoT technologies have

also been adopted in some applications for logistics and training, but their deployment is limited and poorly integrated with other systems.

Besides, IoT functionalities are useful for establishing advanced situational awareness in the area of operations. Commanders make decisions based on real-time analysis generated by integrating data from unmanned sensors and reports from the field. These commanders benefit from a wide range of information supplied by sensors and cameras mounted on the ground, and manned or unmanned vehicles or soldiers. These devices examine the mission landscape and feed data to a forward base. Some data may be relayed to a Command Center where it is integrated with data from other sources.

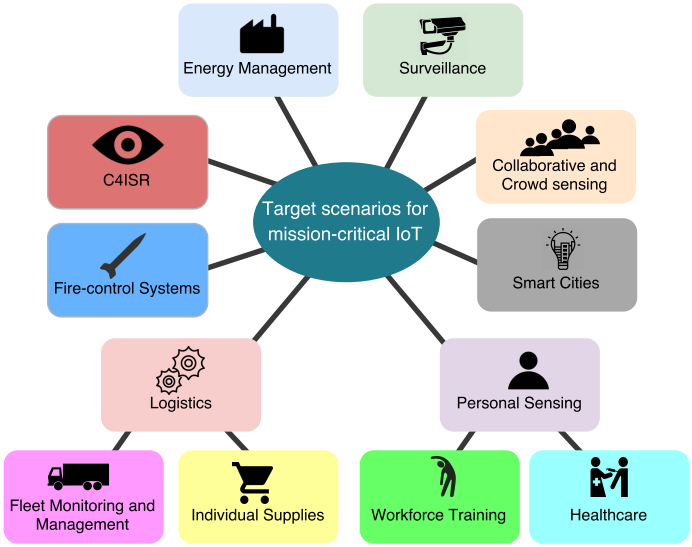


Figure 5.1: Promising target scenarios for defense and public safety.

5.2.1 C4ISR

C4ISR systems use many sensors deployed on a range of platforms to provide advanced situational awareness. Radar, video, infrared or passive RF detection data are gathered by surveillance satellites, airborne platforms, UAVs (Unmanned Aerial Vehicles), ground stations and soldiers in the field. These data are delivered to an integration platform that analyzes them and delivers information up and down the chain of command. These platforms provide a Common Operational Picture (COP) allowing for enhanced coordination and control across the field.

High-level military echelons are provided with comprehensive situational awareness through central operations centers which receive data feeds from platforms. Lower levels also have access to the data in their area. In the case of combat pilots, they receive prioritized data feeds integrated with data from their own sensor systems.

5.2.2 Fire-control systems

In fire-control systems, end-to-end deployment of sensor networks and digital analytics enable fully automated responses to real-time threats, and deliver firepower with pinpoint precision. For example, the U.S. Navy's Aegis Combat system provides C2 as well as an unprecedented ballistic missile defense [127]. Munitions can also be networked, allowing smart weapons to track mobile targets or be redirected in flight. Prime examples are the Tomahawk Land Attack Missile (TLAM) and its variants, navy's precision strike standoff weapons for attack of long range, medium range and tactical targets [128]. Furthermore, the military has invested in the use of long endurance UAVs to engage high-value targets and introduce multi-UAVs applications [129].

5.2.3 Logistics

Logistics is an area where multiple low-level sensors are already being used in defense. Currently, their deployment remains constrained to benign environments with infrastructure and human involvement. The military has already deployed some IoT technologies in non-combat scenarios in order to improve back-end processes. For example, RFID tags have been used to track shipments and manage inventories between central logistics hubs. In the following subsections, we describe examples that belong to two main categories: fleet management and individual supplies.

5.2.3.1 Fleet monitoring and management

Fleet monitoring can be represented by aircraft and ground vehicle fleets with on-board sensors that monitor performance and part status. For example, they track vehicle status and subsystems, and indicate when resupplying low-stock items (i.e., fuel or oil) is needed. Sensors would issue alerts, potentially reducing the risk of fatal failures. The aim is to facilitate condition-based maintenance and on-demand ordering of parts, reduce maintenance staff, and decrease unanticipated failures or unnecessary part replacements. Although IoT deployment carries up-front costs, it can enable significant long-term savings by transforming business processes across logistics. Defense has an opportunity to take advantage in the auto and industrial sectors, and exploit performance data on existing data links, like Blue Force Tracker transponders (already in place on many military vehicles) to limit new security risks. By extension, IoT-connected vehicles could also share information, for example, about available spare parts.

Real-time fleet management includes geolocation, status monitoring, speed and engine status, total engine hours, fuel efficiency, and weight and cargo sensors. Besides, when

tracking shipments, the position and status of the containers can be monitored to identify potential problems.

Regarding aircraft, modern jet engines are equipped with sensors that produce several terabytes of data per flight. This information combined with in-flight data can improve engine performance to reduce fuel costs, detect minor faults or shorten travel duration. Furthermore, it enables preventive maintenance resulting in a long lifecycle (slowing or preventing breakage) and less downtime spent in repairs. The flight data can be tracked in real-time by operators and analysts on the ground.

5.2.3.2 Individual supplies

The deployment of RFID tags, sensors and standardized barcodes allows for tracking individual supplies. IoT provides real-time supply chain visibility (whether it is being shipped, transferred, deployed, consumed, ...) and allows the military to order supplies on demand and simplify logistics management for operational units. This smarter procurement of goods avoids delays caused by out-of-stock parts or inventory-carrying costs. Likewise, it can increase accountability, enhance mission reliability, reduce losses and theft of military equipment, and help with the time criticality on the military maintenance.

At the soldier level, tracking is useful in order to follow a proactive approach to logistics or to meet operational requirements. Soldier material (e.g., water, food, batteries or bullets) can be monitored with alerts issued for a necessary resupply. Aggregate data (e.g., groups of soldiers, companies, battalions...) might also be studied for further enhancements of supply for tactical and emergency units. The analytics might be focused on considering environment, body type, consumption, ... among other variables.

5.2.4 Smart cities operations

In denied area environments, existing IoT infrastructures could be reused in military operations. Ambient sensors can be used to monitor the existence of dangerous chemicals. Sensors monitoring human behavior may be used to assess the presence of people acting in a suspicious way. Leveraging information provided by pre-existing infrastructures might be critical. Several security issues may arise, such as equipment sabotage or deceptive information. The authors of [130] categorize such attacks into four areas: 1) system architecture, firewalls, software patches; 2) malware, security policies and human factors; 3) third-party chains and insider threat; and 4) database schemas and encryption technologies.

5.2.5 Personal sensing, soldier healthcare and workforce training

Body-worn devices are increasingly available. Fitness trackers enable monitoring of physical activity along with vital signs. This information has an obvious value for the users but there is also a significant potential in examining aggregate values of communities. Body-worn sensors, when deployed on a community scale, offer information to support C4ISR. We have to distinguish between participatory and opportunistic sensing. The last one may be of particular relevance for under-cover personnel involved in reconnaissance missions in urban environments. Technologies for monitoring both workforce and their surroundings could aid when inferring physical or psychological states as well as assessing the risk of internal injury based on prior trauma. Soldiers can be alerted of abnormal states such as dehydration, sleep deprivation, elevated heart rate or low blood sugar and, if necessary, warn a medical response team in a base hospital. These wide range of health and security monitoring systems, enable an effective end-to-end soldier health system, including re-provisioning of health services when needed.

In addition, IoT can be used in some training and simulation exercises, i.e., wearable receivers to mimic live combat. An example of live training may use cameras, motion and acoustic sensors to track force during training exercises. The system would send data to trainers' mobile devices, who can coach in real time and produce edited video and statistics to review after the exercise.

Other examples are Cubic's I-MILES (Instrumented-multiple Integrated Laser Engagement System) training solutions [131] which simulate combat using lasers and visual augmentation. They use connectivity, computer modeling and neuroscience-based learning tools to provide a more comprehensive real-time training experience. The solutions simulate artillery fire and provide a battle effect simulator, which include explosive devices like land mines, booby traps, and pyrotechnics. The previously referred applications, and others yet-to-be imagined, could be part of the equipment of the soldiers of the future. A likely evolution of such equipment can be seen in Figure 5.2.

5.2.6 Collaborative and crowd sensing

Collaborative sensing involves sharing sensing data among mobile devices combined with robust short range communications. IoT nodes would be able to utilize placement or other sensors to supplement their own sensing methods. Once security issues (such as trust and authentication) are resolved, the information can be made available to the users. Long-term maintenance of IoT services yield multiple benefits, such as trend or fault detection. Individual sensor parameters must be considered to assign a particular

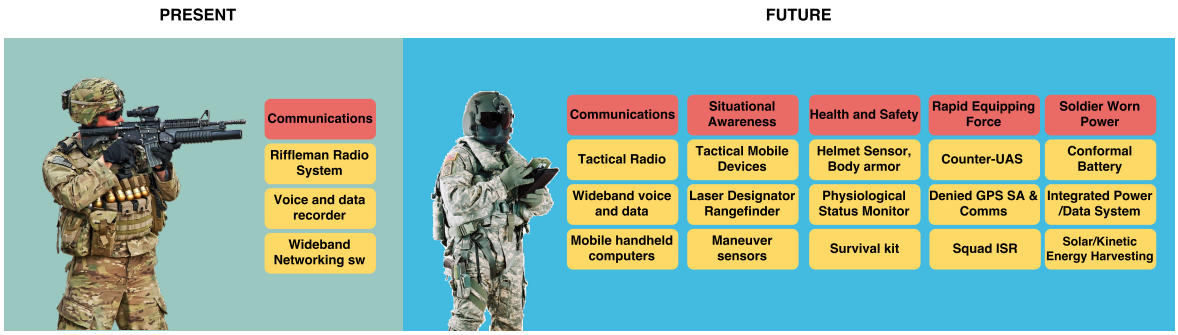


Figure 5.2: Soldiers of today and the future.

relevance to a given reporting device and its feedback can be improved upon data fusion approaches.

IoT can ease ad-hoc mission-focused Intelligence, Surveillance and Reconnaissance (ISR) via pairing sensors with mission assignments. For example, multiple devices can enter an area of interest each with their own mission, but relying on collaborative sensing to accommodate new or unanticipated requirements. Thus, sensor platforms would not have to be burdened with excessive equipment to handle mission scenarios on their own. In the case of a soldier, its situational awareness increases, allowing for improved survival and mission success.

Resource-rich devices might collect data from several sources to form a COP. This would allow for storing much of the collection and for processing the data locally. Higher level functions would aid reducing response times, improving decision-making and reducing backhaul communications requirements.

Crowdsensing promises to be an inexpensive tool for flexible real time monitoring of large areas and assessment for mission impact, hence complementing services potentially available in smart cities. From the perspective of gathering data from a community, deception could be achieved by compromising individual devices. Consequently, the security level is proportionate to the number of present devices, each representing a possible attack vector. Moreover, the paradigm "Bring your own Device" (BYOD) [132] introduces potential security concerns, since the user may have full access and make use of multiple heterogeneous devices that are difficult to control.

Data validation is another domain-dependent task in the context of crowd sending and, likewise, it is further complicated by the high heterogeneity of the devices.

5.2.7 Energy management

The U.S. DoD is already reducing its demand on facility energy by investing in efficiency projects on its installations [133]. The introduction of data and predictive algorithms

can help to better understand usage patterns and significantly decrease military's energy costs.

5.2.8 Surveillance

Security cameras and sensors, combined with sophisticated image analysis and pattern recognition software, ease remote facility monitoring for security threats. In the case of marine and coastal surveillance, using different kinds of sensors integrated in planes, unmanned aerial vehicles, satellites and ships, makes possible to control the maritime activities and traffic in large areas, keep track of fishing boats, and supervise environmental conditions and dangerous oil cargos.

Other examples can be the monitoring of hazardous situations: combustion gases and preemptive fire conditions to define alert zones, monitoring of soil moisture, vibrations and earth density measurements to detect dangerous patterns in land conditions or earthquakes, or distributed measurement of radiation levels in the surroundings of nuclear power stations to generate leakage alerts.

5.3 Operational requirements

As explained previously in Chapter 4, the military has unique operational requirements. Security, safety, robustness, interoperability challenges, as well as bureaucratic and cultural barriers, stand in the way of the broad adoption of new IoT applications. In this section a set of operational requirements grouped by capabilities are assessed in order to cover the scenarios previously discussed.

5.3.1 Deployment features

One of the biggest constraints in a battlefield environment is power consumption. IoT devices are likely to be powered by batteries or solar power, and charged on-the-move from solar panels, trucks, or even by motion while walking. In either case, they should last for extended periods of time (at least for the duration of the mission). Therefore, devices and sensors need to be power-efficient, and end-users have to use them appropriately. Likewise, it is not easy to recharge IoT devices periodically or swap out batteries in deployed devices. Even in the case of body-worn devices, it is impractical to expect soldiers to carry additional batteries on top of their current equipment.

The exploitation of emerging embedded hardware within the military, probably through specialized software components designed to run on those innovative platforms, could lead to a significant increase in processing power and a decrease in energy consumption.

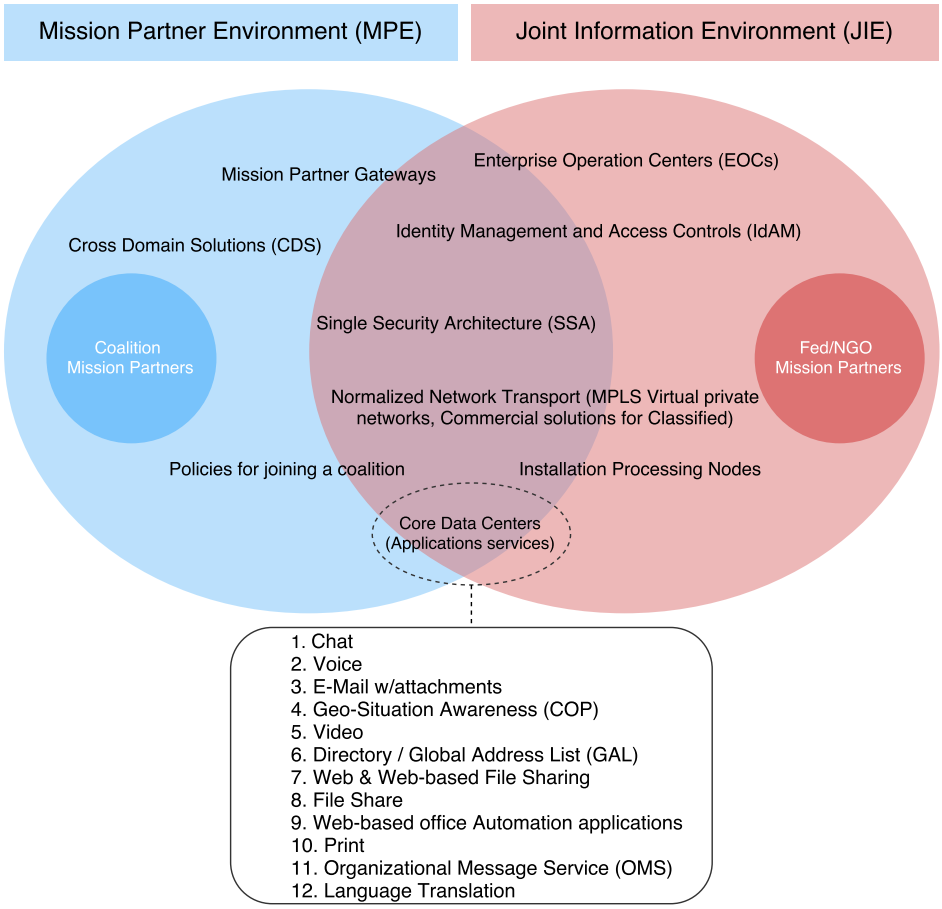


Figure 5.3: Requirements and application services for commanders.

Furthermore, design values (e.g., power cell size or transmission capabilities) and equipment should fulfill the requirements imposed and be compliant with the considerations from military standards (e.g., MIL-STD 810G, MIL-STD 461F, MIL-STD-1275). IoT devices should be ruggedized and prepared to operate under extreme environmental conditions. Nevertheless, a non-negligible share of devices is already designed for harsh industrial environments and, thus, they would be relatively well suited for the adoption in defense environments.

5.3.2 System management and planning

One of the largest gaps in the defense and public safety data ecosystem is digital analytics (data collection, transformation, evaluation and sharing). Much of the massive information collected by sensors is never used and, as for the information that is used, it often depends on manual entry and processing, which incur in significant delays when getting important information in mission-critical scenarios. Those delays can cause missions fail or stall, or force decision-making without relevant facts. For example,

USTRANSMCOM bulk supplies are tracked between major hubs using RFID tags, but when supplies are broken down and distributed beyond the central hubs, they are replaced manually. Officers in the field sign for orders on paper and enter serial numbers into computers by hand. This approach is burdensome and poses risks due to human errors.

Much of the value of IoT is generated by automation, allowing systems to react quicker and with more precision than humans. Few military systems include fully autonomous responses. For example, most unmanned systems deployed are not autonomous but remotely controlled by operators. This management effort needs the development of new lightweight management protocols. For example, monitoring the M2M communications of IoT objects is important to ensure constant connectivity. LightweightM2M [134] is a standard developed by the Open Mobile Alliance (OMA) to interface between M2M devices and servers to build an application-agnostic scheme for the remote management of a variety of devices. The NETCONF Light protocol [135] is an Internet Engineering Task Force (IETF) effort for the management of resource-constrained devices. In [136], the authors propose a framework for IoT management based on the concept of intercepting intermediary nodes in which they execute heavy device management tasks on the edge routers or gateways of constrained networks. The OMA Device Management working group specifies protocols for the management of mobile devices in resource constrained environments [137].

5.3.3 Supported services and applications

A number of commercial devices and electronic equipment have been explored to provide the services required like chat, push-to-talk voice, geo-situational awareness, SRTV (Secure Real-Time Video) or web sharing. A complete list of requirements and application services can be seen in Figure 5.3. The diagram represents the vision of the Joint Information Environment (JIE), which ensures that DoD military commanders, civilian leadership, warfighters, coalition partners, and other non-DoD mission partners, access information and data provided in an agile DoD-wide information environment. This shared IT infrastructure includes enterprise services and a Single Security Architecture (SSA). The Mission Partner Environment (MPE) is integrated with and enabled by JIE. It corresponds to an operating environment that enables C2, within a specific coalition, for operational support planning and execution on a network infrastructure at a single security level with a common language. Regarding the small circles of the diagram, they represent the different participants within a specific partnership or coalition (e.g., the intelligence community, U.S. government agencies, allies, and other mission partners, such as industry organizations and NGOs.

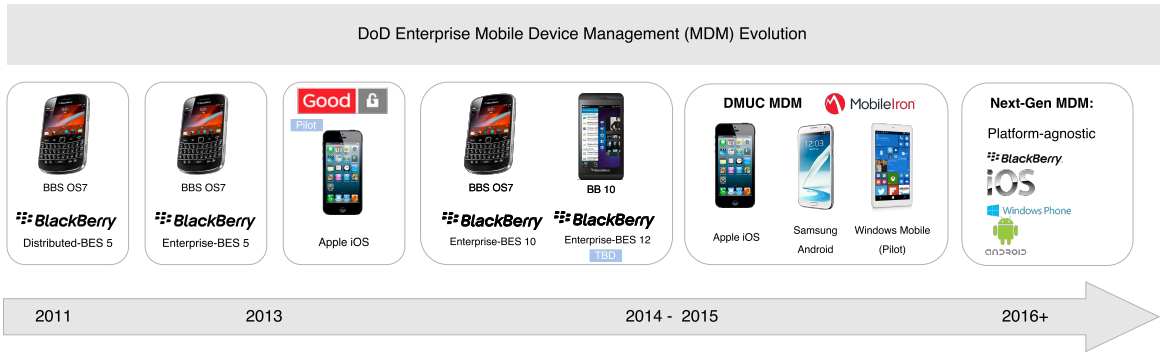


Figure 5.4: DoD enterprise Mobile Devices Management (MDM) evolution.

The U.S. army's Nett Warrior (NW) program [138] has developed ruggedized Android devices. These devices, which are modified from COTS Samsung Galaxy Note II smart phones, provide access to the data-capable Rifleman radio. It aims to connect soldiers in the field with a range of apps, such as Blue Force Tracking, 3-D maps, or an application that shows details on profiles of high-value targets. The devices run a NSA-approved version of the Android operating system and plan to include applications such as foreign language translation. These programs have been piloted on a limited basis. Broader deployment is hampered by the limited usability, functionality and lack of connectivity. Other commercial devices can be seen in Figure 5.4.

The U.S. Air Force has developed apps on commercial iPads. For example, programmers at Scott Air Force Bases created in 2014 an app to plan loads for the KC-10 cargo aircraft [139], winning an award for government innovation. Such an application was designed to automatically gauge pre-flight distribution of cargo in a weight and balance computation considering the crew, fuel and cargo in a drag-and-drop interface.

The American Defense Information System Agency's (DISA) Mobility Program has implemented software packages for NSA-approved Android devices. The program includes secure devices that can access a secret classified network, SIPRNET [140]. DMCC-S (DoD Mobility Classified Capability Secret Device) R2.0 is an example (Figure 5.5) of the new generation of DoD secure mobile communication devices.

5.3.4 Network capabilities

Military network infrastructures are severely limited by frequent disconnections, partitioning, and fluctuations of radio channel conditions. This can lead to issues in sensing availability and constraints on the usage of transducers. The military IoT networks operate over tactical radios that establish and maintain mobile and fixed seamless C2 communications between operational elements and higher echelon headquarters. Tactical radios provide interoperability with all services, various agencies of the U.S.

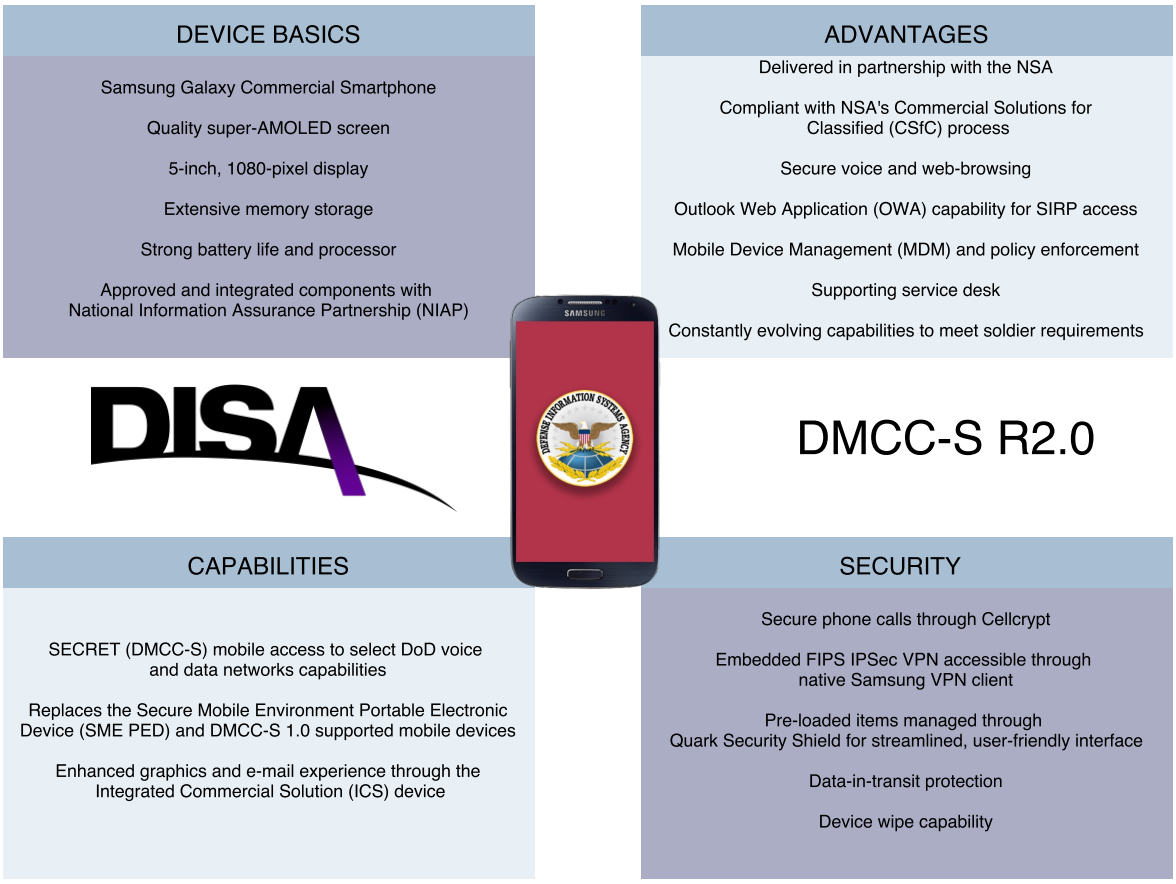


Figure 5.5: Main characteristics of DMCC-S R2.0

Government, commercial agencies and allied coalition forces. High-bandwidth radios that could constitute integrated networks are still under development. For example, Harris Corporation will deliver the first batch of RF-335M tactical radio systems in September 2017 to U.S. Special Operations Command (USSOCOM) [141].

As the connectivity of sensors improves, the system can become overwhelmed with the huge volume of data in transit. This data volume increase may force an upgrade to a system's network infrastructure to increase bandwidth or, alternatively, it may require to increase the performance of intelligent data filtering. In the commercial environment, network bandwidth and QoS (Quality of Service) challenges are addressed using COTS hardware combined with open virtualization platforms to manage network demands dynamically. These advanced network servers provide both high availability and also new approaches to control and provision network systems by delivering a path to Network Function Virtualization (NFV) [142]. NFV offers the operator the ability to configure the network infrastructure dynamically through sophisticated management protocols. Thus, NFV empowers military commanders to quickly configure data feeds for

changing operational requirements and to manage device and data security throughout the system.

Currently, each military force has its own infrastructure, both for connectivity and for the back-office systems. Transitioning to a combat cloud infrastructure will offer greater ability to export both assets and data in the field for joint operations. Also a combat cloud will allow information and control to move forward when appropriate, providing the operational flexibility to deal with coalitions.

Nowadays, any army in the world can have the network infrastructure needed to handle, process and distribute the massive flow of data that would be generated by a widespread IoT [117]. In order to make effective use of IoT, the devices must be able to connect to global networks to transmit sensor data and receive actionable analytics.

5.3.5 Supported network topologies

Mobile ad-hoc networks (MANET) [143] and hybrid wireless sensor networks (WSNs) [144] are the main tactical topologies.The authors of [145] evaluate the performance of network coding in the context of multi-hop military wireless networks. The researchers prove its efficiency in multicast and broadcast communications. They also test the optimal capacity of the system and its ability to recover from lost packets. Network coding operates well even with highly lossy and unreliable links.

Interest has grown in opportunistic sensing systems, particularly on those that take advantage of smartphone-embedded sensors [146]. A network of opportunistic sensing systems can automatically discover and select sensor platforms based on the operational scenario, detecting the appropriate set of features and optimal means for data collection, obtaining missing information by querying resources available, and using appropriate methods to fuse data. Thus, the system results in an adaptive network that automatically finds scenario-dependent objective-driven opportunities with optimized performance. For example, Mission-Driven Tasking of Information Producers (MTIP) [147] is a prototype system for sharing airborne sensors focused on the effective allocation of a large number of potentially competing individual tasks to individual sensors. Nevertheless, specific protocols are needed for advancing autonomous sensing that not only ensure effective utilization of sensing assets but also provide robust optimal performance.

Moreover, the development of a decentralized infrastructure is needed to avoid a single point of failure. Bandwidth is perhaps one of the most precious resources in a tactical environment. It is expected that in dynamic battlefield environments large-scale data analysis will be conducted in near real-time. This fact implies constraints on data analysis coupled with connectivity challenges. Decentralizing computational resources

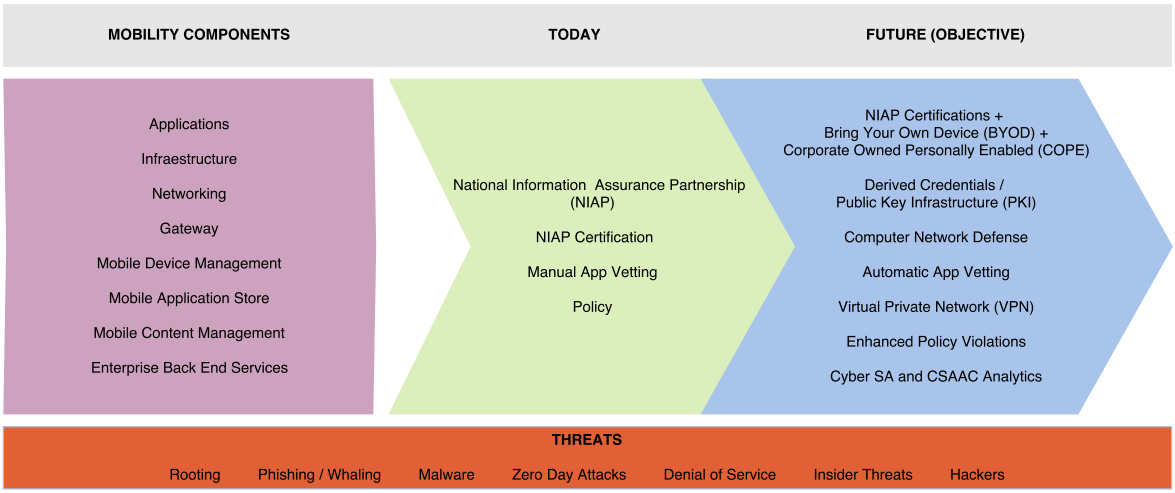


Figure 5.6: Mobility components and their security.

by creating multiple and local cloudlets is insufficient if the overall approach still consists in sending raw data from transducers to a local cloud for processing.

5.3.6 Mobility capabilities

Mobility is another challenge for the IoT implementations because most of the services are expected to be delivered to users on the move. Service interruption can occur when the devices transfer data from one gateway to another. To support service continuity, Ganz et al. [148] propose a resource mobility scheme that supports two modes: caching and tunneling. These methods allow applications to access IoT data when resources become temporarily unavailable. The evaluation results show a reduction of service loss in mobility scenarios of 30%.

The huge number of smart devices in IoT systems also requires efficient mechanisms for mobility management (the components and their needs are illustrated in Figure 5.6). For instance, a feasible approach for M2M communications is presented in [149]. In the scheme presented, group mobility is managed by a leader based on the similarity of their mobility patterns.

5.3.7 Security capabilities

Security is a paramount challenge that needs to be addressed at every level of IoT, from the high volume of endpoint devices that gather data and execute tasks, to cloud-based control systems through network infrastructure. Several protection mechanisms and Electronic Protection Measures (EPM) have been identified within TRANSEC such as Low Probability of Interception (LPI) (e.g., secure PN-sequence generators to prevent

easy sequence estimation, scrambling of transmission data and control information), Low Probability of Detection (LPD) (e.g., frequency hopping and spread-spectrum techniques) and Anti-Jamming (AJ), INFOSEC (e.g., NATO Level 3 security including IP security protocols (IPSec/HAIPE) as well as IP tunneling protocols), COMSEC and NETSEC capabilities.

Privacy issues and profile access operations between IoT devices without interference are critical. IoT nodes require a variety of widely-used and well-established security mechanisms (e.g., SSL, IPSec, PKI) that perform numerous computationally intensive cryptographic operations. Sensitive data needs a transparent and easy access control management. Several proposals can be used, such as grouping devices or presenting only the desired devices within each virtual network. Another approach is to support access control in the application layer on a per-vendor basis. Relevant projects that estimate the network location of objects to perform context-aware services are reviewed in [150]. Current methods for location estimation are based on IP. However, Named Data Networking (NDN) is one of the candidates for naming infrastructure in the future Internet [151].

Military equipment can be subject to either interference, sabotage, potential manipulation or disruption of data flows between different units, resulting either in service interruptions, intrusions, propagation of misinformation, or misleading the COP on the needs of support units. These failures in equipment can compromise both intelligent gathering and planned operations having obvious mission and life-threatening consequences. For example, inadequately secured networks can provide the enemy with intelligence (location, deployment) allowing the adversary to anticipate movements of forces. Furthermore, security vulnerabilities could allow enemies to take control or disable automated systems, preventing workforce from carrying out their mission, or even using their own assets against them. Next, we describe the main security challenges:

- Device and network security: the potential of IoT is derived to a large extent from the ubiquity of devices and applications, and the connections between them. This myriad of links creates a massive number of potential entry points for cyber-attackers. The systems also depend on backbone storage and processing functions which can include other potential vulnerabilities. One of the ways to enhance the security of a complex network is to limit the number of nodes that an attacker can access from any given entry point. This approach conflicts with IoT, which generates much of its value from the integration of different systems. Securing a broad range of devices is also difficult. Many of them have limited capacity with no human interface and depend on real-time integration of data. This complicates

traditional approaches to security, like multi-factor authentication or advanced encryption, which can hinder the exchange of data on the network, requiring more computing power on devices, or needing human interaction.

- Insider misuse: cyber risks and insider threats are a challenge for large organizations. A single mistake from a single user enables an attacker to gain access to the system.

- Electronic warfare: most technologies communicate wirelessly on radio frequencies. Adversaries can use jamming techniques to block those signals making the devices unable to communicate with backbone infrastructure. Wireless connections also raise the risk of exposing the location through radio frequency emissions. Transmitters can serve as a beacon detectable by any radio receiver within range, and the triangulation of such emissions can compromise the mission.

- Automation: the full automation of equipment and vehicles extends the reach of cyber threats to the physical domain.

The authors of [152] propose integrity attestation as a useful complement to subject authentication. Thus, the provision of a data structure can convey integrity assurances and be validated by others. This is particularly useful for IoT, considering that the limited capacity of the computers and communication channels do not allow for complex protocols to detect malfunctions. The document [153] outlines the DoD security model to leverage cloud computing along with the security requirements needed for using commercial cloud-based solutions.

5.3.8 Robustness capabilities

Communication technologies will provide robustness to signal interference and/or loss of network operation. When deployed in locations with other tactical networks (i.e., vehicular deployment), proper measures to avoid interference from adjacent users will be needed. For mesh or Point-to-Multi-Point (PMP) modes, the network will provide redundancy and be robust to a single point of failure. Systems should be robust to jamming, supporting techniques to actively track jamming signals and applying automatic jamming avoidance measures. It should include cognitive radio and dynamic spectrum management techniques to automatically overcome bad conditions in the communications environment.

The operational requirements for robustness also include the physical attributes of the device. Generally, this is addressed by the target platform requirements which, in turn, is dependent on the deployment scenario. Equipment should be also physically

robust to environmental damage, i.e., shock- and water-proof. The IoT system should provide mechanisms to allow for fast switching between the technology chosen and back-up/legacy communications in the event of failure. Although there are many metrics available to assess the performance of IoT devices, evaluating their performance is a challenge since it depends on many components as well as the behavior of the underlying technologies. The evaluation of routing protocols, information processing, application layer protocols, and QoS have been reported in literature, but there is a lack of a thorough performance evaluation for IoT services.

5.3.9 Coverage capabilities

Defense and public safety should invest in resilient, flexible and interoperable capabilities to operate at extended ranges under adverse weather conditions and harsh environments (including LOS and NLOS scenarios) in enemy territory, and enhance connectivity in denied areas. One of the technologies that can deliver mobile and persistent connectivity is CubeSat: nano satellites that can be deployed in large number to create potentially more resilient constellations [154]. CubeSat deployment is also faster than with larger satellites as they can be launched into orbit in clusters or piggybacked on other loads. It supports SDR to enable reconfigurability of data management, protocols, waveforms and data protection.

Other technologies are High-Altitude Platforms (HAPs) and Unmanned Air Vehicles (UAVs) that operate above the range of terrestrial communication systems and can be equipped with communication relays. Unlike satellites, which eventually become defunct, HAPs can be upgraded and enhanced as technologies evolve. They also have significant advantages over manned communications platforms, as they can stay airborne continuously for long periods.

The U.S. military has already deployed four EQ-4B Global Hawk Block 20 Drones with the Battlefield Airborne Communications Node (BACN) system but it will need significantly greater capacity to deliver connectivity to a full suite of connected devices across multiple theaters. DoD is now involved in the development of Northrop Grumman RQ-4 Global Hawk Block 30 and 40, ground stations, and Multi-Platform Radar Technology Insertion programs. The U.S. Navy will get a persistent maritime ISR capability through the MQ-4C Triton. DoD is now funding the procurement of two Low Rate Initial Production (LRIP) systems and continues to fund development activities associated with software upgrades [155].

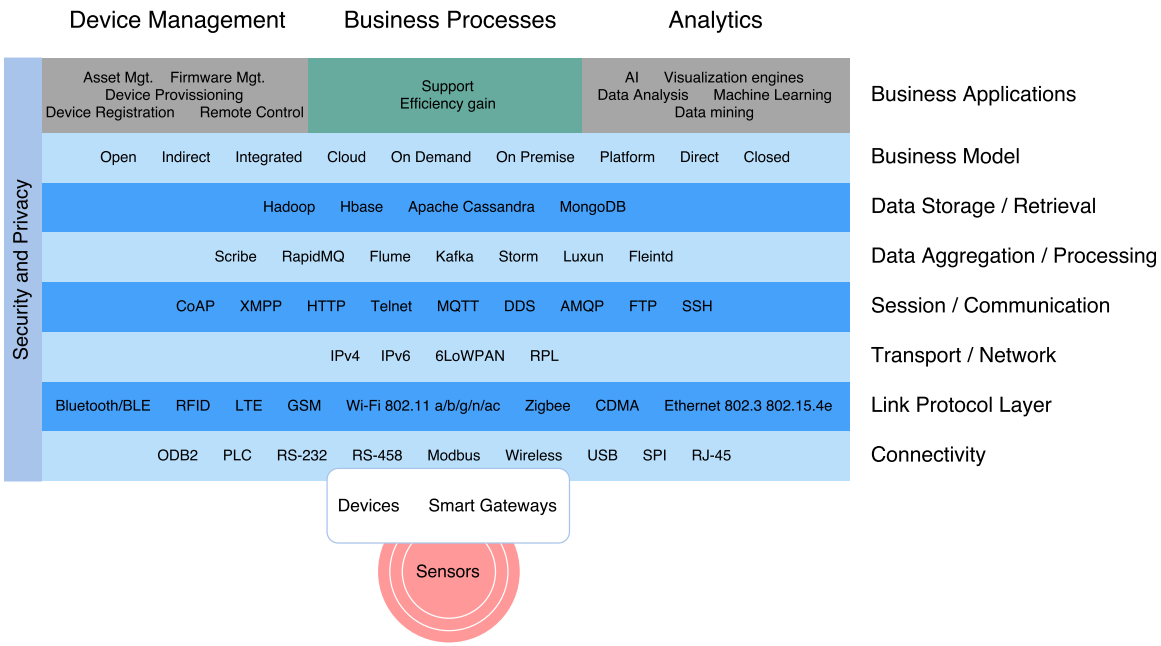


Figure 5.7: IoT landscape.

5.3.10 Availability

Availability must be taken into account in the hardware, with the existence of devices compatible with IoT functionalities and protocols; and in the software, with available services for everyone at different places. One solution to achieve high availability is to provide redundancy for critical devices.

5.3.11 Reliability

The critical part to increase the success rate of IoT service delivery is the communication network. The authors of [156] propose a reliability scheme at the transmission level to minimize packet losses. Other authors [157] exploit probabilistic model methods to evaluate the reliability and cost-related properties of the service composition in IoT systems. The survey [158] reviews applications of the Markov decision process (MDP) framework, a powerful decision-making tool to develop adaptive algorithms and protocols for WSNs, like data exchange and topology formation, resource and power optimization, area coverage, event tracking solutions, and security and intrusion detection methods.

5.3.12 Interoperability capabilities

Taking advantage of the full value of IoT is about maximizing the number of hardware and software systems, nodes and connections in the data ecosystem. However, defense lacks a cohesive IT architecture. The different and heterogeneous systems are developed independently and according to different operational and technical requirements. Frequently, multiple services are involved in an operation, or several departments are involved in a process, but information has to be adapted between their systems manually. The usage of different hardware designs and data standards can impact the cohesion of defense infrastructure, leading to stove pipe systems. The fragmentation of the architecture also complicates the use and development of common security protocols. Adequate interoperability between devices is often not achieved given the variety of functions served by defense hardware, the integration across partners, or when potentially useful devices in an area of operations are to be leveraged (i.e., smart city deployment). IoT capabilities across an enterprise as broad as defense can only be delivered through a suite of common standards and protocols.

To enhance end-to-end interoperability, one of the most popular approaches is the usage of Service-oriented Architectures (SoAs). SoAs use common messaging protocols and well-defined interfaces to share information between multiple services. They consider aspects such as service reuse, rapid configuration, and composability with dynamic workflows. SoAs in the tactical domain could help to leverage commercial IoT capabilities and attempt to address the interoperability challenges specific to C4ISR.

Both military computers and sensor networks should have longer service lives than commercial equivalents, resulting in greater needs to maintain legacy systems. One of the key weaknesses of legacy systems is their lack of interoperability. This limits significantly the ability to integrate new platforms into the defense digital ecosystem, and to leverage existing systems in innovative ways.

DISA is implementing a cohesive digital architecture through the Joint Information Environment (JIE) initiative [159] to unify capabilities, facilitate collaborations with partners, consolidate infrastructure, create a single security architecture, and provide global access to services.

TacNet Tactical radios [160] help to demonstrate how an open systems architecture can enable improved interoperability between next-generation and legacy fighter aircrafts. Lockheed Martin performed tests on a F-22 and F-35 Cooperative Avionics Test Bed (CAT-B). Those aircrafts were flown to assess the capability to share real-time information among varied platforms. The ability to transmit/receive Link-16 communications on F-22 was proven, also the software reuse and reduction of the aircraft system integration and the use of Air Force UCI messaging standards.

U.S. Army CERDEC NVESD [161] has developed ISA under the Deployable Force Protection program. ISA is an interoperability solution that allows components to join a tactical network and use its functionality without requiring neither prior knowledge of the resources available on that network, nor physical integration. ISA uses dynamic discovery to find other ISA-compliant systems, regardless of platform. This dynamic discovery is accomplished by requiring all members to announce the data they provide and functionality they can perform when they connect to the network. Members can change their capabilities on the fly and search for others that provide either data or the functionality they need. ISA understands the capabilities of those sensors and shares their information with operators. When future sensors come online to a network, they can register and communicate their capabilities. Assets and sensors on that network can then subscribe to the types of information they are interested in. ISA seeks to provide the critical capabilities needed for a forward operating base to defend itself. It improves the mobile Soldier's situational awareness by enabling him to query different sensors as he moves through an area, and access to information that was previously unseen to him, such as event messages.

5.3.13 Target platforms

The complexity and high cost of defense systems mean that they will remain in service for years. As previously indicated, the longevity of ground/airborne/seaborne platforms, and a form factor designed for handheld or manpack use, creates interoperability issues as well as operational challenges when enhancing their capabilities and attaching them to the combat cloud. New technologies such as multi-core silicon and virtualization can create affordable solutions. On legacy single-core processors, this virtualization would have a direct impact on platform performance. The processor will have to run both legacy and new code while maintaining strict separation for safety and security reasons. With multi-core technology the performance and separation risks can be mitigated in silicon (with separated cores for legacy and new environments, and separated networks).

5.4 Building IoT for tactical and emergency environments

In order to understand the complex adoption of IoT for defense, this section will review briefly the basics of IoT landscape (a graphical overview of the main elements can be seen in Figure 5.7) to support the requirements previously explained. First, it focuses on the architecture with an overview of the most important elements. Next, the section examines the main standardized protocols and technologies.

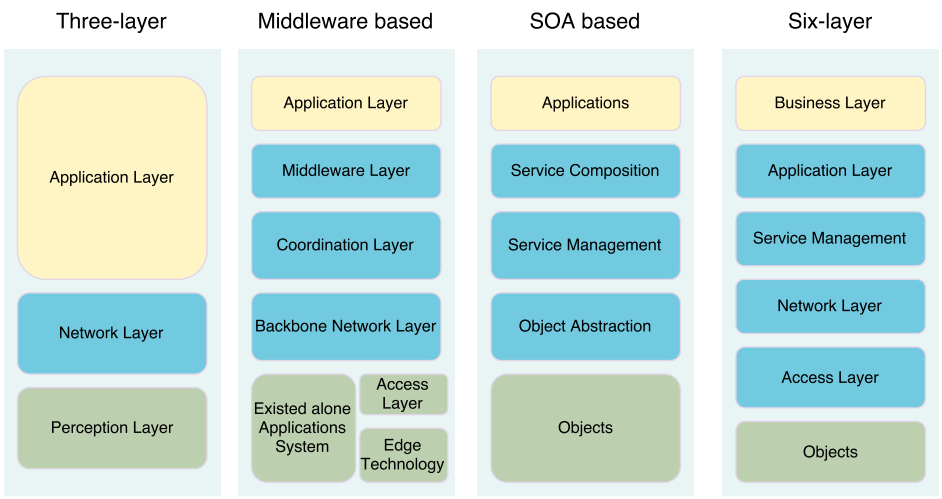


Figure 5.8: The IoT architecture. **(a)** Three-layer; **(b)** Middleware-based; **(c)** SOA-based; **(d)** Six-layer.

The increasing number of IoT proposed architectures has not converged to a reference model or a common architecture. In the latest literature, it can be distinguished among several models, as it can be seen in Figure 5.8. For example, the three-layered basic model (application, network and perception layers) was designed to address specific types of communication channels and does not cover all the underlying technologies that transfer data to an IoT platform.

Other proposals include a middleware based layer [162], a Service-Oriented Architecture (SOA) based model [163] and a six-layer model. There are differences between these models: for example, although the architecture is simpler in the three-layer model, layers are supposed to run on resource-constrained devices, while a layer like "Service Composition" in the SOA-based architecture takes a rather big fraction of the time and energy of the device.

Next, we provide a brief description on the functionality of the most common layers.

- Perception layer: this first layer represents the physical elements aimed at collecting and processing information. Most COTS IoT devices are designed for benign environments and currently focus on home automation, personal services and multimedia content delivery. Miniaturized devices such as transducers (sensors and actuators), smartphones, System on Chips (SoCs) and embedded computers are getting more powerful and energy efficient. The next generation of processors includes new hardware features aimed at providing highly trusted computing platforms. For example, Intel includes an implementation of the Trusted Platform Module (TPM) designed to secure hardware through cryptography. Technologies such as ARM TrustZone, Freescale Trust Architecture and Intel Trusted Execution

enable the integration of both software and hardware security features.Plug-and-play mechanisms are needed by this layer to configure heterogeneous networks. Big data processes are initiated at this perception layer. This layer transfers data to the Object Abstraction layer through secure channels.

- Object Abstraction Layer: it transfers data to the Service Management layer through secure channels. To transfer the data, the protocols used in the COTS IoT nodes either use existing wireless standards or an adaptation of previous wireless protocols in the target sector. Typically, IoT devices should operate using low power under lossy and noisy conditions. Other functions like cloud computing and data management processes are handled at this layer.

- Service Management Layer or Middleware: this layer enables the abstraction of specific hardware platforms. It processes the data received, takes decisions and delivers the services over network protocols.

- Application Layer: it provides the services requested to meet users' demands.

- Business Management Layer: this layer designs, analyzes, develops and evaluates elements related to IoT systems, supporting decision-making processes based on Big Data. The control mechanisms for accessing data in the Applications layer are also handled by this layer. It builds a business model based on the data received from the Application layer. Moreover, this layer monitors and manages the underlying four layers, comparing the output of each one with the output expected to enhance services and maintain users' privacy. This layer is hosted on powerful devices due to its complexity and computational needs.

A generic IoT architecture is presented in [164]. It introduces an IoT daemon consisting in three layers with automation, intelligence and zero-configuration: Virtual Object, Composite Virtual Object, and Service layer. An example of a possible military architecture can be seen in Figure 5.9.

The process of sensing consists in collecting data from objects within the network and sending them back to a data warehouse, a database or a cloud system, to be analyzed and act. Four main classes of IoT services can be categorized:

- Identity-related services: these services are employed to identify objects, but are also used in other types of services.

- Information Aggregation services: these services collect and summarize raw measurements.

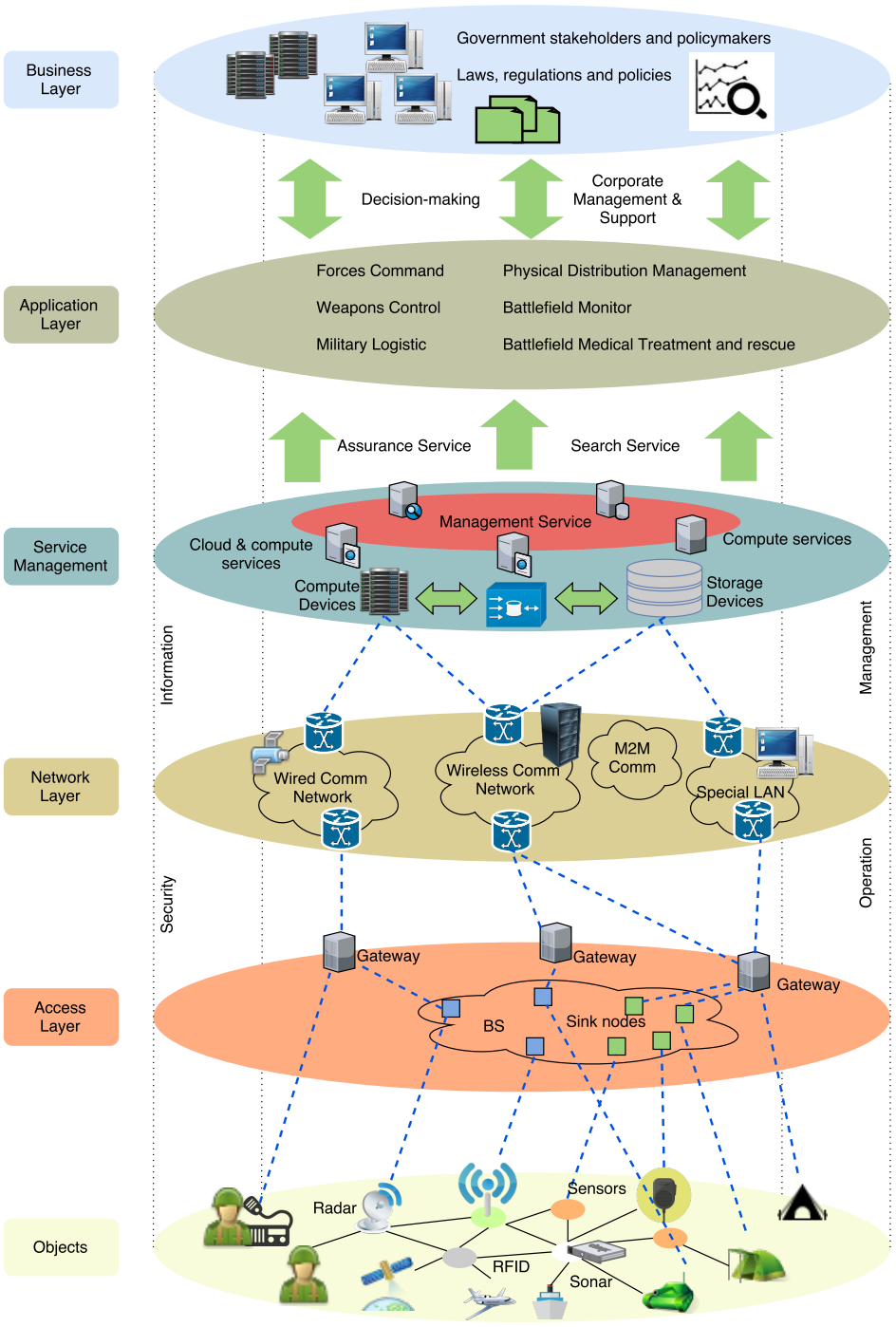


Figure 5.9: Example of military architecture with six layers.

- Collaborative-Aware services: these services act on top the Information Aggregation services and use the obtained data to make decisions.
- Ubiquitous services: these collaborative-aware services function anytime to anyone, anywhere.

Most existing applications provide the first three types of services. The ultimate goal are the ubiquitous services. Semantic analysis is performed after sensing to extract the corresponding knowledge. It includes discovering, resources usage and information modeling. Thereafter, recognizing and analyzing data to take proper decisions within the service. This is supported by semantic web technologies [165] such as the Resource Description Framework (RDF), the Web Ontology Language (OWL) or the Efficient XML Interchange (EXI), adopted as a W3C recommendation.

5.4.1 IoT standardized protocols

The U. S. Defense Standards, also called Military Standards (MIL-STD), are used to help achieve standardization objectives. These documents are also used by other non-defense government organizations, technical organizations and industry. The ASSIST database [166] gathers these documents and also includes international standardization agreements, such as NATO standards, ratified by the United States and International Test Operating Procedures. Furthermore, the DoD is starting to use civilian standards, since numerous contributions to the deployment and standardization of the IoT paradigm come from the scientific community. Among them, the most relevant are the ones provided by the European Commission and the European Standards Organisations (i.e., ETSI, CEN, CENELEC), by their international counterparts (i.e., ISO, ITU) and by other standards bodies and consortia (W3C, Institute of Electrical and Electronics Engineers (IEEE), EPCglobal). The M2M Workgroup of the ETSI and some IETF Working Groups are particularly important.

In this section we provide an overview of some of the standardized protocols that could be used for providing the IoT services described in the previous sections.

5.4.1.1 Application Layer protocols

The following are the most popular Application Layer protocols: Constrained Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP) and Data Distribution Service (DDS). Performance evaluations and comparisons among them have been reported in the literature [167]. Each of these protocols may perform rather well in specific scenarios, but there is no evaluation of all these

protocols together. Consequently, it is not possible to provide a single prescription for all IoT applications, just that they must be designed from the ground up to enable extensible operations.

5.4.1.2 Service discovery protocols

Resource management mechanisms are able to register and discover resources and services in a self-configured, efficient and dynamic way. Such protocols include CoAP resource discovery, CoAP Resource Directory (RD), and DNS Service Discovery (DNS-SD), which can be based on mDNS (Multicast DNS). A detailed description of their characteristics can be seen in [168].

5.4.2 Enabling technologies

Most popular communications technologies include CAN bus, Common Industrial Protocol (CIP), Ethernet, UPB, X10, Insteon, Z-wave, EnOcean, nanoNET, IEEE 802.15.4 (6LowPAN, Zigbee), IEEE 802.11 (Wi-Fi), Bluetooth (Bluetooth Low Energy). The work in [169] investigates IEEE 802.15.4 against IEEE 802.11ah. The latter achieves better throughput than IEEE 802.15.4 in both idle and non-idle channels, although IEEE 802.15.4 presents lower energy consumption, especially in dense networks. Furthermore, cellular networks include WiMAX and 4G/5G LTE. Highly integrated chipsets exist for most of these protocols, allowing for easy hardware integration. The protocols mentioned have supporting development environments and in some cases manufacturers offer open source APIs.

The protocols presented offer at least some form of rudimentary congestion control, error recovery and some ad-hoc capabilities. None of the communication protocols are designed for an actively hostile environment. Another specific technologies in use are RFID, Near Field Communication (NFC) and Ultra-Wide Band (UWB).

5.4.3 Enabling protocols

This subsection briefly addresses two main concerns: network routing and identification, and RFID identification protocols. Regarding routing protocols, Routing Protocol for Low Power and Lossy Networks (RPL) is an IETF routing protocol based on IPv6 created to support minimal routing requirements through a robust topology (Point-to-Point (PtP), PMP).

On the other hand, nowadays, the unique addresses follow two standards: Ubiquitous ID and EPC Global. The EPC (Electronic Product Code) is a unique identification number stored on an RFID tag that is used basically in the supply chain management

to identify items. In order to decrease the number of collisions in the EPC Gen-2 protocol, and to improve tag identification procedure, researchers have proposed to use Code Division Multiple Access (CDMA) instead of the dynamic framed slotted ALOHA. A performance analysis of the RFID protocols in terms of the average number of queries and the total number of transmitted bits required to identify all the tags in the system can be seen in [170]. The expected number of queries for tag identification using the CDMA technique is lower than that of the EPC Gen-2 protocol, because CDMA decreases the number of collisions. However, when comparing the number of transmitted bits and the time to identify all tags in the system, EPC Gen-2 protocol performs better. The EPC Global architectural framework is based on the EPC Information Service, which is provided by the manufacturer, and the ONS (Object Naming Service) that offers features similar to DNS (Domain Name Service). Being a central lookup service, the root of the ONS can be controlled or blocked by a company/country, unlike the DNS system.

Identification methods, such as ubiquitous codes (uCode) and Electronic Product Codes (EPC), are not globally unique, although they provide a clear identity for each object within the network. Addressing methods of IoT objects, that include IPv4/IPv6, assist to uniquely identify objects.

5.4.4 Computation

This subsection reviews the main hardware and software platforms and concepts such as cloud platforms, fog computing and digital analytics.

5.4.4.1 Hardware and software platforms

The growth of smartphone use over the last years has provided the basis for IoT hardware platforms. This tendency derives into new products being presented to the market at a fast pace. SoCs with very low power consumption, small form factor and oriented at supporting wireless communication technologies such as Wi-Fi and BLE, are being developed and enhanced. Arduino, Raspberry Pi, UDOO, FriendlyARM, Intel Galileo, Gadgetter, ESP8266, BeagleBone, Cubieboard, Zolertia Z1, WiSense, Mulle, and T-Mote Sky are just some examples of popular hardware platforms. Most of such devices are built on top of hardware solutions based on ARM Cortex M microcontrollers or ARM Cortex A microprocessors, but some use their own SoCs.

All these hardware platforms can be divided into two groups. On the one hand, there are SBCs (Single-Board Computers) like Raspberry Pi and Intel Galileo, which are powerful, and usually run some kind of modified Linux distribution. They support a vast set of security and communication alternatives, but their power consumption

is high. On the other hand, the second type of platforms includes the motes. The ESP8266 or T-Mote Sky are good examples. They are much less power-hungry, being able to run on standard batteries for extended periods of time. However, they lack the processing capabilities of SBCs, and run on proprietary or ad-hoc software. In addition, one of the main problems of the currently available commercial motes is their lack of support for secure communication protocols and encryption. Nonetheless, motes recently presented address such an issue: for instance, the Arduino MKR1000 includes hardware acceleration for Elliptic Curve Cryptography (ECC), and the ESP32 has support for AES-256, SHA2, ECC and RSA-4096.

Regarding software platforms, examples of Real-Time Operating Systems (RTOS) are Android, Contiki, TinyOS, LiteOS or Riot OS. The most common advanced programming environments and open standards are ARINC 653, Carrier Grade Linux, Eclipse, FACE, and POSIX. It must be also noted that Google and other important technological companies partnered with the auto industry to establish the Open Auto Alliance (OAA) to bring additional features to the Android platform to advance in the Internet of Vehicles paradigm.

5.4.4.2 Cloud platforms

Connected devices need mechanisms to store, process and retrieve data efficiently. However, the amount of data collected in an IoT deployment may exceed the processing power of regular hardware and software tools. Moreover, IoT applications have to be able to detect patterns or anomalies in the data when processing large amounts of data.

The emerging and developing technology of cloud computing is defined by the U.S. National Institute of Standards and Technology (NIST) as an access model to an on-demand network of shared configurable computing sources. Cloud computing enables researchers to use and maintain many resources remotely, reliably and at a low cost. The storage and computing resources of the cloud present the best choice for the IoT to store and process large amounts of data. There are some platforms for big data analytics like Apache Hadoop and SciDB [171]. The DoD is also trying to accelerate the adoption of commercial clouds. The cloud security model [153] defines six information impact levels from 1 (public information) to 6 (classified information up to secret). As of May 2015, there were 26 Level 2 (Unclassified, Low-Impact) commercial cloud services approved with more on the way. Regarding Level 4/5 (Controlled Unclassified Information), there were one milCloud [172] and one commercial cloud solution with more on the way. With respect to Level 6, there was one milCloud.

In terms of resources, besides the powerful servers in data centers, a lot of smart devices around us offer computing capabilities that can be used to perform parallel IoT data

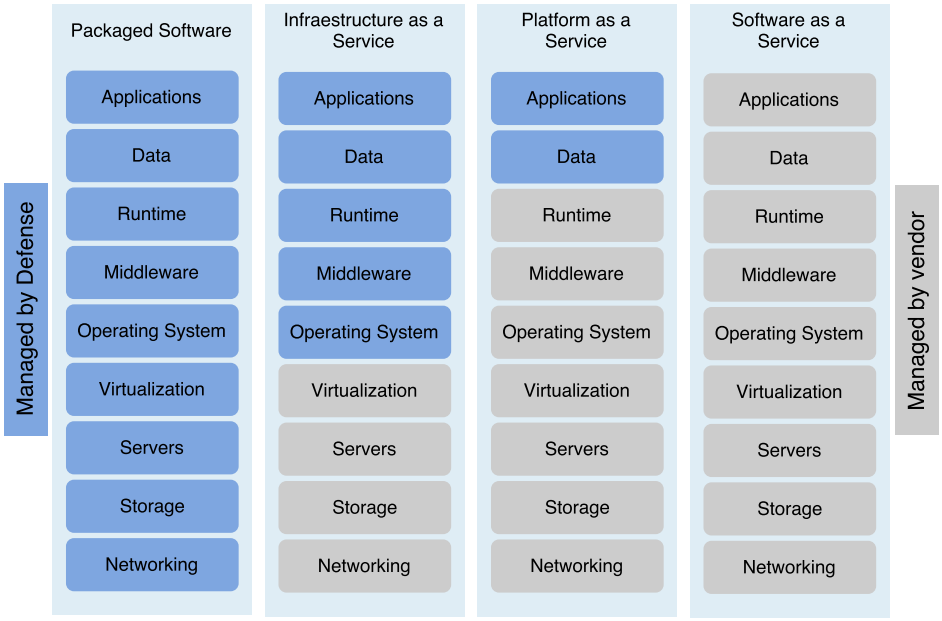


Figure 5.10: Cloud paradigms: security inheritance and risks.

analytic tasks. Instead of providing applications specific analytics, IoT needs a common big data analytic platform which can be delivered as a service to IoT applications. Such an analytic service should not impose a considerable overhead on the overall IoT ecosystem.

The three most popular cloud paradigms are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Their structure and corresponding security risks are represented in Figure 5.10.

A scalable analytic service for time series data, Time Series analytics as a Service (TSaaaS), is presented in [173]. Pattern searching in TSaaaS can support effective searching on large amounts of time series data with very little overhead on the IoT system. TSaaaS is implemented as an extension to the Time Series Database service and it is accessible by RESTful web interfaces. Pattern searches are 10-100 times faster than other existing techniques, and the additional storage cost for the service provider accounts for only about 0.4% of the original time series data.

Other feasible solution for IoT big data is to just keep track of the interesting data. Existing approaches include Principle Component Analysis (PCA), pattern reduction, feature selection, dimensionality reduction, and distributed computing methods [171].

IoT can use numerous cloud platforms with different capabilities and strengths such as Google Cloud, AWS, Bluemix IoT Solutions, GENI, ThingWorx, OpenIoT, Arkessa, Axeda, Etherios, LittleBits...besides public safety providers such as Avaya, Huawei Enterprise, West, or Microsoft. For example, Xively [174] provides an open source PaaS

solution for IoT application developers and service providers. It aims to securely connect devices to applications in real-time, it exposes accessible Application Programming Interfaces (APIs), and it provides interoperability with many protocols and environments. It enables the integration of devices with the platform by libraries and facilitates communication via HTTP(s), Websocket, or MQTT. It integrates with other platforms using Python, Java, and Ruby libraries; and distributes data in numerous formats such as JSON, XML and CSV. It also allows users to visualize their data graphically and to remotely control sensors by modifying scripts to receive and send alerts. It is supported by many Original Equipment Manufacturers (OEM) like Arexx, Nanode, OpenGear, Arduino or mBed.

Nimbits [175] connects smart embedded devices to the cloud, performs data analytics and generates alerts. Moreover, it connects to websites and can store, share and retrieve sensor's data in various formats, including text based, numeric, GPS, JSON or XML. It uses XMPP to exchange data or messages. The core is a server that provides REST web services for logging and retrieving raw and processed data.

The authors of [176] summarize some of the characteristics of a number of available cloud platforms. The metrics include: support of gateway devices to bridge the short range network and wide area network, support of discovery, delivery, configuration and activation of services, provision of a proactive and reactive assurance of platform, support of accounting and billing of services and, finally, support of standard application protocols. All the platforms analyzed by the authors support sensing or actuation devices, a user interface to interact with them, and a web component to run the business logic of the application on the cloud. None of such platforms supports the DDS protocol.

Voegler et al. [177] propose a novel infrastructure to provide application packages on resource-constrained heterogeneous edge devices elastically in large-scale IoT deployments. It enables push-based (commands down to the tactical units) as well as pull-based (from ground to decision-making) deployments supporting different topologies and infrastructure requirements.

The efficient use of cloud based resources requires the previous selection of software architectures for both communications and processing. Centralized cloud approaches, in which raw data are transmitted to the cloud for analysis, are non-viable in military IoT scenarios. For instance, even if a device has a high-bandwidth link to a local resource, it is not likely that all devices will have good connectivity to the same cloud-based platform. Thus, relying on tactical wireless networks, any approach that requires a centralized cloud infrastructure is not likely to work properly. Moreover, in a centralized cloud infrastructure, processing represents a complex and computationally expensive procedure, which leverages sophisticated big data tools. Finally, there is a significant delay between the time of the IoT data generation and when the results become available.

In order to address the issue of distributed infrastructures for IoT data analysis, researchers have started investigating distributed cloud architectures. The idea consists in extending and complementing a small number of large cloud data centers located in the core of the network, where most computational and storage resources are concentrated, with a large number of tiny cloud data centers located at the boundary between the wired Internet and the IoT. This would enable data analysis applications to benefit from the elastic nature of cloud-based resources while pushing the computation closer to the IoT, with obvious advantages in terms of reducing communications overhead and processing times. There is also research to support the processing of raw IoT data close to the source of their generation, particularly the processing and filtering of raw IoT data and the exploitation of IoT specific computational solutions for data analysis purposes. Several proposals have emerged from the realization that not all the raw data generated are equally important and that applications might be better served by focusing only on important data. The Quality of Information (QoI) and Value of Information (VoI) concepts arise to extend Shannon's information theory to consider both the probabilistic nature of the uncertainties. These efforts are highly relevant for the military IoT, since the processing and exploitation of the information is made according to the utility for its users. Thus, the ability of supporting the user in more effective decision making has potential to reduce the amount of computational and bandwidth resources required for data analysis and dissemination.

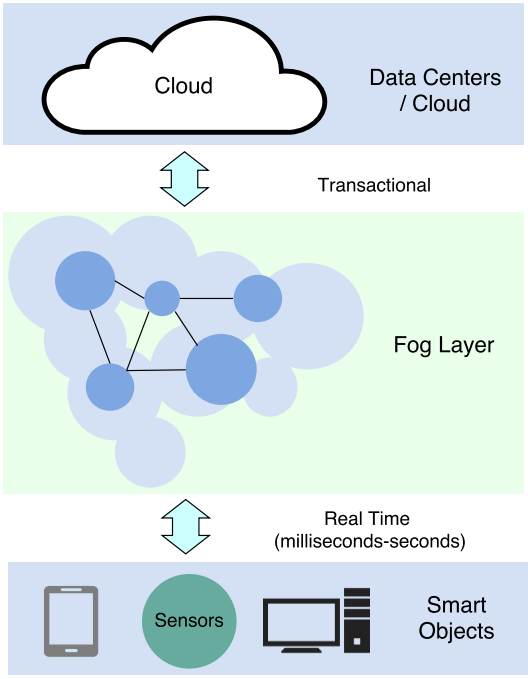


Figure 5.11: Fog Computing Paradigm.

Emerging hardware and computational solutions for embedded platforms require new software architectures to fulfill their potential. For instance, neuromorphic processors, hybrid CPUs/FPGAs processors feature programming models that are different from those of the server CPUs typical of cloud data centers.

5.4.4.3 Fog computing

Several research concepts, such as fog computing, cloudlets, mobile edge computing and IoT-centric clouds have been recently proposed to complement the distributed cloud architectures for IoT data analysis and security [178]. Fog computing has the potential to increase the overall performance of IoT applications as it tries to perform part of high level services, which are offered by the cloud, inside local resources. This paradigm is depicted in Figure 5.11.

Researchers have focused mostly so far on how to extend elastic resource consumption paradigms and big data solutions to distributed cloud configurations, instead of proposing new methodologies, paradigms and tools to efficiently exploit the capabilities of IoT hardware. Fog computing can act as a bridge between smart devices and large-scale cloud computing and storage services. Because of their proximity to the end-users, it has the potential to offer services faster. There is a significant difference in scale between the fog and the cloud: the latter has massive computational, storage, and communications capabilities compared to the former. Mobile network operators are potential providers of fog computing since they can offer fog services like IaaS, PaaS, or SaaS at their service network or at a cell tower, or even a type of transversal service, that is IoT as a Service (IoTaaS).

Fog computing still needs research to resolve other issues like reliability, mobility and security of analytical data on the edge devices. Chang et al. [179] presented a fog computing model that brings information-centric cloud capabilities to the edge in order to deliver services with reduced latency and bandwidth. This situation calls for the need of a better horizontal integration between different application layer protocols. Several attempts of integration have been made in recent literature. For example, Ponte [180] offers uniform open APIs to enable the automatic conversion between various IoT applications protocols such as HTTP, CoAP, and MQTT. Nevertheless, the capability to perform any-to-any automatic protocol conversion implies that the underlying packet communication tends to be more verbose in order to be application agnostic. Furthermore, Ponte assumes the underlying devices to be TCP/IP enabled similarly to many other protocol gateways. Also, resource-constrained devices are not considered at all in this solution.

The fulfillment of complex requirements such as ubiquity, scalability and high-performance lead to a convergence between the IoT and cloud through federation and multi-cloud architectures. Cloud federation is one of the core concepts for the design, the deployment and the management of decentralized edge cloud infrastructures. Since federated systems inherit all of the fundamental aspects of distributed computing, they can certainly leverage many existing standards that have been developed in this arena over the past years.

The near-future evolution of IoT clouds is discussed in [181] where the authors describe a three-stage evolution towards the creation of an IoT federation. The first of such stages is called monolithic and involves embedded devices that would be connected to IoT cloud systems to provide basic IoTaaS (the services would be developed either with stand-alone pieces of software or by means of container virtualization technology). The next stage is named vertical supply chain. In such a stage, the IoT cloud providers leverage IoTaaS offered by other providers. Finally, the third stage corresponds to the real IoT cloud federation, where IoT cloud providers will federate to extend their sensing capabilities, adopting the container virtualization technology massively in order to create more flexible IoTaaS.

Likewise, numerous research projects and initiatives focus on the realization of innovative architectures for the Cloud-IoT, enabling features such as autonomous service provisioning and management. Indicatively, such a concept may be applicable to 5G technological solutions [182] like SDN. For example, cloud-based mechanisms will enable the incorporation of resources and services independent of their location across distributed computing and data storage infrastructures. The challenge will be the integration of these different standardized capabilities into a coherent end-to-end federation model. According to the cloud federation's organization, access and scale, six federation deployment models can be identified [183]: simple pairwise federation, hierarchical federation, peer-to-peer federations, brokers or interclouds.

The main challenges of employing cloud computing for the mission-critical IoT include the synchronization to provide real-time services (since they are built on top of various cloud platforms); the need for a balance between cloud service environments and IoT requirements, considering the differences in infrastructure; and to solve issues like the lack of standardization, the complicated management and the enhancement of the reliability and the security. Hashizume et al. [184] provide an analysis of vulnerabilities, threats and countermeasures in the cloud considering the three service delivery models: SaaS, PaaS and IaaS. The article ends emphasizing the need for new security techniques (such as firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and data protection) as well as the redesign of traditional cloud solutions.

There are two main security challenges in the cloud-centric IoT: secure storage and authorized data sharing in near real time. Authentication prevents access by illegitimate users or devices, and it prevents legitimate devices from accessing resources in an unauthorized way. Scalable authentication schemes have been widely studied for traditional computer networks as well as WSNs. Cloud-centric authentication as a service has also been considered to minimize task overhead on user devices. For example, Butun et al. [116] present a hierarchical authentication as a service for public safety networks. The proposed lightweight cloud-centric multi-level framework addresses scalability for IoT-worn devices. In the proposed CMULA scheme, public safety responders and devices are authenticated through the Cloud Service Provider (CSP). This approach enables easier mobility management. The network consists of four entities: users (the chief officers who are registered in the emergency system and are responsible for managing the responders on site), wearable nodes, a Wearable Network Coordinator (WNC) (responsible for managing all sensors attached to the responders body), and a CSP that serves as certification authority for the IoT-based public safety network. It considers a public key infrastructure (PKI) issuing ECC throughout the cloud-centric IoT. Elliptic Curve Digital Signature Algorithm (ECDSA), a variant of ECC, is used for digital certificate generation and verification. Another variant of ECC, the Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm, is used to exchange the secret message authentication code (MAC) keys in the initialization phase. Once a user is authenticated to a CSP, wearable devices can be accessed through a WNC. Other existing studies on cloud security focus on issues concerning cloud security, identity management, and access control or architecture layers. For example, Li et al. [185] review mechanisms and open issues for mobility-augmented service provisioning. As a result, they discover open challenges with respect to overhead, heterogeneity, QoS, privacy and security. Authors in [186] provide an integrated solution to cloud security based on the so-called Cloud Computing Adoption Framework (CCAF) framework. It protects data security and predicts the probable consequences of abnormal situations by using Business Process Modeling Notation (BPMN) simulations. The multi-layer description of CCAF is as follows. The first layer is for access control: a firewall allows the access just to certain members. The second layer consists of the IDS/IPS to provide up-to-date technologies to prevent attacks such as DoS, anti-spoofing, port scanning, pattern-based attacks, parameter tampering, cross site scripting, SQL injection or cookie poisoning. The identity management is enforced to ensure that the right level of access is only granted to the right person. Finally, the third layer is convergent encryption. The results of CCAF expose real-time protection of all the data, blocking and quarantining the majority of the threats.

5.4.5 Digital analytics

Analytical software manages the excessive volume of data that needs to be transferred, stored and analyzed. It would require flexible acquisition processes by the governments to integrate cutting-edge technologies quickly. Many applications would depend on real-time analysis to enable automated responses. Other systems would process data into simple interfaces that allow humans to leverage big data in convenient ways.

Semantic Web technologies have been acknowledged as important to support for data integration, reasoning and content discovery [187]. Particularly, three established elements have been identified as desirable IoT tactical capabilities:

- Open Integration standards: they facilitate interoperability among devices with different capabilities and ownership through supporting ontologies. IoT ontologies should be integrated with existing community standards.
- Reasoning support: Ontology-based reasoning has been applied towards military sensor management systems, including the assignment of sensors to mission tasks. Gomez et al. [188] present an ontology based on Military Missions and Means Framework that formalizes sensor specifications as well as expressing corresponding task specifications. When there is limited network connectivity, such reasoning capabilities could be applied to continually assess how available IoT resources can be utilized.
- Data Provenance: the steps taken to generate data have been commonly acknowledged as important towards assessment of data quality and trustworthiness. In a military context, issues of provenance will be a dominant concern because the state, ownership, and reliability of devices will be uncertain. The capability will be critical when automated or semi-automated content assessment becomes desirable. New architectures will need to incorporate provenance and trust management tightly integrated in IoT technologies. The W3 PROV specification [189] is a primary standard for digital provenance representation, which is now being extended for IoT.

5.5 Main challenges and technical limitations

There are significant challenges in the development and deployment of existing and planned military IoT systems. Nowadays, only a small number of military systems leverage the full advantages of IoT. Ongoing NATO Research Task Group (RTG) 'Military Applications of Internet of Things' (IST-147) is examining a number of critical issues identified by the recommendations from two previous exploratory team

activities: IST-ET-076, 'Internet of Military Things' which examined topics relevant to the application of IoT technologies, and IST-ET-075, 'Integration of Sensors and Communication Networks', which addressed networking issues. The deployment of IoT-related technologies is in segregated vertical stovepipes making it difficult to secure them, and limiting the ability to communicate across systems and generate synergies from different data sources. Main defense concerns include the dependence of manual entry, the limited processing of data, the lack of automation, and the fragmented IT architecture.

Furthermore, nowadays the military does not have sufficient network connectivity on the battlefield to support broader IoT deployments. It will require key investments in several technical enablers according to its information value loop [117]. The roadmap for near-future research and technology developments is depicted in Table 5.1.

As seen in Table 5.1, security is the most significant demand for IoT adoption across the military. Defense faces a large number of simple devices and applications with unique vulnerabilities for electronic and cyber warfare. Data analytics and process capacity are additional limiting factors.

Table 5.1: Roadmap for technologies and ongoing research.

Research	**Timeframe 2017–2020**
Identification	• Identity management • Open framework for the IoT • Soft Identities • Semantics • DNA identifiers • Convergence of IP and IDs and addressing scheme: unique or multiple IDs • Extend the ID concept (more than ID number) • Electro Magnetic Identification (EMID) • Multi methods, one ID
Architecture	• Network of networks architectures • Adaptive and context based architectures • Self-managing properties (they include self-configuring, self-healing, self-optimizing, self-protecting, self-awareness, self-adaptation, self-evolving and self-anticipating) • Cognitive and experimental architectures • Code in tags to be executed in the tag or in trusted readers with global applications, adaptive coverage, universal authentication of objects, recovery of tags following power loss, more memory, less energy consumption, 3-D real time location/position embedded systems • Cooperative position cyber-physical systems
Infrastructure	• Cross domain application deployment • Integrated IoT, multi-application and multi-provider infrastructures • General purpose IoT: global discovery mechanism

Research	Timeframe 2017–2020
Applications	• IoT device with strong processing and analytics capabilities • Handling heterogeneous high capability data collection and processing • Application domain-independent abstractions and functionality • Cross-domain integration and management • Context-aware adaptation of operation • Standardization of APIs • Mobile applications with bio-IoT-human interaction
Communications	• Wide spectrum and spectrum aware protocols • Ultra-low power system on chip, multi-protocol chips • Multi-functional reconfigurable chips • On-chip antennas • On-chip networks and multi-standard RF architectures • Seamless networks • Gateway convergence • Hybrid network technologies convergence • 5G developments • Collision-resistant algorithms • Plug-and-play tags, self-repairing tags
Network	• Self-aware, self-configuring, self-learning, self-repairing and self-organizing networks • Sensor network locations transparency • IPv6-enabled scalability • Ubiquitous IPv6-based IoT deployment • Software defined networks • Service based network • Multi authentication, integrated/universal authentication • IPv6-based Internet of Everything (smart cities) • Robust security based on a combination of ID metrics
Software	• Goal oriented: distributed intelligence, problem solving, Things-to-Things collaboration environments • IoT complex data analysis • IoT intelligent data visualization • Hybrid IoT • User oriented: the invisible IoT, things-to-Humans collaboration, IoT 4 All and User-centric IoT • Quality of Information and IoT service reliability • Highly distributed IoT processes • Semi-automatic process analysis and distribution • Fully autonomous IoT devices • Micro operating systems • Context aware business event generation • Interoperable ontologies of business events
Signal Processing	• Context aware data processing and data responses • Distributed energy efficient data processing • Cognitive processing and optimization, common sensor ontologies (cross domain)

Research	Timeframe 2017–2020
Discovery	• Automatic route tagging and identification management centers • Semantic discovery of sensors • Cognitive search engines • Autonomous search engines • Scalable Discovery services for connecting things with services while respecting security, privacy and confidentiality
Energy efficiency	• Energy harvesting (biological, chemical, induction) • Power generation in harsh environments • Biodegradable batteries • Nano-power processing unit • Energy recycling • Long range wireless power • Wireless power everywhere, anytime
Security	• Low cost, secure and high performance identification/authentication devices • User centric context-aware privacy • Privacy aware data processing • Security and privacy profiles and policies • Context centric security • Homomorphic Encryption, searchable Encryption • Protection mechanisms for IoT DoS/DdoS attacks • Self-adaptive security mechanisms and protocols • Access control and accounting schemes • General attack detection and recovery/resilience • Cyber Security • Decentralized self-configuring methods for trust establishment • Novel methods to assess trust in people, devices and data • Location privacy preservation • Personal information protection from inference and observation • Trust Negotiation
Interoperability	• Automated self-adaptable and agile interoperability • Reduced cost of interoperability • Open platform for IoT validation • Dynamic and adaptable interoperability for technical and semantic areas
Standardization	• M2M standardization • Standards for cross interoperability with heterogeneous networks • Standards for IoT data and information sharing • Standards for autonomic communication protocols • Interaction standards • Behavioral standards
Hardware	• Smart bio-chemical sensors • Nano-technology and new materials • Interacting/Collaborative tags • Self-powering sensors

Research	Timeframe 2017–2020
Hardware	• Polymer based memory, ultra-low power EPROM/FRAM • Molecular sensors • Transparent displays • Biodegradable antennas • Nano-power processing units • Biodegradable antennas • Multi-protocol frontends • Collision free air to air protocol and minimum energy protocols • Multi-band, multi-mode wireless sensor architectures implementations • Reconfigurable wireless systems • Micro readers with multi-standard protocols for reading sensor and actuator data • System-in Package (SiP) technology including 3D integration of components

5.5.1 From COTS to mission-critical IoT: further recommendations

Despite the ongoing technological research, the following recommendations were obtained from the analysis of the previous sections:

- Rapid field testing should be introduced: the military should consider creating a dedicated technology comprising military personnel in a live training environment to experiment with technologies and get real end-user feedback early in the development process. This testbed could change the way the military accomplishes its mission, or introduces creative new ways to use IoT devices and applications. Its goal would be twofold: to recognize devices and systems with potential applications and, second, to identify completely new strategies, tactics, and methods for accomplishing missions using COTS.

- The military can, to a certain extent, take advantage of civilian mobile waveforms such as 4G/5G LTE. Nevertheless, those advances will need to be paired with military-specific communications architectures (e.g., multiband radios with scarce bandwidth, MANET topologies and defensive countermeasures).

- Platform as a Service (PaaS) should be used to deliver web-based services without building and maintaining the infrastructure, thereby creating a more flexible and scalable framework to adjust and update the systems. Adopting PaaS also carries risks for the military and requires private contractors to implement additional security procedures.

- A comprehensive trust framework should be realized to support all the requirements of IoT for the military. Many state-of-the-art approaches that address issues such as trust and value depend on inter-domain policies and control. In military

environments, policies will likely be contextual and transient, conflated by inter-organizational and adversarial interactions.

- Information theories will need to focus on decision making and cognitive layers of information management and assimilation. Further, methods for eliciting causal relationships from sparse and extensive heterogeneously-sourced data will require additional theoretical research.

There are key enabling technologies in which governments and defense can invest today to enable greater IoT deployment in the near future. Besides, the adoption of IoT will require the compromise of all stakeholders. Another constraint is the current budget environment: Defense is reluctant to spend limited budgets on up-front costs for generating significant future savings. Defense should adopt new ways to access innovation, adopting commercial best practices for technology development and acquisition. An enhanced collaboration with the private sector is needed to field and update IoT systems with cutting-edge technology. Cultural differences between defense and private sector innovators, as well as intellectual property and export restrictions, discourage companies from collaborating with the military. Also companies and innovators may see little benefit in catering the complex and demanding operational requirements of defense and public safety, which is a small and demanding customer in comparison to commercial markets. Creating affordable and high-value systems that deliver enhanced situational awareness for military has a proven business value. Complementing this intelligence with integrated commercial IoT data is also a compelling business model for innovative defense and public safety contractors and system integrators.

5.6 Conclusions

This chapter examined how the defense industry can leverage the opportunities created by the commercial IoT transformation. Main topics relevant to the application of IoT concepts to the military and public safety domain were explained. In order to perform the study, different relevant scenarios were proposed such as: C4ISR, fire-control systems, logistics (fleet management and individual supplies), smart city operations, personal sensing, soldier healthcare and workforce training, collaborative and crowd sensing, energy management and surveillance. The added value and the risk of applying IoT technologies in the selected scenarios were also assessed. Based on the operational requirements, architectures, technologies and protocols that address the most significant capabilities were proposed.

Commercial IoT still faces many challenges such as standardization, scalability, interoperability and security. Researchers working on defense have to cope with additional

issues posed by tactical environments and the nature of operations and networks. There are three main differences between defense/public safety IoT and COTS IoT: the complexity of the deployments, the resource constraints (basically the ones related to power consumption and communications) and the use of centralized cloud-based architectures.

Organic transitions such as supply chain management and logistics will naturally migrate to mission-critical environments. Beyond the earliest military IoT innovations, complex battlefields will require additional research advances to address the specific demands. In addition to addressing various technical challenges, this work identified vital areas of further research in the 2017-2020 timeframe. Moreover, battlefield domains that closely integrate human cognitive processes will require new paradigms in the current Information Theory that scale into deterministic situations.

It can be concluded that a broader deployment of defense and public safety IoT applications will take time. Nevertheless, there are areas where governments and defense can generate significant savings and advantages using existing COTS technologies and business practices. Defense and public safety needs to adopt best practices for technology development and acquisitions from the private sector, and should consider a bottom-up model of innovation and procurement. As in any industry, there is no one-size-fits-all solution to the IoT for defense. The military and first responders should establish a testbed for identifying and experimenting with technologies that could remodel the way missions are accomplished, and which would serve as a link between warfighters in the field and IoT developers. The military should invest in developing new security techniques that can be applied to COTS devices and applications, including those hosted in the cloud. The focus should be on investing in scalable security measures instead of securing individual systems. This approach will give defense and public safety greater leverage in their IoT investments, allowing them better returns per dollar spent on proprietary R&D while exploiting the military IoT potential.

Chapter 6

A Real-Time Pipe Monitoring Cyber-Physical System for the Shipyard 4.0

6.1 Introduction

After the triumph of the lean production systems in the 1970s, the outsourcing manufacturing phenomenon of the 1990s, and the automation that took off in the 2000s, the fourth major disruption in modern manufacturing is Industry 4.0. This industrial revolution can be defined as the next phase in the digitalization of the sector [190], driven by several emerging technologies: the ubiquitous use of sensors, the stunning rise in data volume, the increasing computational power and connectivity, the emergence of analytics, cloud computing and business-intelligence capabilities, new forms of human-machine interaction such as augmented-reality systems, and advances in transferring digital instructions to the physical world, such as CPS, IoT, robotics, and 3-D/4-D printing. Most of these technologies are mature and have been present for some time. Although some of them are not yet ready for a broader application, many are now at a position where their greater reliability and cost-effectiveness are starting to be appealing for industrial applications.

In the short-term, Industry 4.0 is expected to have a major effect on global economies. PwC's 2016 Global Industry 4.0 Survey [191] suggests that annual digital investments are expected to achieve US$907 bn per year through 2020. Survey respondents anticipate that those investments will lead to US$493 bn in additional revenues annually. Furthermore, savings are estimated at US$421 bn in costs and efficiency gains each year.

The foundations of the Industry 4.0 can be transferred straight to a mission-critical infrastructure like a Shipyard 4.0. The deployment of Cyber-Physical Systems in pro-

duction systems gives birth to the "smart factory" and, analogously, to the "smart shipyard". Products, resources, and business and engineering processes are deeply integrated making production operate in a flexible, efficient and green way with constant real-time quality control, and cost advantages in comparison with traditional production systems. Machinery and equipment will have the ability to improve processes through self-optimization and autonomous decision-making. Shipbuilders face similar challenges as industry [192], which can be classified into three main concerns: the vertical integration of production systems, the horizontal integration of a new generation of networks that create added-value, and the acceleration of technologies that require the re-engineering of the entire production chain.

The vertical integration of production systems changes naval production chains. It entrusts the intelligent shipyards to ensure safe production. The more environmental friendly smart ships are capable of network operating together with other ships and ground infrastructure. The horizontal integration of a new generation of value creation networks is critical as it provides an integrated way to satisfy the demands from the different stakeholders, allowing for the customization of ships in a short period of time.

The third challenge is the end-to-end digital integration of engineering across the entire value chain, ranging from design to after-sales service. This evolution implies introducing disrupting technologies that affect the entire life cycle of each piece of the ship: acceleration technologies, such as artificial intelligence, robotics, virtual reality, driverless vehicles for the transport of parts, drones, remote sensing networks or 3D/4D printing, among others. The aim of these technologies is, primarily, to allow shipyards to collect more data and make better use of it. For example:

- Naval Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities will be impacted by the development of a number of technologies based on the information extracted from the emerging data.

- Curved 3D organic light emitting diode (OLED) displays will be supported by form factors that take advantage of capabilities such as voice, handwriting, touch, gesture, eye movement or even brain control. Designers will be able to interact with their designs without a keyboard or mouse, Human-Computer Interfaces (HCI) will encourage innovation and efficient design workflow. Such interfaces will be able to support more natural modes of interaction and will be more intuitive and therefore easier to operate, reducing the need for training.

- Data obtained from remote sensing and intelligent algorithms will accelerate the ship design process, and 2D design will be easily converted into 3D.

- Complex construction and inspection tasks will be supported by augmented reality.
- Graphene strips, with sensors allocated alongside the hull, will provide more accurate data about the hull's working conditions. These will monitor external (seawater temperature, impacts, and fouling) and internal factors (stresses, microbial induced corrosion, and bending). This information will enable a new approach called Hull-Skin-Data centered decisions that would be adopted according to those working parameters.
- An increasing number of embedded sensors will be fitted to pipes so that new laser technologies and robotics can speed up the cutting process. Adaptable hull forms will be developed to better tackle different speed profiles and changing load conditions. Robots will also control the curvature of materials more precisely, thus offering optimal hull form. Moreover, a ballast-free design will be further developed to reduce the transfer of marine invasive species across different waters.
- Instead of leaving the majority of outfitting tasks until the moment after launching, some outfitting, such as piping and heavy machinery, will be developed together with the hull structure speeding the building process up.
- Progressive sensorization will enable automated casting, forging, rolling, cutting, welding or cleaning [193].
- Time spent on the outfitting along the quay will be minimized. Robotics will capture 3D images throughout the vessel and will establish a reference dataset to support real-time ship operations and life maintenance.
- Enhanced crane-lifting capabilities will speed production time up.

Furthermore, with the development of applications based on these emerging technologies, a Shipyard 4.0 can leverage smarter energy consumption, greater inbound/outbound logistics and information storage (asset utilization, supply/demand match, inventories, time to market), workforce safety and control (automation of knowledge work, digital performance management, human-robot collaboration, remote monitoring), and real-time yield optimization.

Navantia (Madrid, Spain) [194] is a Spanish naval company that offers integral solutions to its clients and which has the capacity required to assume responsibility over any naval program in the world, delivering fully operational vessels and support throughout the service life of the product. Its main working areas are the design and construction of hi-tech military and civil vessels, the design and manufacturing of control and combat systems, overhauls and alterations of military and civil vessels, diesel engine

manufacturing, and turbine manufacturing. Although Navantia has developed naval programs all around the world, at a domestic scale, Navantia's main customer is the Spanish Navy (this collaboration dates back 250 years). The high level of the Spanish Navy, with a worldwide operating capacity and collaborations with the most modern navies, allows Navantia to offer value added products. Specifically, this chapter reviews the advances in one of the research lines of the Joint Research Unit Navantia-UDC (University of A Coruña).

Pipes are a key part of ships: a regular ship contains between 15,000 and 40,000 pipes, whose use goes from fuel transportation or coolant for engines, to carry drinking water or waste. With such a huge number and varied typology, it is important to maintain the traceability and status of the pipes, what speeds up their maintenance procedures, accelerates locating them, and allows for obtaining easily their characteristics when building and installing them.

Figure 6.1: Navantia's pipe workshop in Ferrol (Galicia, Spain).

This need for controlling and monitoring pipes can be approached by Cyber-Physical Systems (CPSs). A smart pipe system is a novel example of the benefits of CPS, providing a reliable remote monitoring platform to leverage environment, safety, strategic and economic benefits. While the physical plane focuses on the designs for sensing, data-retrieving, event-handling, communication and coverage problems, the cyber plane focuses on the development of cross-layered and cross-domain intelligence from multiple environments and the interactions between the virtual and the physical world.

Today, the pipe management process varies depending on the shipyard but, in general, it is performed in three different scenarios: the pipe workshop where they are built, the block outfitting and the ship, where assembly takes place. This chapter focuses on

the pipe workshop presented in Figure 6.1, which is handled in a similar way in most shipyards. In this scenario, the way that pipes are currently built can be significantly improved and optimized. In this chapter, a system of smart pipes that avoids paperwork and automates pipe identification, tracking, and traceability control is proposed. The system consists of a network of beacons that continuously collects information about the location of the pipes. Such information is provided by RFID tags that also contain information that allows operators to identify each pipe and determine how to process it at every stage.

The present chapter is aimed at applying the latest research and the best technologies to build a smart pipe system for a shipyard, but it also includes the following five novel contributions. First, it presents the concept of Shipyard 4.0. Second, it describes in detail how a shipyard pipe workshop works and what are the requirements for building a smart pipe system. Third, it is indicated how to build a positioning system from scratch in an environment as harsh in terms of communications as a shipyard. Furthermore, it was not found in the literature any practical analysis on the application of RFID technology in any similar application and scenario. Fourth, the concept of smart pipe is defined and an example of its implementation and the architecture that supports it is shown. Finally, the chapter proposes the use of spatial diversity techniques to stabilize Received Signal Strength (RSS) values, a kind of technique whose application in RFID systems has not been found previously in the literature.

This chapter is based on the following publication [195–197] and is organized as follows. Section 6.2 describes the process of pipe manufacturing in a modern shipyard and analyzes the technologies that can be used for identifying pipes. Section 6.3 details the system design, including the operational and hardware requirements, and the communications architecture. Section 6.4 reviews the system modules and the RSS stabilization techniques proposed. Section 6.5 describes the experimental setup and the tests performed with the technologies selected. Finally, Section 6.6 is devoted to the conclusions.

6.1.1 Pipe manufacturing in a modern shipyard

The floor map of the pipe workshop that Navantia owns in Ferrol (Galicia, Spain) is represented in Figure 6.2. The areas colored represent the main operative areas, while in white are offices and other secondary auxiliary areas. The following are the most relevant areas:

- Pipe reception. In this area raw pipes are stacked by the suppliers. It is divided into two different areas: small pipes are stored in a robotic storage, while large pipes are placed on the floor on diverse spots.

- Cutting. This is where pipes are cut according to the engineering requirements.
- Bending. Some pipes need to be bent to adapt them to the characteristics of the place where they will be installed on the ship.

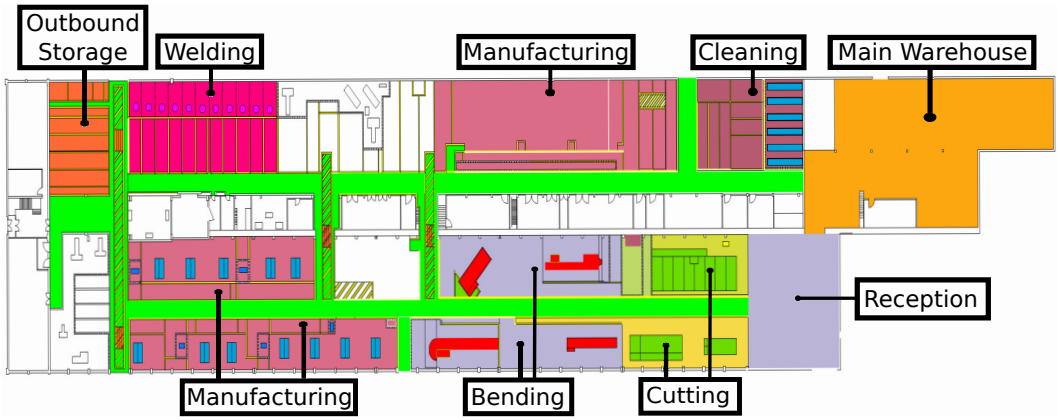


Figure 6.2: Floor map of the workshop.

- Manufacturing. These are actually three areas of the workshop where operators add accessories and where pipes made of multiple sub-pipes are joined.
- Provider's outbound storage. The outbound storage area is where providers collect the pipes and return them after their processing. In times of excessive production load, some work is derived to external providers.
- Welding. There are different booths where operators carry out welding tasks.
- Cleaning. Before manufacturing, pipes have to be cleaned. This area contains bathtubs to expose pipes to hot water, acids, or pressurized water.
- Main warehouse. This is where accessories and tool supplies are stored.

Figure 6.3: Stacking area for large pipes (left) and cutting area of the workshop (right).

The current procedure for managing the pipes consists of the following steps:

Figure 6.4: External storage area in the dock.

1. Initially, pipes are placed in a storage area, where they will be collected by operators according to production needs. In the case of the shipyard that Navantia owns in Ferrol, two zones can be distinguished: one for small pipes and another for the large ones. The area for small pipes is an intelligent warehouse where an operator registers the pipes that arrive and then extracts them on demand according to the characteristics specified. Figure 6.3 (left) shows the stacking area for large pipes, whose occupancy level is not determined automatically.

2. The first pipe processing point is the cutting area (in Figure 6.3, right). In production, as soon as the first cut of a pipe is made, operators place a plastic label that is attached using electric cable (this kind of cable is used because it has to resist being exposed to acids and hot water). This label contains alphanumeric identification information and includes a barcode. Pipes are stacked on pallets, which allows for moving them easily between the different stages of the production chain. Regarding such pallets, it is important to note that:

   - Operators distinguish visually each pallet through an identifier painted on it.
   - Pallets are moved by cranes through the workshop. They are not usually moved until they are considered to be full. When a pallet is moved to a new section, pipes are checked by operators who, by reading the label barcode with a scanner, get information on the process that should be carried out on the pipe. At the same time, the barcode reading operation allows for registering its location, since every scanner is associated with a specific place.

- Each pallet carries paper documentation related to the pipes contained.

3. The second stage of the pipes is bending (if required). There are three benders in the workshop, which can be controlled from a Windows-based PC that is also able to receive and load design files from the engineering department.

4. Before manufacturing, pipes might need to be cleaned. For such a purpose, there is an area for degreasing and rinsing pipes by using water or certain acids.

5. Next, pipes are moved to the manufacturing area, where accessories are added. These elements are transported in metal pallets from the workshop warehouse. There is not a quick communication between the warehouse and manufacturing to indicate when the accessories associated with a pipe are available (i.e., operators have to walk to the warehouse and check the availability of the accessories).

6. After manufacturing, pipes are packed with others on pallets. This packaging is registered before the pallet leaves the manufacturing area.

7. Large pipes can be stored temporarily in a reserved area located at one end of the workshop. Although there are more stacking areas, both indoors and outdoors, there is no real-time control of the occupancy percentage of the areas (i.e., the number of pipes in them).

8. Next to the temporary storage, there is an area of welding stations with plastic separations and other auxiliary areas, mainly dedicated to store pipes.

9. Once the pallet leaves the production area, the traceability of the pipes is lost, and there are no records of their movements and/or location in the different storage areas. The largest storage area is outdoors, next to the workshop, in a nearby dock (as shown in Figure 6.4).

6.2 Related Work

This section reviews the identification, tracking and location systems for shipyards and smart manufacturing and study available technologies for identifying pipes.

6.2.1 Identification, tracking and location systems for shipyards and smart manufacturing

In recent years, several authors have studied and proposed various alternatives that address tasks in ship construction, including hull blasting [198] and welding [199–201],

that can be improved through the application of technological solutions. For example, Kim et al. [202] propose an automated welding machine for shipyards, in which mobile robots use neural networks to recognize the work environment. Similarly, the same authors propose the use of smart robots for welding in a shipyard [203], but in this case they design a display system for the recognition of the areas to be welded.

The problem of locating people in a shipyard has been studied by Kawakubo et al. in [204]. In such a paper, the authors use Bluetooth technology for the location by means of fixed and mobile stations. Thus, the authors achieve a precision of 1.2 m using a fixed network of readers in which each of the readers is placed at a distance of about 8 m.

Sensor networks have also been proposed for monitoring different construction tasks [205]. For instance, a practical example of a real-time monitoring system for the concentration of CO is described in [206]. A more specific development for the construction of ships and maritime platforms in a shipyard is detailed in [207]. There, the authors describe a system of hyper-environments that use sensor networks, virtual reality and RFID to improve the process of supply tracking.

In environments where the presence of metals is high, Radio Frequency (RF) communications are clearly affected. This impact is well illustrated in [208], where a series of experiments with diverse tags showed that the signal strength decays when the tags are placed on a copper metal plate. In this regard, several techniques are analyzed in [209] to improve the performance of RFID tags on metal, showing that the length of the antenna is a variable that can improve impedance adaptation. In an environment close to the shipyard, the authors in [210] analyze the feasibility of adhering passive RFID tags on metal bent pipes.

In order to overcome harsh environments, multiple tags and components have been designed to enable RFID communications in metallic environments. Examples are [211,212] or [213], where UHF RFID tags are specifically designed to be used on various metal surfaces and containers. If conditions such as high temperatures are added to the presence of metals, RF communications are even more complicated. Therefore, components need to be adapted to harsh communications scenarios. An example is studied in [214], where the authors analyze some of the complications faced by hardware in the complicated conditions mentioned, such as data memory retention for long periods of time.

Indoor location technologies and techniques have been recently studied [215]. Fingerprinting has been attracting much attention and different RFID systems have been proposed, although there are not many for industrial highly-metallic scenarios. For instance, an example of an active UHF RFID indoor localization is presented in [216]. Another example can be found in [217], where the authors propose a novel and convex-

optimization framework fusing wireless fingerprints with mutual distance information. Other researchers [218] focused on the reorganization of the fingerprint information in the database.

Shipbuilding is a really complex process and effective process planning is critical for shipyards to compete for business in a resource and time-constrained scenario. Some research papers focused on this issue. For example, Ge et al. [219] proposed a scheduling algorithm based on heuristic rules and a genetic algorithm to solve the spatial scheduling problem of the shipyard and reduce the waste of workplace. Another approach is presented in [220], where the feasibility of applying Supervisory Control Theory (SCT) to production planning and logistics is analyzed. Production plans under a lean shipbuilding mode are presented in the literature, with examples like stochastic discrete event simulation models to estimate the production capacity of each facility. Examples of simulation tools are illustrated in [221] focused on ship construction, on the definition of the manufacturing process and on the resources needed. Resource optimization techniques and models of shipbuilding supply chain networks are also detailed in the literature.

With respect to CPS, just few examples can be found for shipyard environments. For instance, Santos et al. [222] focus on a CPS platform and describe a case study of truck tracking in a shipyard. Choi et al. [223] use a PLC system to monitor and control utilities and facilities such as a boiler, an absorption chiller system or a gas control system, in the shipbuilding area. With the same aim, Kaminski et al. [224] proposed a web-based Geographical Information Systems (GIS) dedicated to marine environment surveillance and monitoring. After studying the state-of-the-art, it was not found any development that specifically addressed pipe monitoring in a shipyard or proposed a similar system like the one presented in this paper.

6.2.2 Technologies for identifying pipes

This subsection analyzes different technologies to perform pipe identification and monitoring in a workshop. Only the most relevant tag-based identification technologies are cited but other approaches (e.g., dead reckoning or image-based technologies) are available. The technologies selected are described briefly to indicate their general characteristics, before being analyzed and compared. A summary of the basic characteristics of the technologies is shown in Table 6.1.

Navantia's current pipe monitoring system is based on barcodes which represent a set of parallel lines of different thickness and spacing that, as a whole, contain certain information. Barcode readers are devices that translate optical impulses into electrical signals, so it is essential to place the code so good visibility and readability be achieved.

Table 6.1: Main characteristics of the identification technologies selected.

Technology	Frequency band	Range	Features	Popular Applications
Barcode/QR	-	< 4 m	LOS, very low cost, visual decoding	Asset tracking and marketing
LF RFID	30-300 KHz (125 KHz)	1-5 cm (< 10 cm)	N-LOS, durability, low cost	Smart Industry and security access
HF RFID	3-30 MHz (13.56 MHz)	30 cm (< 1 m)	N-LOS, durability, low cost	Smart Industry and asset tracking
UHF RFID	30 MHz-3 GHz	10 m	N-LOS, durability, low cost	Smart Industry and toll roads
NFC	13.56 MHz	4-10 cm (< 20 cm)	Low cost, no power	Ticketing and payments
BLE	2.4 GHz	< 50 m	Low power	Wireless headsets
Wi-Fi	2.4-5 GHz	< 100 m	High-speed, ubiquity	LAN, internet access, broadband
Infrared (IrDA)	800 to 1000 μm	< 1 m	Security, high-speed	Remote control, data transfer
UWB	3.1 to 10.6 GHz	< 10 m	Low power, high-speed data	Radar, video streaming
Ultrasound	>20 kHz (2-10 MHz)	<3 m	Inspection of industrial materials	Medicine, positioning and location
ZigBee	868 MHz (EU), 2.4 GHz	< 10 m	Mesh network	Smart Home and Industry
DASH7	315-915 MHz	<5 Km	BLAST network technology	Smart industry and military
ANT+	2.4 GHz	< 10 m	Low power	Health, sport monitoring
Z-Wave	868 MHz (EU)	< 30 m	Simple protocol	Smart Home
WirelessHART	2.4 GHz	< 10 m	HART protocol	Smart Industry
LoRa	2.4 GHz	> 15 m	Long battery life and range	Smart city, M2M
SigFox	868 MHz	3-50 km	Global cellular	Internet of Things, M2M
RuBee	131 KHz	1-30 m (15 m)	Harsh environments	Mission-critical scenarios

The usual reading distance is tens of centimeters, although there is specialized equipment that can reach several meters.

There are two types of barcodes: linear and two-dimensional codes. Linear codes represent alphanumeric information (e.g., Code 39, Code 93) or numbers European Article Number (EAN). Two-dimensional codes are able to encode more information per unit of area than linear codes. An example of two-dimensional codes are Quick Response (QR) codes, which were originally designed for the Japanese automotive industry. The code consists of black squares distributed through a grid with white background that can be read by an optical device. Large boxes at the corners allow to detect the code position, having a fourth one for the alignment and orientation.

QR code reading distance depends on the size of the code: increased distances are obtained thanks to increasing QR code size in proportion. It is usually assumed that code size has to be one tenth of the reading distance (for instance, if a code has to be read at about 20 m, it should have a size of at least 2 m). Regarding the storage capacity of a QR code, it depends on the type of data encoded, the version and the error correction level.

Besides the automotive industry, it is easy to find nowadays QR codes applied in other fields. For example, a QR code traceability system for mitigating food supply chain risks is described in [225].

As we previously introduced in Chapter 3, another identification technology that has experienced a huge growth over the last years is RFID. Such a technology consists of readers and electronic tags (also called transponders). These tags are very low power components that react to waves emitted by radio readers by providing the stored information. RFID systems are usually classified according to two characteristics: their frequency of operation and the way they are powered. Depending on the frequency,

RFID systems may be classified in radio bands. Each band differs from the others in its propagation behavior and spectrum regulations.

As also mentioned, RFID has been used previously for identifying and tracking items in different industries. For instance, an example of a RFID-enabled real-time manufacturing execution system is presented in [226]. The authors there describe devices that are deployed systematically to track manufacturing objects and that collect real-time production data. The paper also details a case study with a company that manufactures large-scale and heavy-duty machinery, whose efficiency (planning and scheduling decisions) is evaluated with real-life industrial data. Other applications of RFID include tracking protective equipment [227] or appliances [228].

Near-Field Communication (NFC) is a technology that evolves from RFID. NFC devices can be passive (tags) or active (for example, smartphones). The technology operates at 13.56 MHz, with a power that allows for the communication between elements at a distance of less than 20 cm. Different authors have studied the use of NFC for identification and positioning. A good example is described in [229] where it is proposed a navigation system for identifying and tracking tags indoors when there are no GPS signals available.

Bluetooth Low Energy (BLE), also known as Bluetooth Smart, is a Wireless Personal Area Network (WPAN) technology oriented to short-range applications (around 10 m) and small devices that is optimized for energy efficiency. It works at 2.4 GHz, sharing the frequency band with other technologies like Wi-Fi. Bluetooth is not designed for a particular application: it defines a series of profiles representing a default solution for a particular use and establishes the requirements for interoperation between devices. Each Bluetooth device can support one or more of these profiles, being the most common the ones that establish links between devices and send data between them. Such devices include beacons (devices that broadcast certain information periodically) which serve as a reference in an indoor location scenario. An example of the use of beacons for tracking is detailed in [230]. The authors describe a real-time simulator using workers' position data to support manager's decision making in a manufacturing system. In such a system, BLE beacons are used to collect data easily in an experimental manufacturing line.

Similarly to Bluetooth, Wi-Fi (IEEE 802.11 a/b/g/n/ac) is also a widespread and popular technology. It may work at 2.4 GHz or/and 5 GHz. Due to its popularity, many researchers have studied its use for providing location and tracking services. There are several techniques for indoor location over Wi-Fi which are based, in general, in determining the position of the clients with respect to the access points using the angle or the time of arrival of the signals [231], the RSSI (Received Signal Strength Indicator) [206] or fingerprinting [215].

Another well-known technology is infrared communications. Infrared radiation is a form of electromagnetic and thermal radiation of a frequency lower than the visible light perceived by the human eye. Infrared sensors are opto-electronic devices capable of measuring the radiation of the bodies found in their field of view (it requires direct LOS (Line-of-Sight) between the reader and the object). An example of a system that uses infrared for tracking is described in [232], where a sensing device that can simultaneously monitor urban flash floods and traffic congestion is presented.

Ultrasounds have also been used extensively for positioning and tracking. As its name implies, ultrasounds are sound (mechanical) waves whose frequency is above the threshold of human hearing. Ultrasonic sensors are devices capable of converting sound signals to electrical signals. These devices operate like radar or sonar, evaluating the echo produced by the waves to estimate the distance between the reader and objects. A good overview of indoor ultrasonic positioning systems can be found in [233].

One of the latest technologies that can be applied to identification is UWB. UWB is a short range radio technology that allows for the transmission of large amounts of information over a wide spectrum of frequencies, achieving a very low power density and very short duration pulses. A detailed review of UWB indoor positioning systems and algorithms is provided in [234].

ZigBee can be also used in positioning and tracking applications. ZigBee is a technology for creating low-power and low-cost wireless sensor networks. It is able to create mesh networks of intermediate devices that allow for achieving large coverage distances. All ZigBee devices are designed for low consumption and high security (encryption). ZigBee transmission rate depends on the operating frequency which may differ among regions, varying between 20 kbits/s and 250 kbits/s. An example of the use of ZigBee in smart manufacturing is provided in [235]. The authors there describe a system that uses RFID devices as data collectors and a ZigBee wireless network to transmit the data to the different levels of the enterprise management.

DASH7 is a standard evolved from RFID that provides long range wireless communications and is designed for low power applications that require low bandwidth (up to 200 kbits/s). It works at frequencies between 315 MHz and 915 MHz, and allows for the connection with objects on the move. In the literature, there are not many well-documented DASH7-based developments. An exception is [236], where the DASH7 Alliance Protocol v1.0 specification is analyzed and two practical applications are detailed: bird tracking and a greenhouse monitoring application.

ANT+ is a subsystem of the ANT base protocol (a technology designed for wireless sensor networks, similar to BLE but oriented to the use with sensors) that defines a protocol stack that allows for the operation in the 2.4 GHz band. It is designed for interoperability and data transfer over a network. Most ANT+ developments are

related to fitness and healthcare. An example is detailed in [237], where mobile health monitoring systems in elderly patients is studied. Such a paper proposes a proof of concept solution that allows patients to measure their weight and blood pressure with ANT+ sensors connected to their Android smartphones.

Z-Wave is a specification for wireless communications oriented to home automation. Its aim is to minimize the devices consumption to make the use of batteries suitable, reaching transmission speeds of up to 100 kbits/s. It works in the frequency rage around 900 MHz and has a theoretical range (in open space) of up to 100 m. Z-Wave creates a mesh infrastructure with at least one controller and an end device. No academic sources that propose a Z-Wave based system for identification or tracking were found.

WirelessHART is a wireless technology based on HART (Highway Addressable Remote Transducer Protocol). HART is the implementation of a protocol of industrial automation. This wireless technology works in the 2.4 GHz band, creating networks through a mesh architecture capable of self-organization. An example of the use of WirelessHART in a CPS system can be found in [238], where a system simulator to evaluate the performance of wireless real-time mesh networks is presented.

LoRa (Long-Range Wide Area Network) is a low consumption wireless network protocol designed for secure and low cost communications in the field of Internet of Things (IoT). It uses a frequency range just below 1 GHz, being designed to communicate sensors in unfavorable environments. It uses a star topology where a device (gateway) forwards messages between end devices. The connection with these devices in terms of frequency is negotiated according to the distance and the message length, so as not to interfere with each other. Thus, transmission speeds between 0.3 kbits/s and 50 kbits/s are achieved. A comprehensive analysis of the LoRa performance is analyzed in [239].

Another long-range technology is SigFox, which is actually a telecommunications network that follows the style of cellular networks. It is designed to provide low cost and low speed transmissions. Being a network operated by a company, a subscription must be paid for its service that allows up to 140 messages per device per day, 12 Bytes per message and a transmission rate of 100 bits/s at 868 MHz. In [240] it can be found a good reference for understanding the insights on the application of SigFox in industrial applications.

Finally, RuBee (IEEE 1902.1) is a point-to-point wireless communication standard based on magnetic waves. It works in low frequencies (131 KHz), what implies that it has a long wavelength (around 2000 m) and a low transmission speed (1200 baud). Its main feature is that it does not use radio waves but it emits magnetic waves, allowing for the communication in unfavorable environments (with the constant presence of liquid, metal, and NLOS (Non-Line-of-Sight) communications). By using such a low frequency, RuBee consumes little power (a tag may last between 5 and 15 years) with

a range of up to 15 m. An example of an end-to-end asset visibility model for military logistics using RuBee is described in [241].

6.3 System design

Mission-critical infrastructures have unique operational requirements. Hence, this section details the system design, including its specific operational and hardware requirements, and its communications architecture.

6.3.1 Operational requirements of smart shipyard pipes

Based on the study of the real shipyard environment described in Section 6.1.1, different research lines have been detected to improve the efficiency in the pipe processing chain and have a significant impact on the shipyard productivity. In this section, a set of operational requirements grouped by functionality are assessed in order to cover the scenario previously described.

6.3.1.1 Automating the identification of the pipes in the workshop

Nowadays, the identification of pipes is performed manually, which means that operators have to spend part of their working time reading barcodes. This process requires direct Line-Of-Sight (LOS) between the reader and the tag, and is susceptible to reading errors. Likewise, this approach is burdensome and poses risks due to human errors (it is susceptible of not being performed or being performed at incorrect time instants). Nevertheless, operators require information on how to process pipes, thus they have to perform their identification and read the information associated with each of them. The system proposed should allow for carrying out the identification of the pipes with the smallest possible error in order to avoid manual tasks from the operators involved in the process. Additionally, the system should offer the operators dynamic information about the work to be done on the pipe.

6.3.1.2 Location of the pipes

The system currently installed in Navantia's workshop determines the location of a pipe visually or at the instants in which the quality control processes are performed by middle management. However, the remaining time the pipe is in an unknown position. This unawareness of the exact or approximate position of the pipes causes loss of time due to the seeking for pipes. The system proposed should locate in real or near-real time the pipes circulating in the workshop, not only the ones being processed, but also those that are stored. Thus, the system should trace and real-time monitor the pipes

within the workshop and the ones that left the manufacturing area. Note also that the location awareness of the pipes would help to automate different tasks like notifying an operator on the arrival of a pipe to a certain workshop stage.

6.3.1.3 Pipe tracking

The aim of pipe tracking is to find a system that identifies a pipe during the production process. Today's operation faces many demands, the pipes can be on the workshop for many years and they suffer from very aggressive processes (e.g., treatment with acids) during its manufacturing. Pipes are made of metallic materials and they are grouped on pallets in significant amounts (tens of units) which makes difficult their visual and/or electronic identification.

6.3.1.4 Optimization of the manufacturing time

It has been observed in the shipyard that the pipes manufactured in the workshop have different storage times: the oldest pipe may rust at the time of assembly, while others (most of them) show no signs of external corrosion. Knowing the real needs of demand for construction, or the available pipes and the workshop capabilities, enhances the storage times to avoid problems of stock excess (i.e., space problems) and corrosion (e.g., rust). Thus, the system should minimize part stock time and, consequently, it should decrease the likelihood of exposure to external elements.

6.3.1.5 Route optimization

Once a visualization system for locating the pipes is created, it will be possible to improve the system's capacity for providing additional recommendations thanks to the identification information and the location data collected. A good example is the optimization of routes for the transfer of pipes. For instance, given a pipe placed in the cutting area, it would be interesting to know what is the fastest route to move it to its storage spot in the dock. The ultimate goal is to optimize manufacturing and assembly times by obtaining the best routes for the transportation and final installation of the pipes.

6.3.2 Technical requirements of smart shipyard pipes

In this section, a set of technical requirements is assessed in order to cover the research lines previously discussed.

6.3.2.1 Hardware requirements

This subsection reviews the main hardware needs focusing on the tagging system and on the concerns regarding the deployment.

Tagging system

Electronic tags require a number of features to optimize their performance in aggressive environments in terms of electro-magnetic propagation and exposure to external interferences (i.e., shocks, hits, pressure, acids, high temperature liquids, among others). The following are the main constraints faced by an electronic tag-based system when operating in the shipyard scenarios previously described:

- Deployment. Tags are deployed on a workshop, where there are different areas (a detailed description of the workshop is given previously in Section 6.1). In addition, it must be emphasized that tags should be as small as possible so as not to cause problems during the treatment and handling of the pipes.
- Presence of metals. There are many metallic elements in the workshop that originate signal reflections and interfere in RF communications in the HF and higher bands. Therefore, only technologies prepared to tolerate the presence of a significant level of metallic elements should be considered.
- Presence of water. Navantia's pipe workshop is not particularly cold, but it is next to the sea, so humidity levels are relatively high (between 40% and 95%).
- Exposure to liquids, acids, salinity, fuel or other corrosive substances. The tags selected should support the degreasing, metal pickling, and rinsing processes that are carried out in the workshop during the manufacturing of the pipes. Specifically, Table 6.2 indicates examples of the exposure to different chemical solutions, temperatures and time durations that should be supported.

  Additionally, the following situations should be considered:

  - During cleaning, pipes might be exposed to pressurized water through a pressure washing machine.
  - During testing, pipes could be also exposed to hot air, water and oil (in hydraulic systems).
  - If the tags do not support the aggressive processes described in Table 6.2, the addition of an external protection has to be considered.
  - The encapsulation of tags/readers must be able to resists acids, salinity, fuel and other substances that may corrode them.

Table 6.2: Procedures for pipe cleaning.

Pipe type	Process	Solution	Temperature	Duration	Observation
Bent pipes	Degreasing	Water and T-149-E (6.25% ± 1%)	70 °C ± 10 °C	15 ± 5 min	
	Pickling	Hot water	60 °C ± 10 °C		PH: from 5 to 8
Carbon steel pipes	Degreasing	Water and T-149-E (6.25% ± 1%)	70 °C ± 10 °C	45 ± 5 min	
	Pickling	Water and DECAPINOX C (10% ± 2%)	25 °C ± 10 °C	15 ± 5 min	
	Rinsing	Hot water	60 °C ± 10 °C		PH: from 5 to 8
Cooper alloys	Degreasing	Water and T-149-E (6.25% ± 1%)	70 °C ± 10 °C	15 ± 5 min	
	Passive Pickling	Water and SCALE-GO (4.37% ± 1%)	50 °C ± 10 °C	15 ± 5 min	
	Rinsing	Hot water	60 °C ± 10 °C		PH: from 5 to 8
Stainless steel	Degreasing	Water and T-149-E (6.25% ± 1%)	70 °C ± 10 °C	15 ± 5 min	
	Passive Pickling	Water and DECAPINOX C (10% ± 2%).	25 °C ± 10 °C	15 ± 5 min	
	Rinsing	Hot water	60 °C ± 10 °C		PH: from 5 to 8

- Potential communications interference. The technology selected must be able to transmit in the presence of the most common sources of electromagnetic interference (e.g., Wi-Fi, Bluetooth, the use of mechanical saws) and other unusual sources (e.g., radar tests, whose frequency ranges from tens of MHz to GHz, and their power can reach several KW).

- Reading distances. The monitoring system must be able to provide access to location data from a remote computer. Such identification/location information must be as accurate as possible, regardless of the distance required to read the pipes/pallets to be monitored. It is important to note that the workshop is 205 m long, so a network of readers would probably need to be created to cover the whole building.

- Tolerance to high temperatures. During manufacturing, pipes can be exposed to high temperatures in two processes: while washing them in water/acids, or during welding.

- Pressure. During both the storage and the transfer of the pipes it is possible that they (and their tagging system) will be exposed to pressure due to the accumulation of weight and collisions. Pressure varies depending on the weight and strength supported by the base material. Note that, in general, between 30 and 35 pipes are moved into each pallet, and that such pallets support up to 2 T.

  The following are the most common situations where external pressures are produced:

  – When moving a pallet with other pipes on top. There is no standard criteria for stacking pipes but, usually, the heaviest are placed at the bottom of the pallet.
  – When lifting a block of the ship to its mounting position.

  - During manufacturing, it may be necessary to round heads/ends, thus strokes can be applied what involves deformations.

- Battery duration. Since pipes arrive at the workshop, up to three years may go by until they depart from the storage areas to be installed on a ship. Therefore, battery should last at least such a period of time.

- Mobility. The technological solution selected must provide portable readers for dynamic and *in-situ* operation on the various identification, location, and traceability systems.

Readers/scanners location

Readers should be located in places where there is access to both a data network and electricity. Similarly, those locations should be in places where they interfere the operator work as little as possible.

- Electricity. The typical workshop usually has numerous electrical outlets in different locations. Thus, it should not be a problem to power the hardware of the system.

- Data. Ethernet and Wi-Fi networks should be available to allow for receiving and sending data to the readers deployed. In Navantia's workshop, while these networks are available in most of the workshop, the number of Ethernet sockets, except in certain locations, is scarce and they are almost always associated to control equipment (e.g., the pipe storage robot or the bending machines). For such a reason, it is almost essential to place switches or hubs that allow for adding new Ethernet devices easily.

6.3.2.2 Software requirements

The system should include the following basic functionalities regarding user features:

- The system should display the location of the pipes in the workshop in real or near-real time. Ideally, the visualization should be implemented in a multi-platform system, which should allow for monitoring the whole workshop from a remote computer, a tablet and even a smartphone.

- Easy interaction with the basic pipe information. In addition to viewing pipes in a map, it is desirable that users can access certain information about them.

- Filtering the pipes displayed. Once the system is operating, numerous pipes would be displayed while moving through the workshop. Therefore, it is convenient that a user filters them in order to only show a specific pipe or a subset that meet certain criteria.

- The system should be able to issue different notifications about relevant events that happen in the workshop. For instance, a Business Intelligence (BI) module should issue a notification when a pipe goes from one workshop stage to another (e.g., from the cutting area to bending).

6.3.3 Selection of the identification technology

This section chooses the technology more appropriate for automating the identification and location of the pipes in the shipyard workshop. After exposing the requirements, the technologies best adapted to the application environment can be determined. A comparison that considers all the factors mentioned such as deployment, presence of metals, presence of water, exposure to liquids, acids, salinity, fuel or other corrosive substances, potential communications interference, reading distances, tolerance to high temperatures, pressure, battery duration, mobility, and cost, is shown in Table 6.3.

At the view of the table, it can be observed that some of the technologies explained in Section 6.2.2 can be directly discarded since they do not fulfill any of the significant requirements of the system. The technologies that are fully compliant with the operational and technical requirements described in Sections 6.3.1 and 6.3.2 are in green color, the ones that partially fulfill the requirements are shown in yellow, and the non-compliant ones are colored in red.

Note that, an asterisk in Table 6.3 means that custom tags are required and that they are currently on the market. For instance, high temperatures are only supported by customized tags. The practical experience of Navantia has shown that the upper peak temperature can be set at 105 °C. This temperature can be easily supported: regular electronic tags usually tolerate peaks of 125 °C, but specialized tags can reach up to 200 °C or 300 °C. The same happens with corrosive chemicals (including water) or high pressure: the tags required have to be designed to support them.

In order to choose the technology more appropriate for automating the identification and location of the pipes, first, a number of technologies were discarded following Table 6.3, since they do not properly address some of the most relevant system requirements:

- LF and HF RFID: the reading distance they reach is not enough for building a ubiquitous real-time CPS system.

Table 6.3: Comparison of the different identification technologies. Note that an asterisk means that custom tags available on the market are required. Color meaning: green (fully compliant with the operational and technical requirements), yellow (partial fulfillment), and red (non compliant).

Factor	Deployment	Metal	Water	Corrosion	Interference	Reading Dist.	Temperature	Pressure	Battery	Mobility	Cost
LF RFID				*			*	*			
HF RFID				*			*	*			
UHF RFID				*			*	*			
BLE				*			*	*			
Wi-Fi											
UWB											
Ultrasounds											
ZigBee											
DASH7				*			*	*			
Z-Wave				*							
WirelessHART											
RuBee											

- 2.4 GHz RFID: due to its operating frequency, its performance decreases in the presence of metals, liquids, or the interference from other systems that work on the same frequency band.
- BLE and Wi-Fi: these technologies share operating frequency with the 2.4 GHz RFID, so they suffer from the same problems in terms of interference.
- ZigBee, Z-Wave, and WirelessHART. These technologies are aimed at creating sensor networks: their application in location is possible but they are not suitable for the shipyard environment described in this chapter. In addition, ZigBee and WirelessHART work in the 2.4 GHz band, which must be avoided.

Next, it is possible to discard technologies that, by their nature, cannot be rejected at a first instance, but which pose risks:

- Ultrasounds. Its biggest disadvantage is the need for direct LOS between the reader and the tags. Although the frequencies used do not interfere directly with the test environment, they can interfere with sensor communications and/or armament of the ships, and even with marine animals.
- UWB. They obtain an excellent precision in location applications but it is difficult to adapt to the shipyard environment described due to its short range and its problems with the presence of metal objects.

Finally, three technologies were chosen for their theoretical characteristics and because they are suitable for the shipyard environment. These are:

- RuBee. It does not suffer from electromagnetic interference. Moreover, RuBee tags are designed to withstand adverse conditions and their battery lasts up to 15 years. It has been also tested in weapon control environments, where it was shown that its use is safe [242].
- DASH7/active UHF RFID. Both UHF RFID and DASH7 work in a frequency range to some extent sensitive to the interference present in the shipyard environment but slightly less aggressive than in the 2.4 GHz band. They have a theoretical reading distance of up to 100 m.
- UHF RFID. As already mentioned, the use of frequencies below 1 GHz decreases the influence of the environment conditions. UHF technology has the advantage of having been tested thoroughly in location and tracking applications. In addition, tags are usually inexpensive.

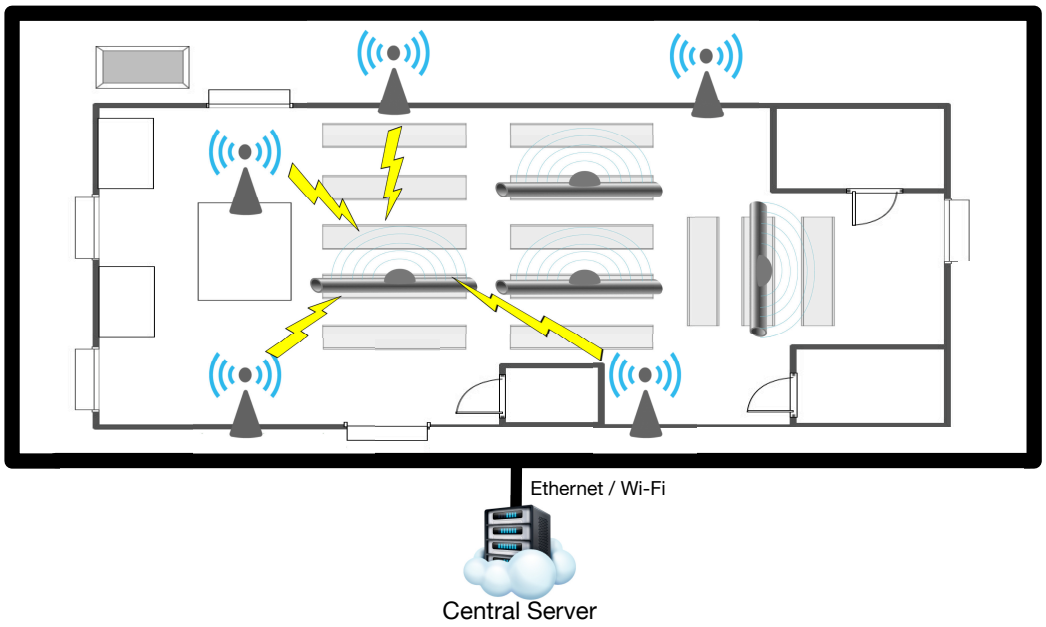


Figure 6.5: Communications architecture of the smart pipe system.

6.3.4 Communications architecture

The communications architecture proposed relies on an infrastructure of beacons that identify pipes throughout different areas. Such an architecture is illustrated in Figure 6.5. Each of the beacons reads the identifiers of the pipes/pallets and estimates its position. Contrary to the current Navantia system, it is possible to put aside the concept of pallet, allowing the system to focus only on pipes. The removal of the pallet

concept simplifies the deployment. Tags are only on the pipes, concentrating the logic of identification, location and tracking in the readers that are deployed. Therefore, a careful planning of the location infrastructure is required. It is possible to increase the accuracy of the system by scaling it, increasing its granularity (i.e., the number of readers deployed) in exchange for an increase of the economic cost.

6.4 Implementation

We concluded in the previous section that there are three technologies with high potential to carry out the identification and location of the pipes: RuBee (IEEE 1902.1), DASH7 (active UHF RFID) and passive UHF RFID. After arriving at these conclusions, various suppliers of each technology were contacted. In the case of RuBee an unexpected restriction arose: the only worldwide supplier refused to sell the hardware (as a distributor would do), because recently they had changed their business model (as of writing, they only sell completely closed projects, from design to implementation). Thus, the range of technologies reduced to active and passive RFID.

6.4.1 System modules

The system was designed assuming an RFID-based implementation and it consists of the software modules shown in Figure 6.6. Such modules perform the following tasks:

- Location module: it is the core of the system. It obtains the coordinates of each tag after processing the signal strength.
- RSS acquisition module: it is the interface with the RFID readers. It allows for obtaining the signal strength from each tag.
- RSS collection module: it is in charge of storing the signal strength values in the RSS database.
- Business Intelligence module: it decides which notifications should be shown depending on the current position of a pipe, its historical position (where it has been in the past) and the states through which it has passed.
- Display module: it displays the positions of the pipes and the relevant notifications on a user screen. It allows operators to filter the pipes based on various parameters for easy viewing.
- SAP/Manufacturing Execution System (MES) client: it allows for obtaining the data about the characteristics of the pipes, which are stored in different remote repositories.

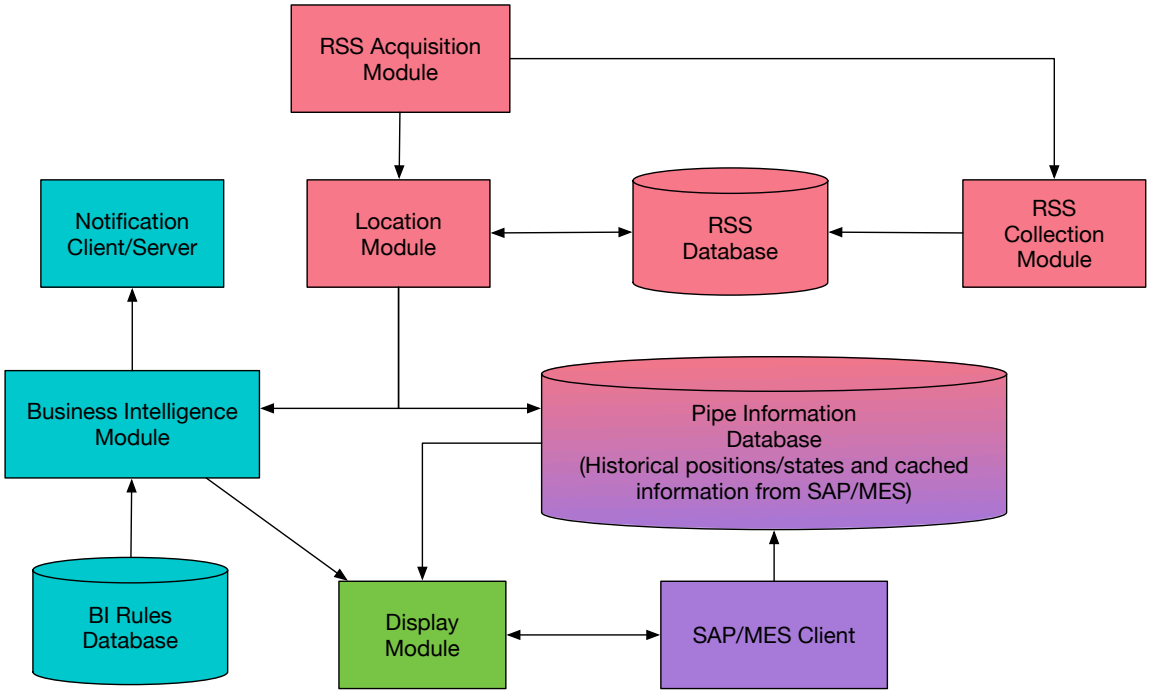


Figure 6.6: Modules of the smart pipe system proposed.

The processing and collection modules were implemented in the programming language Python. Django was used as a web framework and Nginx as a web server. The display module was implemented using websockets, Javascript, and jQuery.

There are also three databases that collect the information needed by the system (in the implementation presented in this chapter, they all are SQLite databases):

- RSS database: it stores the signal strength values collected by the RSS Collection Module. At the same time, it can be used by the real-time Location Module to determine the location of the tag.
- Pipe information database: it stores the information received about the pipes from third-party systems such as SAP or MES.
- Business intelligence rules database: it contains the necessary rules for the BI system.

6.4.2 RSS-based location techniques

This section describes the models and techniques used in the implementation of the Location module. Its experimental behavior will be analyzed in the tests performed in Section 6.5. The algorithms include modeling RSS with respect to the distance,

a Kalman filter to reduce the noise or spatial diversity techniques to increase RSS stability. Note that, in this chapter, the term RSS is used instead of Received Signal Strength Indicator (RSSI): RSS is more generic than RSSI, which is commonly used for estimating signal strength in Bluetooth and Wi-Fi devices.

6.4.2.1 RSS Mathematical Model

RSS can be used to determine the location of each tag by relating it directly to the signal propagation. However, this method depends on the variability of RSS, which is influenced by obstacles and by the presence of metallic elements. In fact, the indoors propagation of radio waves is mainly affected by two types of losses: the path loss and the losses due to small and large scale fading. Fading is usually associated with reflections, diffraction or absorption, commonly present in real environments. The small scale fading arises due to the multipath propagation effect, while large scale fading is related to the shadowing effect. From the RSS values it is possible to derive the mathematical model that allows us to relate them with the distance. The simplest approach is to average the RSS values for each distance. Another approach is based on the construction of a mathematical formula that models the system behavior. The proposed formula which closely reflects the path loss in the indoor environment is the log distance path loss model. This model can be seen as a generalization of both the free space propagation model and the two-ray ground propagation model. Thus, the behavior of the signal is simplified through the following model [243]:

$$PL(d)[dB] = PL(d_0) + 10\,n\,log(d) + X_\sigma \tag{6.1}$$

where:

- $PL(d)[dB]$ is the attenuation in decibels suffered at distance d.
- $PL(d_0)[dB]$ is the attenuation in decibels at a reference distance d_0, typically obtained through measurements.
- n is a calculated value that minimizes the Minimum-Squared Error (MSE) difference between the model and the empirical results.
- X_σ is a Gaussian variable with mean zero and standard deviation σ.

Considering the model and using the RSS as inputs, the distance d can be easily obtained with the expression:

$$d = 10^{\frac{RSS - RSS_{d_0}}{10 \times n}} \tag{6.2}$$

A second version of this model was also created to evaluate its performance in the pipe workshop. Such a version is based on RSS fingerprinting, where two main phases are distinguished: calibration and positioning.

Calibration: the objective of this stage is to set up a fingerprint database that can be used 'online' when positioning. A set of tags is deployed in specific and strategic locations, known as 'calibration spots'. In these spots, the signal level of the tags is read, processed by filtering duplicated entries (an entry is considered duplicated when a reader gets the same signal level from the same tag) and eventually stored. Such readings alone lack any kind of positioning information so a linking process between tag coordinates and signal levels has to be performed. Note that, when calibration spots are selected, their specific coordinates on the map of the factory are collected. This information, which is introduced manually into the system, and the signal levels read are connected through the tag identifier. Therefore, an assignment is made between a pair of coordinates and a set of signal levels, which is what is known as a 'fingerprint database'.

Positioning: the positioning stage starts when the system is fully launched and deployed tag readings are being received. Every RSS value collected is compared with the fingerprints stored in the database, obtaining a set of values (distances) that represent the relationship between the reading itself and the calibration information. At this point, it is possible to discard some of the calibration locations, ignoring distances lower than a threshold (the exact value of this threshold depends on the scenario). The rest of them, known as 'potential candidates', are considered as viable locations. However, not every candidate has the same potential as it depends on the distance. Therefore, a weighting process must be performed to assign weighted probabilities to every potential candidate following Equations:

$$\begin{aligned} weight_i &= \frac{\sum_{i=1}^{n}(dist_i)}{dist_i}, \\ prob_i &= \frac{weight_i}{\sum_{i=1}^{n}(weight_i)} \end{aligned} \tag{6.3}$$

where n is the total number of candidates. In this way, every reader proposes a set of potential candidates according to their likelihood. Then, the global probability for every candidate can be calculated as the product of the probabilities reported by every reader:

$$prob_i = \prod_{j=1}^{m}(prob_{i_j}) \tag{6.4}$$

where m is the number of RFID readers.

When a potential candidate presents a really high probability which implies that a reader indicates that such a candidate is almost certainly the correct location, the final probability is calculated in a slightly different way, giving more weight to higher probabilities and ignoring the lower ones:

$$prob_i = \sum_{j=1}^{m} (round(prob_{i_j})) \tag{6.5}$$

where, again, m is the number of readers. Therefore, the usual decision is carried out using a soft decision algorithm (Equation 6.4) but when there are highly-probable candidates, a hard decision is taken (Equation 6.5).

The final location is obtained from the maximum probability of the candidates. If two candidates obtain the same probability, the geometric mean between their coordinates is calculated. Additionally, there is a refining process that determines how quickly a pipe moves through the factory and filters possible positioning errors. Thus, a μ parameter conditions the updating of the pipe coordinates:

$$\begin{aligned} X_i'' &= X_i * \mu + X_i' * (1 - \mu) \\ Y_i'' &= Y_i * \mu + Y_i' * (1 - \mu) \end{aligned} \tag{6.6}$$

where (X_i, Y_i) are the current coordinates of a specific pipe, (X_i'', Y_i'') are its new ones and (X_i', Y_i') are the ones of the potential candidate selected.

To illustrate the precision of the system, Figures 6.7 and 6.8 present, respectively, the mean and the variance of the error for nine UHF active tags (Active RuggedTag-175S, read with an NPR ActiveTrack-2) positioned simultaneously in different calibration spots. It can be observed that, on average, most tags remain within a meter of error, which is really good for the test scenario. It is important to note that accuracy decreases fast when the pipes are positioned out of the calibration spots, but this can be easily solved by adding more calibration spots.

6.4.2.2 Kalman Filtering

The fundamental problem that faces the RSS indoors is the noise, which causes inaccuracies when determining the location. There are different methods to filter noise. Among them, the Kalman filter is popularly used for guidance, navigation and control of vehicles. A detailed explanation of how Kalman filtering works is out of the scope of this chapter, but the interested reader can check [244] for a detailed description of the theory behind it. For the experiments shown in Section 6.5, Kalman filtering was adapted to reduce noise on RSS, based on the work described in [245].

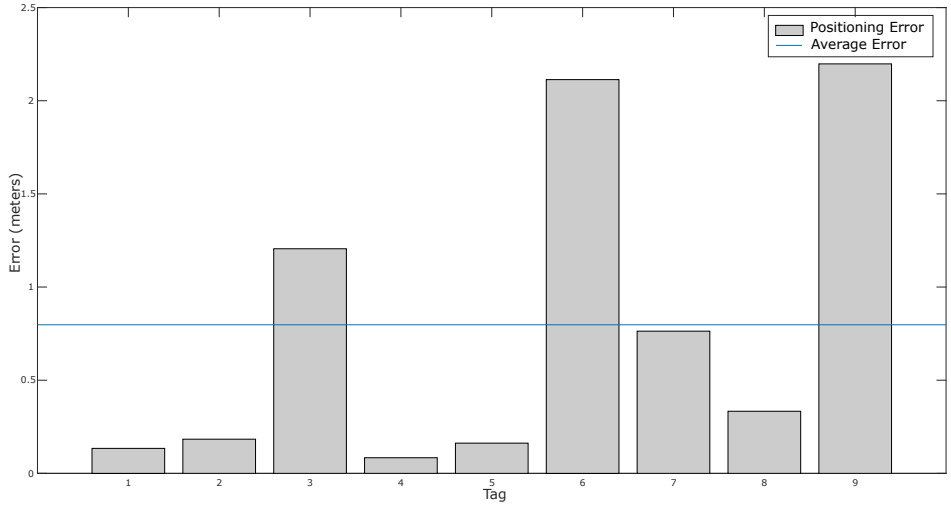


Figure 6.7: Mean positioning error for different tags.

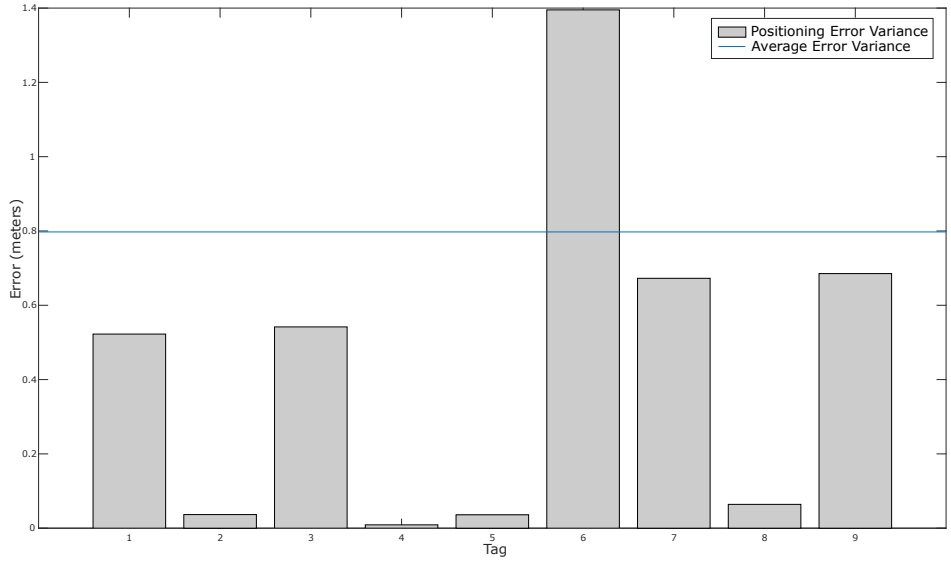


Figure 6.8: Variance of the positioning error for different tags.

First, it should be clarified that a regular Kalman filter assumes that its model is linear (there is an extended version for non-linear models) so the transition from the current state to the next state should be performed through a linear transformation. Hence, the general Kalman filter expression for a transition can be formulated as:

$$\mathbf{x}_t = \mathbf{A}_t\mathbf{x}_{t-1} + \mathbf{B}_t\mathbf{u}_t + \boldsymbol{\epsilon}_t \tag{6.7}$$

where $\mathbf{x}_t$ and $\mathbf{x}_{t-1}$ are the current and previous states, respectively, $\mathbf{A}_t$ is a transformation matrix, $\mathbf{u}_t$ is a control input, $\mathbf{B}_t$ is the control input model, and $\boldsymbol{\epsilon}_t$ is the noise.

This general expression can be simplified by assuming that pipes remain in specific places during the measurements performed. Thus, RSS is expected to be constant, having a varying contribution from the noise. Then, the control input $\mathbf{u}_t$ can be ignored and $\mathbf{A}_t$ can be assumed to be the identity matrix, what results in the following expression:

$$\mathbf{x}_t = \mathbf{x}_{t-1} + \boldsymbol{\epsilon}_t \tag{6.8}$$

Regarding the observation model, it is in general expressed as:

$$\mathbf{z}_t = \mathbf{C}_t\mathbf{x}_t + \boldsymbol{\delta}_t \tag{6.9}$$

where $\mathbf{C}_t$ is a transformation matrix and $\boldsymbol{\delta}_t$ the noise related to faulty measurements. Since RSS observations and states are equal (RSS is estimated by using old RSS values), the transformation matrix $\mathbf{C}_t$ becomes the identity matrix, so the expression ends up being as follows:

$$\mathbf{z}_t = \mathbf{x}_t + \boldsymbol{\delta}_t \tag{6.10}$$

Once transitions have been defined, the prediction step can be formulated. Such a step indicates what is expected for the next state without taking measurements into account. Since RSS is expected to be constant, the expression is simple:

$$\overline{\boldsymbol{\mu}_t} = \boldsymbol{\mu}_{t-1} \tag{6.11}$$

$$\overline{\boldsymbol{\Sigma}_t} = \boldsymbol{\Sigma}_{t-1} + \mathbf{R}_t \tag{6.12}$$

In contrast to $\mathbf{x}_t$, which is the true value, $\boldsymbol{\mu}_t$ is the value predicted. $\boldsymbol{\Sigma}_t$ is the certainty of the prediction. Such a certainty depends on the previous certainty and on the noise $\mathbf{R}_t$. In addition, the bar over $\overline{\boldsymbol{\mu}_t}$ and $\overline{\boldsymbol{\Sigma}_t}$ means that it is still needed to incorporate the information added by the measurement.

With the prediction estimate $\boldsymbol{\Sigma}_t$, it is possible to calculate the Kalman gain, which is defined as:

$$\mathbf{K}_t = \overline{\boldsymbol{\Sigma}_t}(\boldsymbol{\Sigma}_t\mathbf{Q}_t)^{-1} \tag{6.13}$$

where $\mathbf{Q}_t$ is the measurement noise. Then, the update step can be obtained, where the prediction $\boldsymbol{\mu}_t$ and the certainty $\boldsymbol{\Sigma}_t$ are calculated as:

$$\boldsymbol{\mu}_t = \overline{\boldsymbol{\mu}_t} + \mathbf{K}_t(\mathbf{z}_t - \boldsymbol{\mu}_t) \tag{6.14}$$

$$\boldsymbol{\Sigma}_t = \overline{\boldsymbol{\Sigma}_t} - \mathbf{K}_t\boldsymbol{\Sigma}_t \tag{6.15}$$

From this equation it can be observed that, the larger the Kalman gain, the bigger the influence of the measurement on the estimation. In the same way, if the Kalman gain is low, the prediction is more trusted than the measurement.

6.4.2.3 Spatial Diversity Techniques

Multiple-Input Multiple-Output (MIMO) technology offers substantial performance gains in wireless links [246]. Thanks to the use of multiple antennas for transmission and/or reception, the serious effects produced by fading on the RSS can be decreased. Likewise, it is possible to use spatial diversity to improve the stability of the mathematical model proposed thanks to the fact that there are several receiving antennas. To reduce the impairments caused in the signal by these environments, spatial diversity takes advantage of the fact that there exists a low probability of getting simultaneously a deep fading on all the signal paths. Then, assuming uncorrelated channels and using spatial diversity techniques, it is possible to combine the RSSs in such a way that the effects of fading and multipath are reduced.

These techniques are based on the classic algorithms of combination and selection, typically used in systems that increase the capacity or stabilize the signals received. Although in this chapter the same names as the ones used in the traditional algorithms are used, this is not totally precise because the implementations are adapted to the RSS parameter [247], modifying the principles of the classic schemes, which are focused on data processing.

Combination Methods

- Equal Gain Combiner (EGC). This method weights equally all the antennas, performing the average of all the RSSs according to the following equation:

$$EGC = \frac{1}{N} \sum_{i=1}^{N} \mathbf{RSS}_i \tag{6.16}$$

  where N is the number of antennas and $\mathbf{RSS}_i$ is the level of received signal for the i-th antenna. For the sake of clarity, in the curves shown in the experiments section, the term "Mean" was used instead of "EGC" but its computation is identical.

- Maximum-Ratio Combiner (MRC). Unlike EGC, this method weights each RSS depending on its signal quality. That is, it gives more weight to the most positive RSSs than to the lower ones. To carry out this computation the following expression

is used:

$$MRC = \sum_{i=1}^{N} \left\{ \frac{\mathbf{RSS}_i - \mathbf{RSS}_{min}}{\sum_{i=1}^{N} \{\mathbf{RSS}_j - \mathbf{RSS}_{min}\}} \right\} \mathbf{RSS}_i \tag{6.17}$$

where $\mathbf{RSS}_{min}$ is the smallest RSS that can be obtained.

Selection Methods

- Selection Combiner (SC). This technique consists in sorting the available measurements from higher to lower, choosing only one value. The aim of this method is to achieve the best RSS level for each instant, without considering the RSS fluctuations. In practical applications, the highest value is usually chosen, which is the criterion used in the implementation evaluated in the Experiments section.

- Switch-and-Stay Combiner (SSC). This algorithm first chooses one antenna through which the RSS is received until it falls under a preset threshold. In that moment, the algorithm switches to the next antenna without verifying its RSS. There exists the possibility of changing the threshold dynamically, but in the present chapter it is only considered the case when the threshold remains constant. It is important to emphasize that the switching between antennas is performed in a blind way, so it is not guaranteed to get a better RSS with the switching. Without a doubt, the most important issue for this method is the calibration of the optimum switching threshold. To carry out this task, the optimum threshold was decided according to an estimator of the signal dispersion. Specifically, in the experiments, the threshold was set depending on the signal variance.

- Scanner Combining (ScanC). This method is similar to SCC, but instead of making a blind switching when the threshold is exceeded, it checks each antenna until it finds one over the threshold. If there are not any antennas above the threshold, the method keeps on using the same antenna. Like with SCC, the value of the switching threshold is very important because it decides the system behavior. Besides, as in the SCC algorithm, a switching threshold that minimizes the variance was considered during the experiments.

6.5 Experiments

This section presents the results of several tests conducted to validate the technologies selected and the CPS software developed. Regarding the tests, they were performed to determine which of the two technologies selected, passive and active RFID, adapted better to the peculiarities of the environment and the characteristics of a pipe workshop.

6.5.1 Selected hardware

Based on the requirements enumerated in Sections 6.3.1 and 6.3.2, the most promising readers and tags for both technologies were selected. They are described in the next subsections.

6.5.1.1 Passive RFID Hardware

The passive UHF reader selected was a Speedway Revolution R420 from Impinj (Seattle, United States) [248]. The reader has connections for up to 4 antennas (four panel high-gain antennas were used during the tests) and the ability to exchange data via Ethernet, USB, RS-232, or a GPIO port. Reader data is accessed through its native REpresentational State Transfer (REST) API. Similarly, a mobile reader (A6-UHF Long Range) based on Windows CE was chosen to provide mobile identification to operators [249].

A wide range of tags allows for carrying out a reliable validation of the technology thanks to its diverse nature/objectives. Specifically, the following models from Omni-ID [250] were selected: Fit 400 UHF Tag on-metal, Exo UHF Tag on-metal family (Exo 600, Exo 750 and Exo 800), Dura UHF Tag family (Dura 600, Dura 1500 and Dura 3000), and Adept 360°-ID UHF Tag on-metal. Its main physical specifications can be seen in Table 6.4.

The Fit 400 is a small form factor high performance RFID tag. It is the perfect solution when space is limited but performance is demanded. With respect to the Exo family, Omni-ID Exo 600, with a small footprint, is well suited for being attached to metal bars. Omni-ID Exo 750 is designed with a broad read angle and with a global RF response. Omni-ID Exo 800 is a long range passive UHF RFID tag capable of being read on, off and near metal surfaces. Designed in a surprisingly small form factor, it features a rugged design for long term use outdoors and in industrial environments.

In the Omni-ID Dura family, Dura 600 is a small form factor RFID tag, with extreme impact resistance and superior on-metal performance. Omni-ID Dura 1500 is a durable and long range tag. Designed with heavy industry in mind, it features extreme impact resistance and high temperature ratings. Omni-ID Dura 3000 is designed for heavy industry and outdoor applications. Its features include high impact resistance, water proof and a durable case (it is optimized for tracking large assets in open storage environments, without worrying about batteries).

The Omni-ID Adept 360° is a UHF RFID tag for the toughest environmental applications. The tag is encased in an industrial steel frame with a tether attachment designed to meet the needs of heavy industry applications.

Table 6.4: Specifications of the passive Radio Frequency Identification (RFID) tags selected.

Family	Model	Max. Reading Range (m)	Dimensions (mm^3)	Weight (g)
Fit	400	4 m	13.1 × 7.1 × 3.1	380 g
Exo	600	Fixed reader: 6 m, handheld: 3 m	With holes: 80 × 15 × 12, without: 60 × 15 × 12	12 g
	750	Fixed reader: 7 m, handheld: 3.5 m	51 × 48 × 12.5	25.6 g
	800	Fixed reader: 8 m, handheld: 4 m	110 × 25 × 13	26 g
Dura	1500	Fixed reader: 15 m, handheld: 7.5 m	140 × 66 × 14	75 g
	3000	Fixed reader: 35 m, handheld: 20 m	210 × 110 × 21	265 g
	600	Fixed reader: 5 m, handheld: 2.5 m	49 × 38 × 9.5	12 g
Adept	360	10 m	136.5 × 48 × 5.5	126 g

6.5.1.2 Active RFID Hardware

The active reader chosen was NPR ActiveTrack-2 [251] that, according to the manufacturer, has a coverage radius of 45 m with standard antennas. High gain antennas were acquired to extend its coverage to about 90 m.

Different tags can be used with the chosen reader (i.e., different sizes, different features). Among all the models, the Active RuggedTag-175S [252] was chosen since it is designed to stand aggressive environments and is sonically welded (what helps to resist the effects of maritime environments). According to the manufacturer, its lithium CR2032 battery lasts more than 4 years. Its dimensions are $63.75 \times 37.72 \times 25.4\, mm^3$ and a weight of 51 g.

6.5.2 Test methodology

The tests were conducted with the readers inside Navantia's pipe workshop. These tests primarily focused on demonstrating the suitability of the tags selected for the pipe workshop and assessing the most favorable cases for determining how far RFID tags can be read in the best case scenario: if the results for the best case are not as good as expected then, obviously, the system will perform worse in more complex situations.

Two different kinds of experiments were performed. First, the maximum reading distance was obtained, taking diverse factors into account (e.g., the type of tag, the number of reading antennas, type of antennas, or the shape of the antenna array). The second kind of experiments were associated with obtaining a mathematical function that relates signal strength with distance in order to locate accurately the tags.

6.5.2.1 Physical suitability

Tests were conducted in order to ensure tag durability and resistance. The tags were exposed to the exact conditions at which pipes are subjected in the pipe workshop during their degreasing and rinsing processes. Tests were performed regarding exposure

Figure 6.9: Resistance tests in the pipe cleaning area.

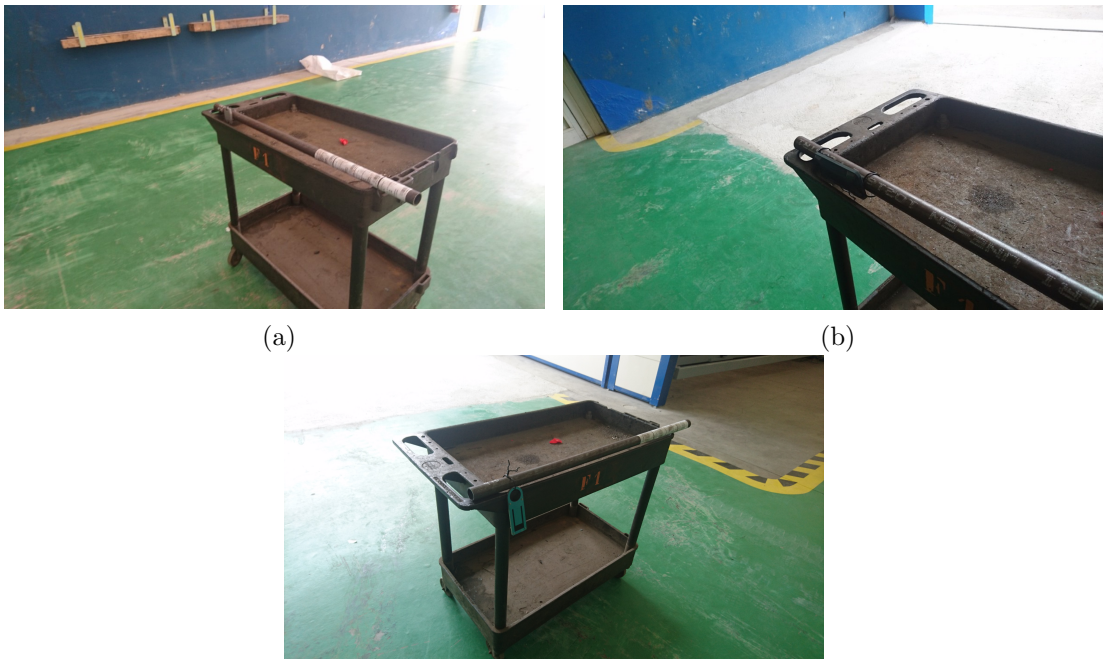
to liquids, acids, salinity, fuel or other corrosive substances, as illustrated in Figure 6.9. The tags resisted without problems the tests.

(a) (b)

Figure 6.10: Measurements with passive UHF reader with two antennas. (**a**) At 17 meters; (**b**) At 2 meters.

6.5.3 Passive RFID tests

This section reviews the main results of the passive RFID tests. As already mentioned, two different kinds of experiments were performed: ones regarding the maximum reading distance and others to obtain a mathematical function to locate accurately the tags. Specifically, the following tests focus on maximizing the reading distance, improving the antennas reading angle, modeling RSS versus distance, reducing noise using Kalman filtering and increasing RSS stability through spatial diversity techniques.



(a) (b)

(c)

Figure 6.11: An example of tags used for measurements. (**a**) Exo 750 UHF Tag; (**b**) Dura 1500 UHF Tag; (**c**) Adept 360 UHF Tag.

6.5.3.1 Maximum reading distance

These tests were conducted to determine, for each of the tags acquired, the maximum distance at which the tags can be read when they are oriented in the most favorable position (parallel to the reader antennas). Specifically, these tests were carried out in a side of the pipe workshop, taking advantage of its width (about 17 m). At one end of the workshop, the passive UHF reader was placed with their antennas, and a pipe of 31 mm diameter with the different tags adhered was placed in a wheel cart.

The layout of the different elements used in the measurements can be seen in Figures 6.10 and 6.11. In these first measurements, which focused on the determination of the maximum reading distance, only two antennas were used. When tests were performed to include spatial diversity, four antennas were used (with more antennas distributed over the reading area, it is more likely to capture the signal or some reflections). Thus, on the left of Figure 6.12 it is shown the system while capturing with an array of four antennas.

Table 6.5 shows a summary of the reading distances achieved when reading the passive tags selected at different distances through the two panel antennas. The distances at which a good percentage of the readings is achieved (i.e., when readings are obtained more than 95% of the time) are colored in green. The distances where no readings were obtained, or where a reading was achieved sporadically, are in red. Table 6.5 allows

(a) (b)

Figure 6.12: Measurements with passive UHF reader with four antennas. (**a**) Linear array; (**b**) L-shaped array.

us to conclude that Exo 800, Dura 1500, Dura 3000 and Adept 360° are the tags that can be read further. However, Dura 3000 and Adept 360° have to be excluded from the final selection for this specific application: the former is so big (210 mm × 110 mm × 21 mm) that it would hinder the operator work on the pipe, while the latter has an inadequate form factor (it is designed to be hanged).

In the rest of the chapter, for the sake of brevity, most of the curves represented will refer only to Exo 800 tags, since the conclusions drawn from the experiments are identical to the ones obtained with the Dura 1500.

6.5.3.2 Improving the antenna's reading angle

The beam of the panel antennas of the UHF system is relatively narrow on purpose in order to increase reading distance. However, in exchange, the maximum reading angle in which a tag can be read is reduced. To quantify such an angle, two antenna configurations were tested: a linear array and an 'L-shaped' array. The study of the system coverage was performed for the two tags that offered a better balance between range and physical size (i.e., Exo 800 and Dura 1500).

Table 6.5: Reading distances achieved with the different tags.

Tag \ Reading Distance	1 m	2 m	3 m	4 m	5 m	6 m	7 m	8 m	9 m	10 m	11 m	12 m	13 m	14 m	15 m	16 m	17 m
Fit 400																	
Exo 600																	
Exo 750																	
Exo 800																	
Dura 1500																	
Dura 3000																	
Dura 600																	
Adept 360°																	

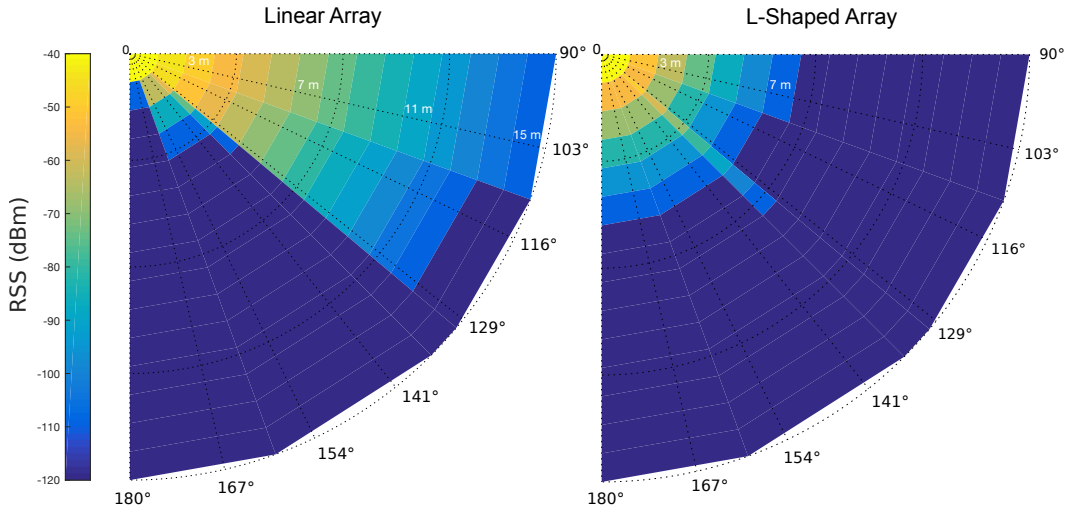


Figure 6.13: Linear versus L-shaped array coverage for Exo 800.

Figure 6.13 (left) shows the reading range for the Exo 800 tag when using the linear array. In the representation, the tag movement with respect to the array of antennas is indicated, being 90° the existing angle when facing the four antennas. The conclusions drawn are identical for both Dura 1500 and Exo 800: it can be clearly seen that, when moving the tag to obtuse angles (between 90° and 180°), reading distance decreases. Some improvement in reading may be achieved at certain distances but this is due to punctual reflections that occur in the specific location where the measurements were performed. Therefore, the Figure indicates that a configuration of antennas aligned provides a good maximum distance as long as tags are located preferably frontwards but, as the tag moves towards more obtuse angles (and similarly to more acute angles), the system loses much of its reading range. This means that the system would also work in places to control the movement of the tags through certain areas (for example, when moving from one room to another), but it would not work for a constant monitoring of all the workshop tags.

In Figure 6.13 (right), the results for the 'L-shape' array show that, in exchange for losing reading distance (because two frontal antennas are used instead of four), the reading probability at one side of the array is improved significantly.

6.5.3.3 Modeling RSS versus distance

As concluded previously, the two most promising tags are the Dura 1500 and the Exo 800 tags. Their performance was evaluated in a LOS scenario. Figure 6.14 shows the distribution of RSS (measured in dBm for this Figure and for the others presented in this chapter) with respect to the distance when evaluating the Exo 800: it can be seen how the signal levels decline as the distance to the reader increases. From these RSS

values, it is possible to look for the mathematical model that allows us to relate them with the distance between the reader and the tag. Therefore, in order to determine the location of a pipe in the workshop, a mathematical function has to be found that takes the received signal level of a tag as an input and that returns the estimated distance to the reader as an output.

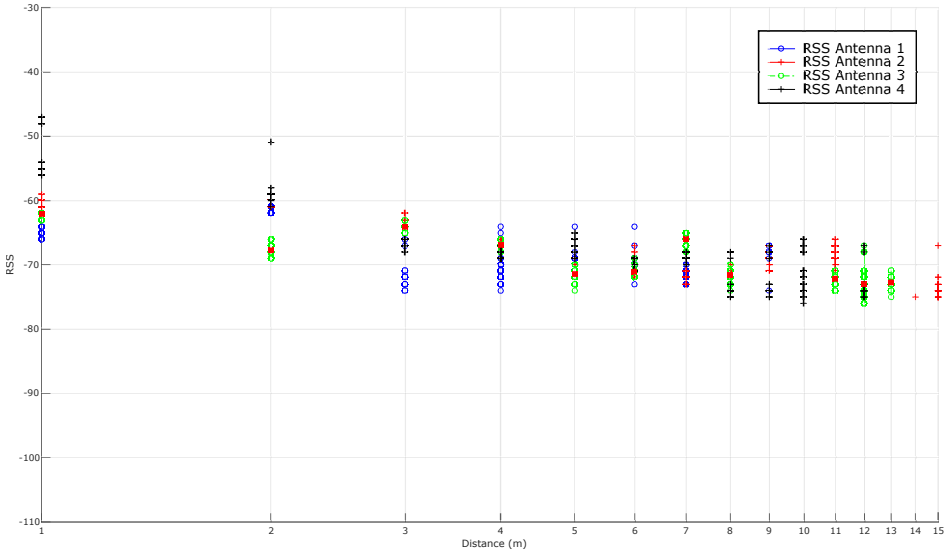


Figure 6.14: Exo 800: Received Signal Strength (RSS) for each antenna.

As explained in Section 6.4.2, there are different ways to obtain this mathematical function. The most direct way is to average the RSS for each distance, what is represented in Figure 6.15. In the same Figure, the theoretical model is also adapted to the RSS received and plotted for $PL(d_0)$ and n values equal to $-54.5\,\text{dBm}$ and 1.8638, respectively. Ideally, the RSS-based curves should follow a model to obtain a mathematical function that relates RSS to distance but it can be observed that, in practice, RSS oscillates over the distance.

Additionally, it is relevant to highlight that there are antennas at the sides of the linear array that receive no signal at different distances (for instance, in this LOS scenario, antenna 2 is the only one that receives RSSs at a distance of 14 m and 15 m).

6.5.3.4 Reducing noise: Kalman filtering

Theoretically, RSS values should only depend on the distance between a tag and the reader. However, in reality, signal strength is influenced by the environment (for instance, the reflections created by metal objects or the absorption related to the presence of water in the air) and, consequently, RSS experiences high levels of fluctuation. In order to filter it, a Kalman filter was applied as described in Section 6.4.2.2.

Figure 6.16 compares the results shown in Figure 6.15 with the ones obtained after applying Kalman filtering to each antenna. It can be seen how the filtered versions of the curves are, in general, slightly close to the theoretical model and seem to be smoother (i.e., more stable). However, at the sight of Figure 6.16, the improvement added by the filter is not obvious (it will be perceived better in the next subsection where multi-antenna techniques are also applied).

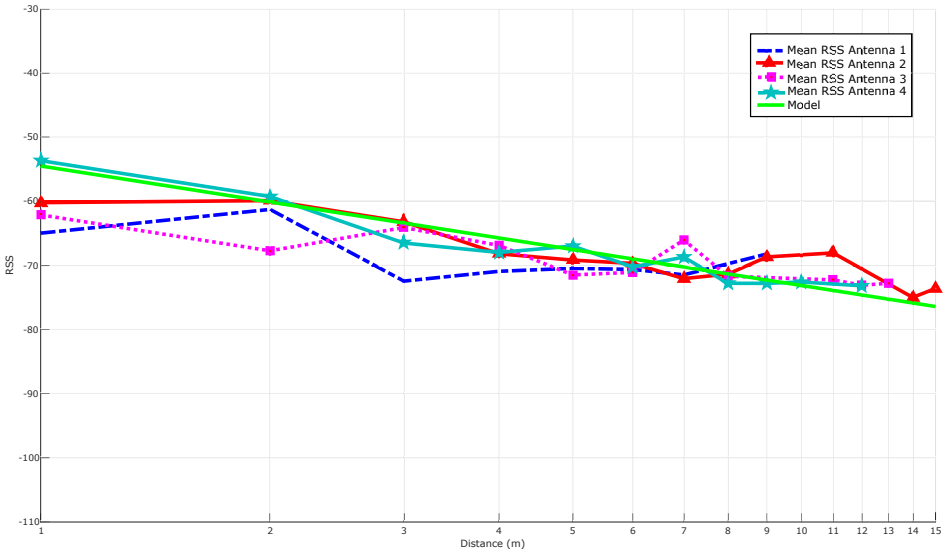


Figure 6.15: Exo 800: mean curves for each antenna and model obtained with the mean of the four antennas.

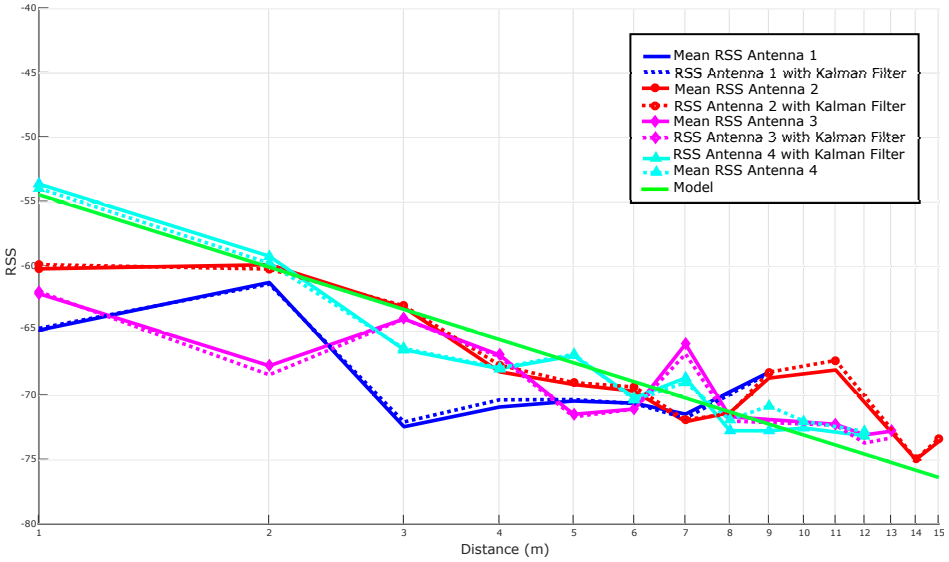


Figure 6.16: Exo 800: Comparison of the RSS curves with and without Kalman filtering.

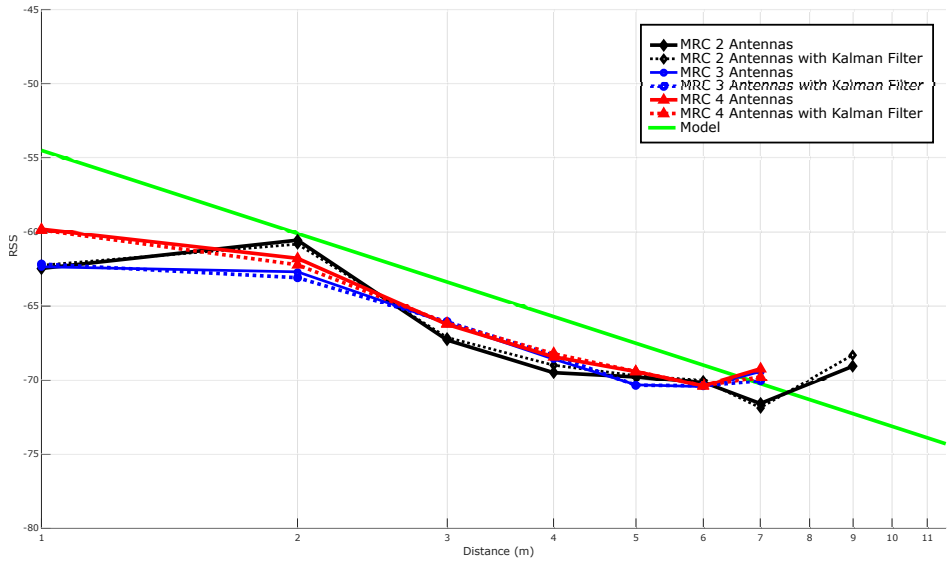


Figure 6.17: Stabilizing Exo 800 RSS with the Maximum-Ratio Combiner (MRC) technique.

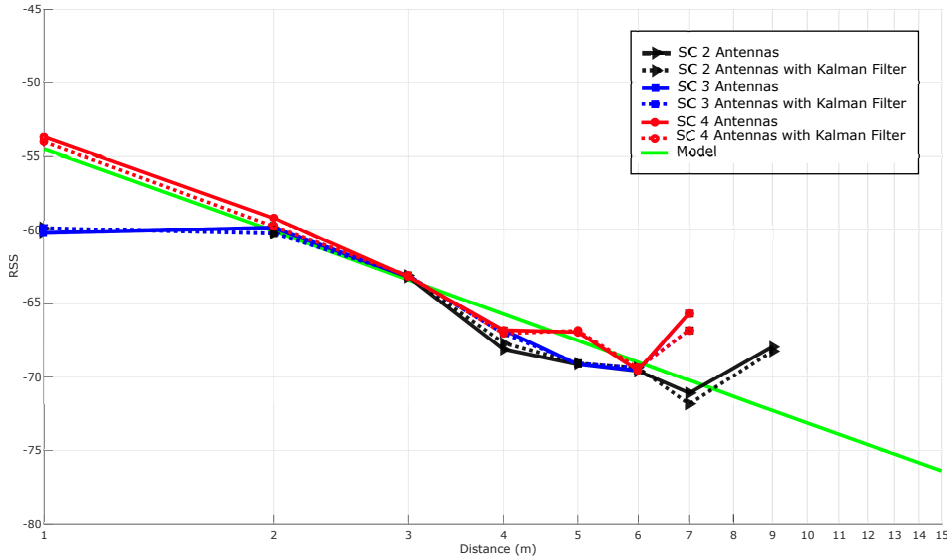


Figure 6.18: Stabilizing Exo 800 tag RSS with the Selection Combiner (SC) technique.

6.5.3.5 Increasing RSS stability through spatial diversity techniques

The techniques detailed in Section 6.4.2.3 can be applied easily to the RSS signals collected by the four antennas of the passive UHF RFID system. Figures 6.17–6.20 show the results obtained after applying MRC, SC, SSC and ScanC techniques. Note that, since there are no RSSs for some antennas at certain distances, the curves end before reaching 15 m. The Figures show that, although the multi-antenna techniques yield curves relatively smooth for low distances, they oscillate for the highest distance values. At a plain sight, it can be observed that the curves for ScanC are the ones that

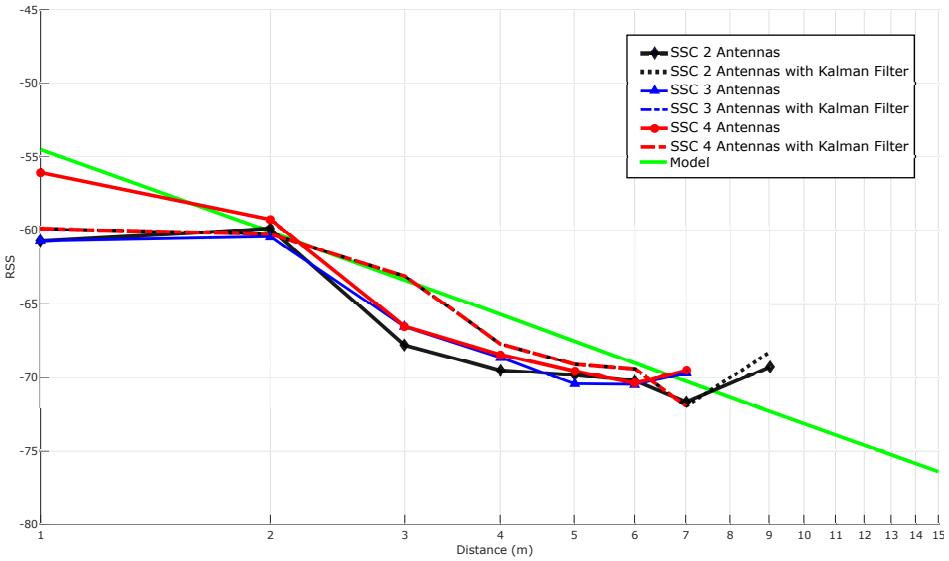


Figure 6.19: Stabilizing Exo 800 tag RSS with the Switch-and-Stay Combiner (SSC) technique.

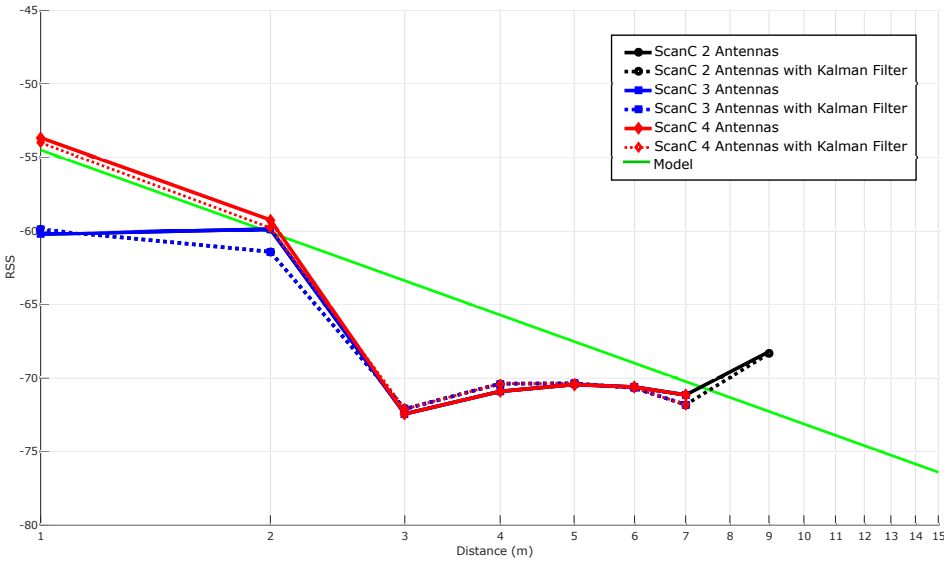


Figure 6.20: Stabilizing Exo 800 tag RSS with the ScanC technique.

oscillate the most, while the application of MRC, SC and SSC yields curves with an almost constant slope.

Regarding the results obtained for the techniques after applying the Kalman filter designed, it can be stated that the resulting RSS curves are really similar. To quantify the stability of the RSS obtained, and the level of improvement achieved thanks to filtering, the Euclidean distance of the curves obtained with respect to the curve of the theoretical model was measured. The results are shown in Figure 6.21. It can be concluded that the addition of antennas stabilizes the RSS and creates curves more

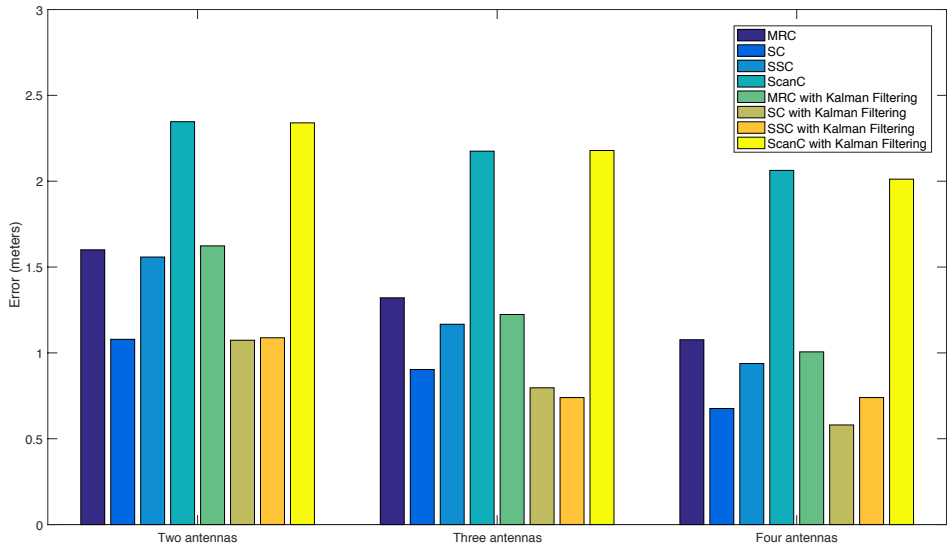


Figure 6.21: Comparison of RSS stabilization techniques applied to the Exo 800.

similar to the model. Moreover, the use of Kalman filtering, as of implemented, enhances the stability of the multi-antenna techniques applied but in some cases, the gain is small.

Table 6.6 shows the mean error of every technique when estimating the distance based on the RSS received for the Exo 800 tags. The table quantifies the improvement achieved by using Kalman filtering: except for the two-antenna MRC, the rest of techniques clearly improve their precision. Furthermore, it can be observed that the SC technique is the most accurate while ScanC is the one that obtains the worst results, with a precision of roughly 2 m.

Table 6.6: Mean error (in meters) of the different multi-antenna techniques.

#Antennas \ Technique	MRC	Filt. MRC	SC	Filt. SC	SSC	Filt. SSC	ScanC	Filt. ScanC
2	1.6006	1.6235	1.0791	1.0738	1.5583	1.0882	2.3467	2.3399
3	1.3210	1.2236	0.9034	0.7967	1.1668	0.7398	2.1751	2.1790
4	1.0769	1.0061	0.6759	0.5802	0.9381	0.7398	2.0629	2.0119

6.5.3.6 Key findings

After analyzing the results obtained indoors with LOS, it seems that the passive UHF RFID system is suitable only for situations where transitions between areas want to be controlled: due to its limited reading range, it is not useful for a ubiquitous real-time control. Moreover, such a limited range also increases hardware costs since the larger the area to cover, the more readers and antennas would be needed for the deployment.

An 'L-shaped' antenna array helps to mitigate the reduced reading angle of the system but it decreases to almost a half the reading distance. Regarding the stabilization of the RSS, the results obtained show that it is possible to reduce the system noise (and, therefore, increase the accuracy) of the system by exploiting spatial diversity and applying Kalman filtering.

6.5.4 Active RFID tests

Tests were conducted with the active reader following the same methodology as in the passive case: first, the propagation with LOS was measured, and the tags were then tested at different angles and locations throughout the workshop.

6.5.4.1 Maximum reading distance

Before performing the tests in the same way as with the passive system, the total reading range of the tag was measured: it was found that the active tag could be read 95% of the time at a distance of 100 m when using high-gain antennas. This figure is greater than the one indicated by the manufacturer in a LOS scenario (90 m) but it must be taken into account that in the pipe workshop there are many metal objects (for instance, the ceiling is metallic) what generates reflections that, in this case, favor the propagation of wireless signals.

The reading distance was next measured, like previously for the passive system, in order to carry out a fair comparison between both RFID systems (one of the moments during the measurement campaign is shown in Figure 6.22). Thus, the reader remained static at a point in this process, while a pipe placed in a wheeled cart had an Active RuggedTag-175S attached. Note that the reader can use omnidirectional and high-gain antennas, but since the latter provide more reading range, the results obtained when using them will be the only ones shown in this section.

Figure 6.22: Measurements with the active UHF reader.

6.5.4.2 Modeling RSS versus distance

Figure 6.23 shows the RSS values obtained for the active RFID system. Like in the passive system, signal levels decrease as the distance between the reader and the tag increases. It is relevant to note that between 10 and 14 m a light stabilization occurs, which is associated almost certainly to the existence of reflections from metallic elements (at that point it is where the robotic storage of small pipes is placed).

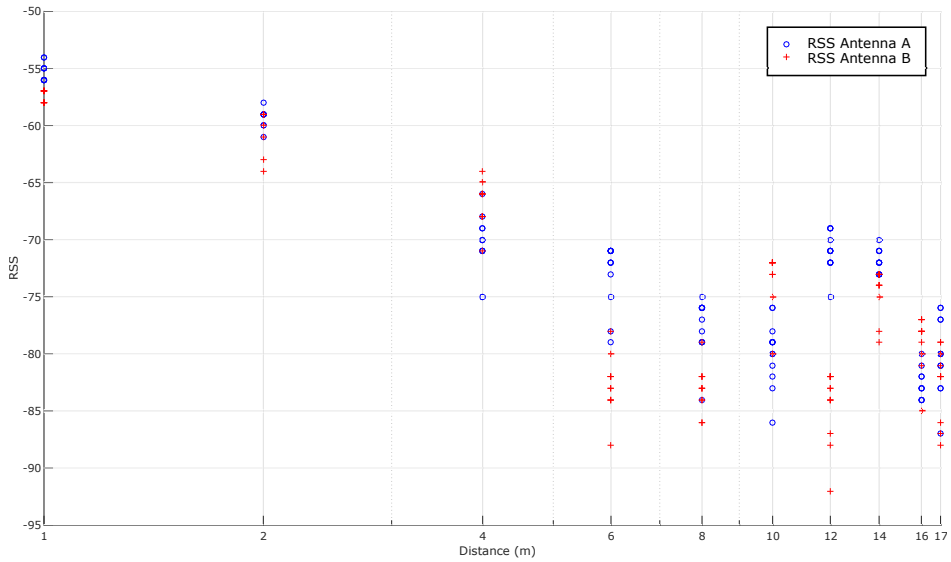


Figure 6.23: RSS values when using high-gain antennas.

The model explained in Section 6.4.2.1 can be applied (with $PL(d_0)$ equal to -56.5 dBm and n equal to 1.8261) to the RSS collected from the active reader. The curve for the model is shown in Figure 6.24 where it can be observed that, for low distance values, the mean RSS from both antennas follows the model closely but, as the distance increases, RSSs oscillate remarkably.

6.5.4.3 Reducing noise: Kalman filtering

A Kalman filter is applied to the mean RSS of each individual antenna and for the mean of both. The resulting curves are shown in Figure 6.25. Like in the passive case, it seems that the filtered RSSs generate slightly more stable curves. Nonetheless, the improvement added by the filter is observed better through the results obtained for the multi-antenna experiments described in the next subsection.

6.5.4.4 Increasing RSS stability through spatial diversity techniques

It is possible to take advantage of the spatial diversity offered by the two reader antennas to improve the stability of the RSS curves. The results obtained for the MRC, SC,

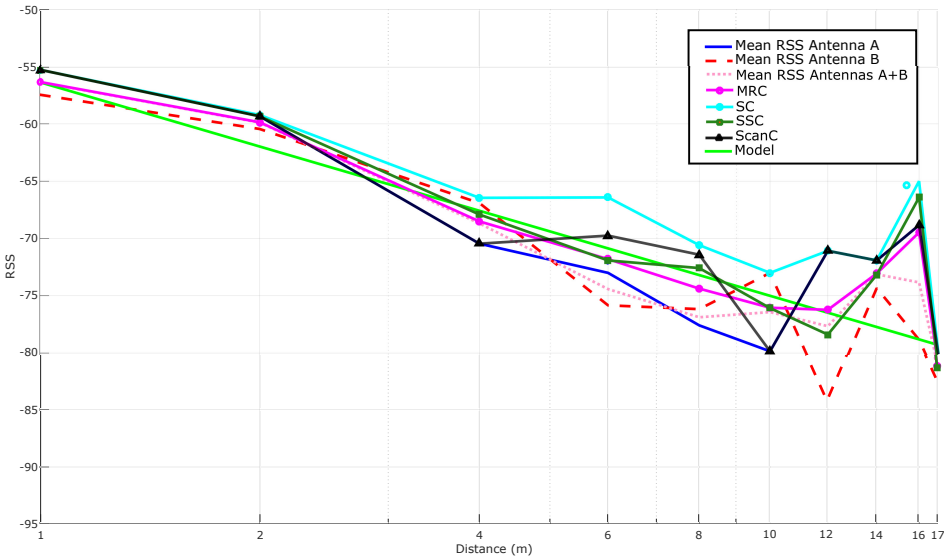


Figure 6.24: RSS means and multi-antenna techniques when using high-gain antennas.

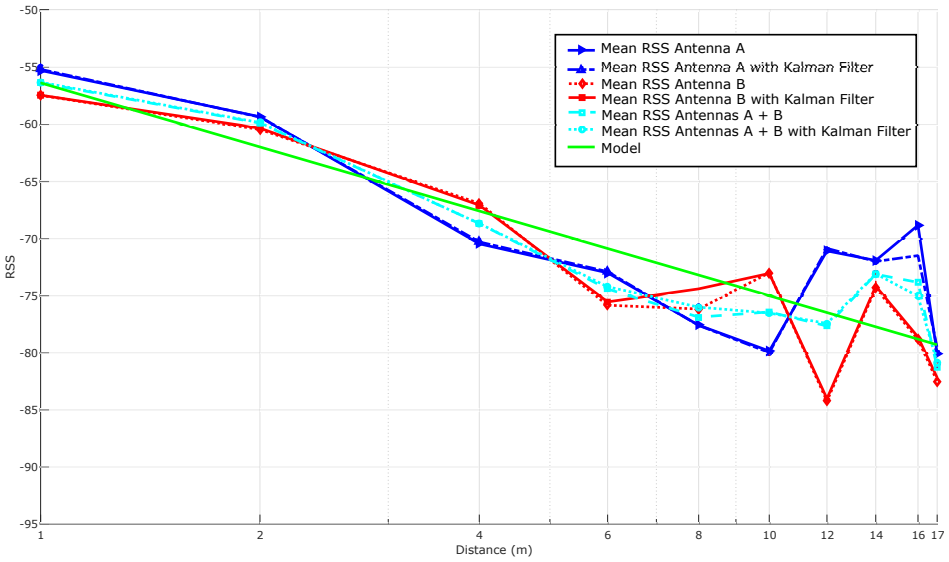


Figure 6.25: Comparison of the RSS curves when using Kalman filtering in the active system.

Table 6.7: Mean error (in meters) of the different multi-antenna techniques for the active system.

Technique / Max. Distance	MRC	Filt. MRC	SC	Filt. SC	SSC	Filt. SSC	ScanC	Filt. ScanC
10 m	0.9057	0.6212	1.6425	1.1268	1.0485	1.1008	1.0060	0.5650
16 m	3.5396	2.9744	4.8282	4.0904	3.5497	3.2720	4.0793	3.5286
17 m	3.8662	3.3645	5.3449	4.6672	3.8546	3.422	4.5838	4.1054

SSC, and ScanC techniques are also shown in Figure 6.24. Likewise, these results can be compared among them with respect to the theoretical model and when applying

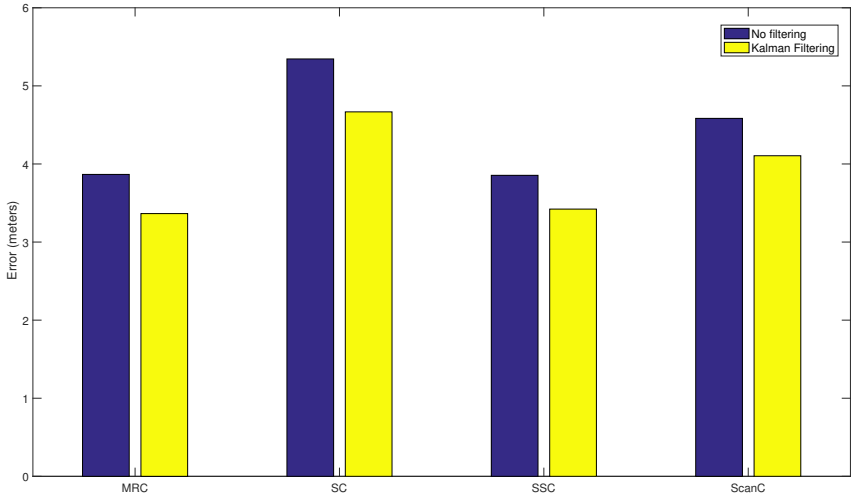


Figure 6.26: Multi-antenna technique stability with and without Kalman filtering.

Kalman filtering: as it can be concluded from Figure 6.26, MRC and SSC provide similar results and, in all cases, Kalman filtering improves the stability of the RSS.

Table 6.7 shows the mean error for every multi-antenna technique when estimating the distance based on the RSS received. The mean error is computed in the table for different reading distances in order to verify what can be observed after analyzing the RSS curves visually: for distances up to 10 m, the RSS follows closely the theoretical model, but after that distance, RSS oscillations alter the estimations, deriving into a clear loss of accuracy. Thus, the system precision up to 10 m is around 1 m, but it increases up to 3–4 m for higher distances. The table also shows the worsening of the accuracy when increasing the reading distance from 16 m to 17 m: although there is only 1 m between them, the system loses approximately 50 cm of precision. Finally, Table 6.7 allows us to conclude that Kalman filtering clearly improves the precision of the system and, among the different spatial diversity techniques, the filtered version of MRC is the most accurate technique in this specific scenario.

6.5.4.5 Key findings

The results obtained for the active RFID system while transmitting in the pipe workshop in the best case scenario (with LOS) showed that the tags offer long range readings. This means that the system is suitable for real-time monitoring in wide areas of the workshop with just one reader (what also decreases the deployment costs). However, although the accuracy of the RSS-based location system is roughly 1 m for distances up to 10 m when applying multi-antenna techniques and Kalman filtering, it increases

Table 6.8: Main features of state-of-the-art indoor positioning systems.

System	Scenario	Technology	Accuracy (Average Error)
LIPS [253]	Buildings	Wi-Fi	∼0.76 m
SDM [254]	Small building (598 m^2)	Wi-Fi	∼3 m
OIL [255]	Area with four rooms	Wi-Fi	Order of meters
EZ [256]	Small (486 m^2) and big buildings (12,600 m^2)	Wi-Fi	∼2 m (small) and 7 m (big)
WiGEM [257]	Small (600 m^2) and medium (3,250 m^2) buildings	Wi-Fi	< 8 m
WILL [258]	Medium academic buildings (1,600 m^2)	Wi-Fi	86% room level accuracy
UnLoc [259]	Different setups (largest 4,000 m^2)	Wi-Fi and inertial sensors	∼1.69 m
Zee [260]	Medium sized building (2,275 m^2)	Wi-Fi	∼3 m together with EZ or Horus.
LiFS [261]	Medium sized building (1,600 m^2)	Wi-Fi	89% room level accuracy
Walkie-Markie [262]	Medium size office (3,600 m^2) and shopping mall	Wi-Fi	∼1.65 m
RADAR [263]	Area 975 m^2, more than 50 rooms	Wi-Fi	∼3–5 m
Horus [264]	4th floor of the Computer Science building	Wi-Fi	∼3–5 m
AiRISTA Flow [265]	Asset tracking	Wi-Fi	∼1 m
IZat [266]	Automotive	Wi-Fi, GPS, 4G	∼5 m
Ubisense [267]	Smart factory	UWB	∼15 cm
Dart [268]	Manufacturing	UWB	∼30 cm
3D-LOCUS [269]	Laboratory	Ultrasound	∼8 mm
Elpas [270]	Healthcare and commercial	IR, UHF and LF RFID	∼1 m
SpotON [271]	Laboratory	Active RFID	∼3 m
Topaz [272]	Areas of ∼1000 m^2	Bluetooth+IR	2–3 m
Landmarc [273]	Laboratory	Active RFID	< 2 m
Sparse distribution [274]	Not specified	Passive RFID	< 10 cm
GPs [275]	Area of 1600 m^2 (55 rooms)	Active RFID	∼1.5 m
Robotics-based [276]	3rd floor of Duncan Hall at Rice University	Wi-Fi	∼1.5 m
MultiLoc [277]	4th floor (more than 10 rooms)	Wi-Fi	∼2.7 m
Zigbee IPS [278]	Engineering building 7.26 × 16.5 m^2	Zigbee	∼3.01 m
TIX [279]	Office (1020 m^2)	Wi-Fi	∼5.4 m
BLE fingerprinting [280]	Office (600 m^2)	BLE	< 2.6 m, high beacon density
GSM fingerprinting [281]	Large multi-floor buildings	GSM	∼5 m
NDI [282]	Industry and healthcare	Infrared (3D)	0.1 mm
IRIS_LPS [283]	Lecture hall (100 m^2)	Infrared + stereo camara	< 16 cm
Bat [284]	Building (1000 m^2), three floors	Ultrasound	3 cm
Cricket [285]	Different rooms	RF + Ultrasound	10 cm, orientation accuracy 3°
Sonitor [286]	Healthcare	Ultrasound,Wi-Fi and LF	Room level accuracy
COMPASS [287]	Office building (312 m^2)	Wi-Fi, no real-time tracking	∼1.65 m
OPT [288]	Context aware app in personal network	IEEE 802.15.4	1.5–3.8 m
Easy Living [289]	In-home and in-offices	Multiple tech	Accuracy non guaranteed
Beep [290]	Room 20 × 9 m^2: users can use their own devices	Sound source location	0.4 cm

rapidly with further distances, what indicates that it is necessary to make use of more sophisticated positioning algorithms.

The accuracy values obtained are in the same magnitude order as those found in the literature (the most relevant examples can be seen in Table 6.8). These examples can be examined as evidence of the behavior of the technologies in non-adverse environments, mainly offices and university buildings. Nevertheless, direct comparison with the behavior of the smart pipe system proposed is difficult because a coherent methodology

does not exist between the different works: various technologies, different algorithms or techniques, or distinct beacon spatial density are considered. One of the main factors that differentiate the environment presented with the ones exhibited in other publications is that the experimental conditions of our proposal, although sometimes similar regarding the scenario size, are quite adverse due to the massive presence of metals, thus facing a truly challenging deployment.

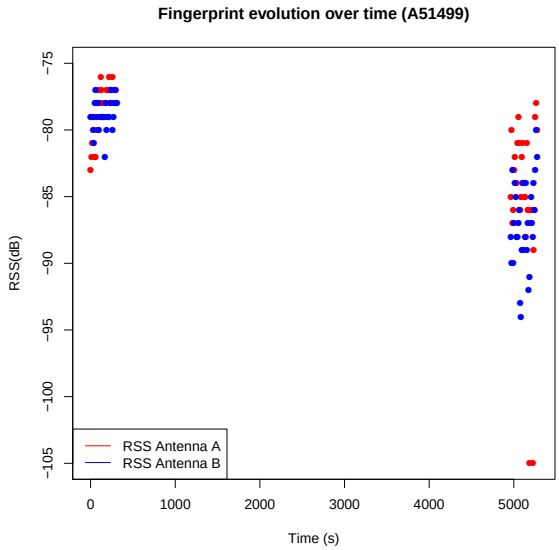


Figure 6.27: Power received on the A51499 reader for the same tag in two different time instants.

Nevertheless, fingerprinting theory is based on the fact that the RSS fingerprints collected during the calibration and positioning phases are similar but, during the tests performed in the workshop, different alterations have been observed in the signal levels that reduce the accuracy of the system:

- Reading angle of the tag: signal levels vary considerably depending on the orientation of the tag. The reason is that the tag antenna is directional so, depending on the direction, some rebounds will be caught or not. In an open space or in a regular office this effect is negligible but in the workshop, where there is a high degree of reflections, the influence of the antenna angle is remarkable.
- Antenna angle of the reader: signal levels vary noticeably between both antennas, even though they are only about 10 cm apart. Except in specific directions, the antenna that best receives is the one that is polarized just like the antenna of the tag. The diversity between antennas provides redundant information but the large differences between the different orientations of the antenna complicate the exploitation of such redundancy.

- Height: since most of the metal obstacles of the pipe workshop are below 1.5 meters, RSS differs greatly depending on the height. A specific calibration for each position to be monitored would be needed, not only in 2D, but also in 3D.

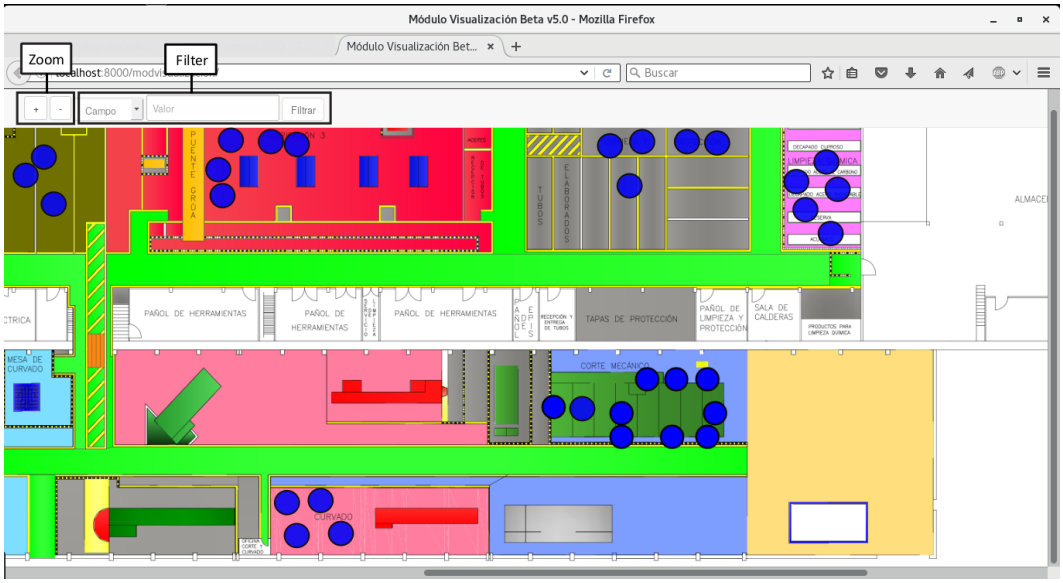


Figure 6.28: Floor map of the workshop with located pipes (blue circles).

- Multiple sources of interference: there is a continuous transit of people and metal objects that alter notably signal levels. Figure 6.27 represents the received signal levels for a reader at two time instants: the first one during calibration (time instants near 0) and the second one during the positioning phase (about 80 minutes later). The difference in the dispersion of the RSS is observed in the Figure, which are modified due to the alterations that occurred in the environment (e.g., pipe pallets were relocated). Thus, a fingerprinting system would have to adapt dynamically to the environment conditions to improve its accuracy.

- Stacking of pipes: when tags are next to pipes of significant dimensions, the observed signal levels oscillate up to 40 dB, making almost unfeasible the location using fingerprinting.

6.5.5 Display module of the smart pipe system

Once verified that constant monitoring can only be achieved with an active RFID system, additional tests were conducted for the ubiquitous real-time CPS system while transmitting in the pipe workshop. The results obtained can be seen by the operators thanks to the display module, which can be accessed through any device with a regular web browser (i.e., from PCs, Macs, smartphones and tablets). The system shows the

location of the pipes in real time in the way shown in Figure 6.28, where the blue circles represent the pipes or a set of pipes within a radius of 2 m (this is useful for pallets that carry several pipes).

Considering that numerous pipes are displayed while moving through the workshop, a filter can be used to only show a specific pipe or a subset that meets certain criteria. Moreover, operators can zoom in and out throughout the floor map to watch specific areas. Operators, in addition to viewing the pipes in a map, can access certain information about them. This functionality is illustrated in Figure 6.29 and implies obtaining data on specific parameters (i.e., pipe identifier, area or material).

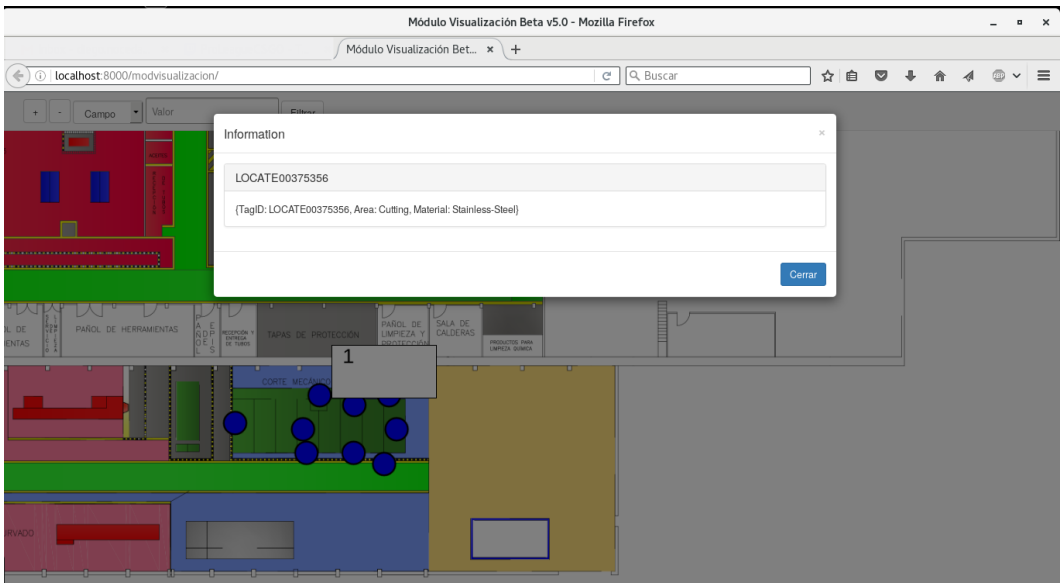


Figure 6.29: Example of the information shown to the operators about the basic characteristics of a pipe.

Accuracy can also be studied from this display module: the position oscillations of the pipes due to the RSS noise are observed. Such a noise is drastically reduced with the techniques analyzed in the previous sections and gives a really stable representation of the state of the pipe workshop in locations with LOS.

6.5.6 Automatic event detection using smart pipes

The concept of smart pipe is based on the fact that a pipe actually informs its position through its communications transceiver signal level. Such an information, when accurate, allows for implementing a wide range of very useful services. The services are provided by the business intelligence module, which processes the position information and shows meaningful notifications through the display module. Figure 6.30 illustrates an example of a smart service: when a pipe crosses from one area to another, a pop-up is shown

Figure 6.30: Notifications shown on the right upper part when a pipe crosses from one area to another.

on the upper right part of the screen indicating the event, the pipe identifier and a timestamp. This event warns the operators when a certain pipe is coming towards their work area so that they are prepared to receive it.

These notifications represent a simple but useful service. In future releases, the software will incorporate other services like the measurement of the time spent by a pipe in certain areas (to create statistics about the performance of the different areas/operators), the quantification of the level of occupation of the stacking areas, or the possibility of triggering certain automatic behaviors (for instance, through the workshop machinery and robots) when a pipe reaches certain point.

6.6 Conclusions

This chapter described the selection and validation of the necessary technology to perform improved traceability and location of the pipes used in the construction of ships. The proposed smart pipe system is a novel example of the benefits of CPS, thus providing a reliable remote monitoring platform to leverage strategic applications and enhancements in the shipyard environment. The system is based on the concept of smart pipe, a kind of pipe able to transmit signals periodically that allows for providing useful services in a shipyard. This chapter conducted a detailed analysis of the shipyard environment, the scenarios that involve pipes in their process, the operational and technical requirements, and a feasibility study to choose the best technology and communications architecture. Also, a comprehensive technology validation has been made. Through multiple tests it was confirmed that:

- The passive RFID system, due to its limited range, is only suitable for situations where the aim is to control the movement between areas, but not for ubiquitous real-time control.
- This passive system, when making use of an 'L-shaped' array of antennas, mitigates the low angle of reading, but it reduces the reading distance to almost a half.
- In the case of active RFID readers, their use allows for reaching longer distances and get constant monitoring of tags in wide areas. However, the longer the distance, the less accurate the RSS-based distance estimations are.
- Multi-antenna algorithms and Kalman filtering help to stabilize RSS and improve the accuracy of the positioning system.

Given all these factors, it is verified that active RFID is the best positioned technology for implementing the CPS proposed. Further research needs to be carried out to explore even more accurate positioning algorithms in order to minimize the influence of the interference caused by the environment.

To summarize, this chapter presented the foundations for enabling an affordable CPS for Shipyards 4.0. The system design proposed allows shipyards to collect more information about the pipes and to make better use of it. Furthermore, with this system working, the development of applications related to the monitoring of elements different than pipes (e.g., wearables for operators, tools and shared machines) is straightforward. Thus, the forthcoming applications will enable the Shipyard 4.0 to leverage smarter energy consumption, greater inbound/outbound logistics and information storage, workforce safety and control, and real-time yield optimization.

Chapter 7

Conclusions

The main purpose of this thesis is to assess the feasibility of applying emerging technologies in mission-critical scenarios around three key critical infrastructure sectors: transportation, defense and public safety, and shipbuilding. This chapter presents the main conclusions derived from this work and proposes study lines for further research.

Transportation

Chapter 2 provides an understanding of the progress of communications technologies in the railway domain since the implantation of GSM-R. It describes the motivations for the different alternatives over time and the evolution of the railway requirements with their main specifications and recommendations. The aim of this work is to envision the potential contribution of LTE to provide additional features that GSM-R could never support. Furthermore, the ability of Industrial IoT for revolutionizing the railway industry and confront today's challenges is presented, jointly with the rise of the paradigm of Internet of Trains. For instance, today main industrial developments were described, exposing the main short and medium-term IoT-enabled services for smart railways.

Chapter 3 presented a detailed review of the most common flaws found in RFID-based IoT systems, including the latest attacks described in the literature. Next, a novel methodology that eases the detection and mitigation of such flaws was presented. Besides, after analyzing the latest RFID security tools, the methodology proposed was applied through one of them (Proxmark 3) to validate it. Thus, the methodology is tested in a transportation scenario where tags are commonly used for access and payment. In such systems it is possible to extract information, to capture tag-reader communications to perform MitM attacks, and to emulate both readers and tags. Therefore, the methodology proposed shown to be useful for auditing security and reverse engineering RFID communications in transport applications.

The final remark was that, although many applications can make use of advanced security RFID measures, certain developers have adopted the technology without taking such mechanisms into account. In the case of the transportation tag analyzed, its security could be improved by adding a higher security layer (e.g., encrypting internal data), enabling some of the already existing security protocols, or simply replacing the tag with a more secure version. A methodology like the one proposed can help IoT application developers to perform audits and determine the security level of an RFID system before taking it from a test environment to a mission-critical scenario. It must be noted that, although this chapter was aimed at fostering RFID communications security in transport, the methodology can be applied to any RFID communications protocol.

Defense and public safety

The strategic advantages of 4G broadband technologies massively deployed in civil scenarios are examined in Chapter 4. The analysis performed is able to determine the technologies required in the middle and long term to comply with the operational requirements of the terrestrial army, and the state-of-the-art COTS military equipment that covers such needs. After the definition of the NATO scenarios, an analysis of the operational requirements is performed. In a second step, the technical requirements are derived and used as input for the applicability analysis of 4G Worldwide Interoperability for Microwave Access (WiMAX), Long Term Evolution (LTE) and Wi-Fi. For this work, it was necessary to characterize the technical implementation requirements of 4G standards, and analyze capabilities, aptitudes and challenges when deploying a tactical network. Also, modifications and their related techniques were identified and evaluated for the three standards in order to design a novel Military Broadband Wireless Communication Systems (MBWCS). The study confirmed that the development of an innovative MBWCS would be clearly optimized if 4G standards were taken as basis.

Chapter 5 focuses on providing a holistic approach to IoT applied to defense and public safety (PS). It presented a thorough study of the most relevant operational requirements for mission-critical operations and defense, an overview of the key challenges, and the relationship between IoT and other emerging technologies. In order to perform the study, different relevant scenarios were proposed such as: C4ISR, fire-control systems, logistics (fleet management and individual supplies), smart city operations, personal sensing, soldier healthcare and workforce training, collaborative and crowd sensing, energy management, and surveillance.

As a result of the study, it is concluded that commercial and industrial IoT still faces many challenges, such as standardization, scalability, interoperability, and security.

Researchers working on defense have to cope with additional issues posed by tactical environments, and the nature of operations and networks.

Organic transitions such as supply chain management and logistics will naturally migrate to mission-critical environments. But, beyond the earliest military IoT innovations, complex battlefields will require additional research advances to address the specific demands. In addition to addressing various technical challenges, this work identifies vital areas of further research in the 2017-2020 timeframe.

Shipbuilding industry

Chapter 6 presents the foundations for enabling an affordable CPS for Shipyards 4.0. The CPS proposed consisted of a network of beacons that continuously collects information about the location of the pipes, its design allows shipyards to have more information on the pipes and to make better use of it. Furthermore, with this system working, the development of innovative applications related to the monitoring of elements different than pipes (e.g., wearables for operators, tools, shared machines) is straightforward.

After defining the novel concept of Shipyard 4.0, the chapter described in detail how a shipyard pipe workshop works and what are the requirements for building a smart pipe system. Moreover, it indicated how to build a positioning system from scratch in an environment as harsh in terms of communications as a shipyard, showed an example of its implementation and the architecture that surrounds it. The system was designed assuming an RFID-based implementation: UHF RFID technology was the best positioned technology for implementing the CPS proposed, and through multiple tests it was confirmed that the active UHF RFID system enables constant monitoring of tags in wide areas. Furthermore, the chapter proposed the use of spatial diversity techniques and Kalman filtering to stabilize RSS values.

7.1 Future work

This thesis covered a broad suite of issues that arise from the advent of disruptive technologies. The approaches proposed have demonstrated to be sound, and it is expected that their contribution will be important over the next years since IoT, CPS, RFID, 4G/5G wireless communications, and COTS technologies applied in mission-critical scenarios are likely to continue to be a hot topic in the near future. Any of these technologies can be further investigated. Nevertheless, the following points are of special interest.

The methodology presented in Chapter 3 detected several vulnerabilities in transportation tags regarding data privacy. For this reason, we plan to perform audits and

determine the security level of other commercial RFID systems in order to bring into the attention of the authorities responsible if flaws are discovered. Moreover, this kind of tags identify nowadays elements in an increasing number of practical applications, like animal identification, healthcare, passport control, transportation, supply chain traceability, maritime freight container tracking, protective equipment verification, or toll payments.

According to the European Commission, NFC will be the preferred technology for transportation cards in the near-future, and today many smartphones currently support it. NFC is partially compatible with numerous RFID standards and it is straightforward to develop an Android application to read the data (there have already been attacks to ISO/IEC 14443-A tags using mobile phones). Thus, a future research line is to apply the methodology in a similar manner in order to detect possible attacks that threaten security, and enhance the methodology proposed to audit security and reverse engineering other communications protocols.

In Chapter 4 it was confirmed that the development of an innovative Military Broadband Wireless Communication System (MBWCS) would be clearly optimized if 4G standards are taken as basis. Once the feasibility has been confirmed, and after a cost-benefit analysis of the implementation of a 4G scenario-based MBWCS, the way-ahead would be setting up of a specific RTG for NATO IST-ET-068. This RTG shall cover two approaches. The first one will create a MBWCS easing to some extent the requirements, identifying what can be included with a positive cost-benefit trade-off, i.e., adding a crypto device. The second one will evolve the high-level assessment into the quantitative domain, thus performing a detailed design of the envisaged MBWCS, conducting exhaustive simulations and prototyping activities with the WiMAX, LTE and WLAN promising features and modules concerning the specified requirements' compliance. The conclusions obtained confirmed that today standards only imply a partial compliance of some of the requirements identified and none of them are able to comply with the full specification. Thus, 5G systems will be examined to assess the compliance of the requirements proposed in order to design a disruptive MBWCS.

Regarding the shipbuilding industry, there are several factors that affect accuracy in the real-time pipe monitoring CPS developed: the reading angle of the tag, the antenna angle of the reader, the height, or the stacking of pipes. Although some of these aspects have been commented in Chapter 6, it is necessary a more in-depth analysis.

Further research needs to be carried out to explore even more accurate positioning algorithms in order to minimize the influence of the interference caused by the environment. It would be interesting to study the relationship between the multiple sources of interference and the accuracy of the fingerprinting positioning module. In a similar

manner, there are other recent algorithms that would be really interesting to evaluate in this environment.

A future line of research might involve using the smart pipe system for providing novel services in a shipyard. For this reason, the functionality of the Business Intelligence module is planned to be increased, and devise other services like the measurement of the time spent by a pipe in certain areas (to create statistics about the performance of the different areas/operators), the quantification of the level of occupation of the stacking areas, or the possibility of triggering certain automatic behaviors (for instance, through the workshop machinery and robots) when a pipe reaches certain point. Note also that the identification and location awareness of the pipes will help to automate different tasks, like notifying an operator on the arrival of a pipe to a certain workshop stage.

Furthermore, it has been observed that the pipes manufactured in the workshop have different storage times: the oldest pipe may rust at the time of assembly, while others (most of them) show no signs of external corrosion. Knowing the real needs of demand for construction, or the available pipes and the workshop capabilities, enhances the storage times to avoid problems of excess (i.e., space problems) and corrosion (e.g., rust). Thus, a new version of the CPS will take advantage of the awareness to minimize stock time and, consequently, decrease the likelihood of exposure to external elements.

Once developed the visualization system for locating the pipes, it will be possible to improve the system's capacity for providing additional recommendations. A good example is the optimization of routes for the transfer of pipes. For instance, given a pipe placed in the cutting area, it will be interesting to know what is the fastest route to move it to its storage spot in the dock. The ultimate goal will be to optimize manufacturing and assembly times by obtaining the best routes for the transportation and final installation of the pipes.

For instance, with the CPS proposed, the development of applications related to the monitoring of elements different than pipes (e.g., wearables for operators, tools, shared machines) is straightforward. Thus, the forthcoming applications will enable the Shipyard 4.0 to leverage smarter energy consumption, greater inbound/outbound logistics and information storage, improved workforce safety and control, and real-time yield optimization.

Chapter 6 tested the CPS in the pipe workshop. Today, the pipe management process varies depending on the shipyard but, in general, it is performed in three different scenarios: the pipe workshop where they are built, and the block outfitting and the ship where assembly takes place. These two additional scenarios might be assessed. As a result, new outdoor location algorithms and maybe additional communication technologies shall be included.

In addition to the future works mentioned above, which are already in progress, there are some other lines of research that we would like to tackle. First, Chapter 2 determined medium-term IoT-enabled services for smart railways. As future work, it would be interesting to develop a CPS for this sector. The CPS will provide a reliable remote monitoring platform to leverage environment, safety, strategic and economic benefits. While the physical plane will focus on the designs for sensing, data-retrieving, event-handling, communication, and coverage problems, the cyber plane will be aimed at developing a cross-layered and cross-domain intelligence from multiple environments. In a similar manner, as we presented in Chapter 5, several proposals of novel CPSs can be implemented for defense and public safety.

Finally, new technologies, protocols, methods are constantly emerging. Consequently, recent alternatives should be studied in order to take advantage of the best technologies available for a mission-critical scenario.

Acronyms

5G	5-th Generation
3GPP	3rd Generation Partnership Project
A-GNSS	Assisted Global Navigation Satellite Systems
AAA	Authentication, Authorization, and Accounting
ACV	Armored Combat Vehicles
ADC	Analog-to-Digital Converter
AJ	Anti-Jamming
AMC	Adaptive Modulation and Coding
ARP	Allocation and Retention Priority
ARQ	Automatic Repeat Request
ASCI	Advanced Speech Call Items
BFT	Blue Force Tracking
BI	Business Intelligence
BLE	Bluetooth Low Energy
BS	Base Station
BSC	Base Station Controller
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CA	Carrier Aggregation
CBTC	Communications Based Train Control
CC	Command Center
CCBG	Critical Communication Broadband Group
CCTV	Closed-Circuit Television
CoMP	Coordinated Multi-point
COMSEC	Communications Security
COP	Common Operational Picture

COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical System
CR	Cognitive Radio
CRC	Cyclic-Redundancy Check
CSFB	Circuit Switched FallBack
CSI	Channel State Information
D2D	Device-to-device
DASH	Dynamic Adaptive Streaming over HTTP
DoD	Department of Defense
DSS	Data Distribution Subsystems
EGC	Equal Gain Combiner
EIRENE	European Integrated Railway Radio Enhanced NEtwork
eLDA	enhanced Location Dependent Addressing
eMBMS	Evolved Multimedia Broadcast Multicast Service
EMCON	Emissions Control
eMLPP	enhanced Multi-Level Precedence and Pre-emption
EPM	Electronic Protection Measures
eREC	Enhanced Railway Emergency Call
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
FEC	Forward Error Correction
FPGA	Field-Programmable Gate Array
FRS	Functional Requirements Specification
GSM-R	Global System for Mobile Communications-Railways
HAP	High-Altitude Platforms
HARQ	Hybrid Automatic Repeat Request
HCI	Human-Computer Interfaces
HF RFID	High Frequency Radio Frequency IDentification
HMI	Human-Machine Interface
IaaS	Infrastructure as a Service
IMS	IP Multimedia Subsystem
INFOSEC	Information Security
IoT	Internet of Things
IrDA	Infrared
ISR	Intelligence Surveillance and Reconnaissance
ITS	Intelligent Transportation Systems

JIE	Joint Information Environment
LAN	Local Area Network
LF RFID	Low Frequency Radio Frequency IDentification
LOS	Line Of Sight
LPD	Low Probability of Detection
LPI	Low Probability of Interception
LPP	LTE Positioning Protocol
LTE	Long Term Evolution
LTE-A	LTE-Advanced
QR	Quick Response
RFID	Radio Frequency IDentification
REST	REpresentational State Transfer
RSS	Received Signal Strength
M2M	Machine-to-Machine
MANET	Mobile Ad Hoc Network
MBWCS	Military Broadband Wireless Communication System
MES	Manufacturing Execution System
MIMO	Multiple-Input Multiple-Output
MitM	Man-in-the-Middle
MORANE	Mobile Radio for Railway Networks in Europe
MPE	Mission Partner Environment
MRC	Maximum-Ratio Combiner
MSE	Minimum-Squared Error
MTC	Machine Type Communications
NLOS	Non Line-of-Sight
NCW	Network Centric Warfare
NEC	Network-Enabled Capability
NETSEC	Network Security
NFC	Near-Field Communication
NFV	Network Function Virtualization
NII	Network Information Infrastructure
OTAR	Over-The-Air Rekeying
PaaS	Platform as a Service
PAPR	Peak-to-Average Power Ratio
PPDR	Public Protection Disaster Relief
PMP	Point-To-Multipoint
PoC	Push-to-Talk over Cellular

ProSe	Proximity Services
PtP	Point-to-Point
PTT	Push-to-talk
QoI	Quality of Information
RAMS	Reliability, Availability, Maintainability and Safety
RFID	Radio-frequency identification
ROHC	Robust Header Compression
SaaS	Software as a Service
SC	Selection Combiner
SSC	Switch-and-Stay Combiner
ScanC	Scanner Combiner
SDR	Software Defined Radio
SIL	Safety Integrity Level
SNMP	Simple Network Management Protocol
SSB-ASK	Single-Sideband ASK
SSC	Switch-and-Stay Combiner
SOA	Service-Oriented Architecture
SON	Self-Organizing Networks
TCCA	TETRA + Critical Communications Association
TETRA	Trans European Trunked RAdio
TLS	Transport Layer Security
TRANSEC	Transmission Security
UAV	Unmanned Aerial Vehicle
UHF	Ultra-High Frequency
UID	Unique Identifier
UWB	Ultra-Wide Band
VGCS	Voice Group Call Service
VoI	Value of Information
VoIP	Voice-over-Internet Protocol
VoLGA	Voice over LTE via Generic Access
VoLTE	Voice over LTE
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WirelessHART	Wireless Highway Addressable Remote Transducer Protocol
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Networks

Bibliography

[1] Business Insider (BI) Intelligence. *The Internet of Things: Examining How the IoT Will Affect the World*; Technical Report; Business Insider: New York, USA, November 2015.

[2] Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32.

[3] Vermesan, O.; Friess, P. *IoT—From Research and Innovation to Market Deployment*; River Publishers: Aalborg, Denmark, 2014.

[4] Takanokura, M.; Matsui, M.; Tang, H. Energy management with battery system for smart city. In Proceedings of the 33rd Chinese Control Conference (CCC), Nanjing, China, 28–30 July 2014; pp. 8200–8203.

[5] Alam, K.M.; Saini, M.; Saddik, A.E. Toward social internet of vehicles: Concept, architecture, and applications. *IEEE Access* **2015**, *3*, 343–357.

[6] Manyika, J.; Chui, M.; Bisson, P.; Woetzel, J.; Dobbs, R; Bughin, J; Aharon, D. *The Internet of Things: Mapping the Value beyond the Hype*; Technical Report; McKinsey Global Institute, 2015.

[7] Ericsson. *Ericsson Mobility Report on the Pulse of the Networked Society*; Technical Report; Ericsson: Stockholm, Sweden, November 2015.

[8] Zheng, D.; Carter, W.A. *Leveraging the IoT for a more Efficient and Effective Military*; Technical Report; Rowman & Littlefield: Lanham, MD, USA, 2015.

[9] Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376.

[10] Miorandi, D.; Sicari, S.; Pellegrini, F.D.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516.

[11] Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805.

[12] Akyildiz, I.F.; Jornet, J.M. The Internet of nano-things. *IEEE Wirel. Commun.* **2010**, *17*, pp. 58–63.

[13] Marketsandmarkets.com. *Smart Railways Market by Solution (Passenger Information, Freight Information, Rail Communication, Advanced Security Monitoring, Rail Analytics), Component, Service (Professional, Managed), and Region - Global Forecast to 2021*; Technical Report; Marketsandmarkets: Pune, India, November 2016.

[14] International Transport Forum (2011). Available online: http://www.itf-oecd.org/sites/default/files/docs/11outlook.pdf (accessed on 28 February 2017).

[15] Hofestadt, H. GSM-R: Global System for Mobile radio communications for Railways. In Proceedings of the International Conference on Electric Railways in a United Europe, IET, 1995. pp. 111-115.

[16] Ljubic, I.; Simunic, D. Advanced Speech Call Items for GSM-Railway. In Proceedings of the 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, Aalborg, Denmark, 17–20 May 2009, pp. 131-136.

[17] Fraga-Lamas, P.; Rodríguez-Piñeiro, J.; García-Naya, J.A.; Castedo, L. Unleashing the potential of LTE for next generation railway communications. In *Communication Technologies for Vehicles, Proceedings of the 8th International Workshop on Communication Technologies for Vehicles (Nets4Cars/Nets4Trains/Nets4Aircraft 2015))*, Sousse, Tunisia, 6–8 May 2015; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9066, pp. 153–164.

[18] Rodríguez-Piñeiro, J.; Fraga-Lamas, P.; García-Naya, J.A.; Castedo, L. Long term evolution security analysis for railway communications. In Proceedings of the IEEE Congreso de Ingeniería en Electro-Electrónica, Comunicaciones y Computación (ARANDUCON 2012), Asunción, Paraguay, 28–30 November 2012.

[19] Fraga-Lamas, P.; Rodríguez-Piñeiro, J.; García-Naya, J.A.; Castedo, L. A survey on LTE networks for railway services. In Proceedings of the IEEE Congreso de Ingeniería en Electro-Electrónica, Comunicaciones y Computación (ARANDUCON 2012), Asunción, Paraguay, 28–30 November 2012.

[20] Moreno, J.; Riera, J. M.; Haro, L. d., Rodriguez, C. A survey on future railway radio communications services: challenges and opportunities. *IEEE Commun. Mag.* **2015**, *53*, 62–68.

[21] Aguado, M.; Jacob, E.; Higuero, M.; Saiz, P.S.; Berbineau, M. *Broadband communication in the high mobility scenario: the WiMAX opportunity*, WIMAX New Developments, Dalal, U. D. and Kosta, Y. P. (Ed.), InTech: Hampshire, England, 2009.

[22] Fokum, D.; Frost, V. A Survey on Methods for Broadband Internet Access on Trains. *IEEE Commun. Surv. Tutor.* **2010**, *12*, 171-185.

[23] Masson, E.; Berbineau, M. *Broadband Wireless Communications for Railway Applications: For Onboard Internet Access and Other Applications*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2016.

[24] He, R.; Ai, B.; Wang, G.; Guan, K.; Zhong, Z.; Molisch, A. F.; Briso-Rodriguez, C.; Oestges, C. High-Speed Railway Communications: From GSM-R to LTE-R. *IEEE Veh. Technol. Mag.* **2016**, *11*, 49–58.

[25] International Union of Railways (UIC) - GSM-R Operators Group, European Integrated Radio Enhanced NEtwork (EIRENE). *Functional Requirements Specification Version 8.0.0*; Technical Report; EIRENE: Paris, France, December 2015.

[26] International Union of Railways (UIC) - GSM-R Operators Group, European Integrated Radio Enhanced NEtwork (EIRENE). *System Requirements Specification Version 16.0.0*; Technical Report; EIRENE: Paris, France, December 2015.

[27] Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community, 2008.

[28] European Telecommunications Standards Institute (ETSI). *ETSI TS 103 066 v1.1.2 (2012-04),Railways Telecommunications (RT); Rel-4 Core Network requirements for GSM-R*; Technical Report; ETSI: Sophia-Antipolis, France, 2012.

[29] Pushparatnam, L., Taylor, T. *GSM-R Procurement & Implementation Guide*; nternational Union of Railways (UIC), V 1.0-15.03.2009; UIC: Paris, France, August March 2009.

[30] International Union of Railways (UIC) - High speed. Available online: http://www.uic.org/highspeed (accessed on 28 February 2017).

[31] Ai, B.; Cheng, X.; Kurner, T.; Zhong, Z.-D.; Guan, K.; He, R.-S.; Xiong, L.; Matolak, D.W.; Michelson, D.G.; Briso-Rodriguez, C. Challenges Toward Wireless Communications for High-Speed Railway. *IEEE Trans. Intell. Transp. Syst.* **2014**, *15*, 2143–2158.

[32] European Union Agency for Railways. Set of specifications # 1 (ETCS baseline 2 and GSM-R baseline 1). Available online: http://www.era.europa.eu/Core-Activities/ERTMS/Pages/Set-of-specifications-1.aspx (accessed on 28 February 2017).

[33] European Union Agency for Railways. ERTMS GSM-R QoS Test Specification. Available online: http://www.era.europa.eu/Document-Register/Pages/O_2475.aspx (accessed on 28 February 2017).

[34] European Telecommunications Standards Institute (ETSI). *ETSI TR 103 134 V1.1.1 (2013-03) Railway Telecommunications (RT); GSM-R in support of EC Mandate M/486 EN on Urban Rail*; Technical Report; ETSI: Sophia-Antipolis, France, March 2013.

[35] Memorandum of Understanding (MoU) between the European Commission, the European Railway Agency and the European Rail sector Associations (CER - UIC - UNIFE - EIM - GSM-R Industry Group - ERFA) concerning the strengthening of cooperation for the management of ERTMS. Available online: http://www.era.europa.eu/Document-Register/Pages/Memorandum-of-Understanding-concerning-ERTMS.aspx (accessed on 28 February 2017).

[36] International Union of Railways (UIC). *LTE / SAE - The Future Railway Mobile Radio System? A Future Railway Mobile Radio System v1.1*; Technical Report; UIC: Paris, France, 2009.

[37] TCCA (TETRA & CRITICAL COMMUNICATIONS ASSOCIATION), P3 communications GmbH. *Study on the relative merits of TETRA, LTE and other broadband technologies for critical communications markets*; Technical Report; TCCA: Aachen, Germany, February 2015.

[38] GSMA (GSM Association). *Document IR.92 - IMS Profile for Voice and SMS Version 9.0*; Technical Report; GSMA: London, United Kingdom, April 2015.

[39] Zhang, W. Study on Internet of Things application for High-speed Train Maintenance, Repair and Operation (MRO). In Proceedings of the National Conference

on Information Technology and Computer Science (CITCS 2012), Lanzhou, China , 16–18 November 2012; pp. 8–12.

[40] Turner, C., Ravi, P. T., Tiwari, A., Starr, A., Blacktop, K. A review of key planning and scheduling in the rail industry in Europe and UK. *Journal of Rail and Rapid Transit* **2016**, *230*, 984–998.

[41] Turner, C., Ravi, P. T., Tiwari, A., Starr, A., Blacktop, K. A software architecture for autonomous maintenance scheduling: Scenarios for UK and European Rail. *International Journal of Transport Development and Integration* **2017**, *1*, 371–381.

[42] Trenitalia: Creating a Dynamic Maintenance Management System Powered by SAP HANA. Available online: http://www.sap.com/italy/assetdetail/2015/12/b6caea0d-507c-0010-82c7-eda71af511fa.html (accessed on 28 February 2017).

[43] VR Group strives for punctuality through analytics. Available online: http://www.sas.com/sv_se/customers/vr-group-en.html (accessed on 28 February 2017).

[44] The Internet of Trains - Analysing sensor data helps Siemens keep operators on track by reducing train failures (Case study/Transportation). Available online: http://assets.teradata.com/resourceCenter/downloads/CaseStudies/EB8903.pdf?processed=1 (accessed on 28 February 2017).

[45] La SNCF mise sur l'IoT industriel avec Ericsson, IBM et Sigfox. Available online: https://aruco.com/2016/04/sncf-internet-objets-industriel/ (accessed on 28 February 2017).

[46] Thaduri, A.; Galar, D.; Kumar, U. Railway assets: a potential domain for big data analytics. *Procedia Computer Science* **2015**, *53*, 457-467.

[47] Soh, S. S.; Radzi, N. H. M.; Haron,H. Review on Scheduling Techniques of Preventive Maintenance Activities of Railway. In Proceedings of the 2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation, Kuantan, Malaysia, 25–27 September 2012; pp. 310-315.

[48] Núñez, A., Hendriks, J., Li, Z., De Schutter, B., Dollevoet, R. Facilitating maintenance decisions on the Dutch railways using big data: The ABA case study. In Proceedings of the 2014 IEEE International Conference on Big Data (Big Data), Washington, DC, 27–30 October 2014; pp. 48–53.

[49] Hodge, V. J.; O'Keefe, S.; Weeks, M.; Moulds, A. Wireless Sensor Networks for Condition Monitoring in the Railway Industry: A Survey. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 1088–1106.

[50] Chen, R.; Wang, P.; Xu, H. Integrated Monitoring System for Rail Damage in High Speed Railway Turnout. In Proceedings of the 2013 Fourth International Conference on Digital Manufacturing and Automation, Qindao, Shandong, China, 29–30 June 2013, pp. 704-709.

[51] Li, H.; Yao, T., Ren, M., Rong, J., Liu, C., Jia, L. (2016). Physical topology optimization of infrastructure health monitoring sensor network for high-speed rail. *Measurement* **2016**, *79*, 83–93.

[52] Ambellouis, S.; Bruyelle, J. L. *Focus on Railway Transport. In Intelligent Video Surveillance Systems*, 1st ed.; John Wiley & Sons: New York, New York, USA, 2012.

[53] Dominguez, M.; Fernandez, A.; Cucala, A. P.; Blanquer, J. Efficient design of automatic train operation speed profiles with on board energy storage devices. *WIT Transactions on the Built Environment* **2010**, *114*, 509–520.

[54] Salmane, H.; Khoudour, L.; Ruichek, Y. A video-analysis-based railway-road safety system for detecting hazard situations at level crossings. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 596-609.

[55] Govoni, M.; Guidi, F.; Vitucci, E. M.; Espoti, V. D., Tartarini, G.; Dardari, D. Ultra-wide bandwidth systems for the surveillance of railway crossing areas. *IEEE Commun. Mag.* **2015**, *53*, 117-123.

[56] Barro-Torres, S. J.; Fernández-Caramés, T. M.; González-López, M.; Escudero, C. J. Maritime Freight Container Management System Using RFID. In Proceedings of EURASIP Workshop on RFID Technology, La Manga del Mar Menor, Spain, September 2010.

[57] Fernández-Caramés, T. M.; Fraga-Lamas, P.; Suárez-Albela, M.; Castedo, L. Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications. *Sensors.* **2017**, *17*, 28.

[58] Fernández-Caramés, T. M.; Fraga-Lamas, P.; Suárez-Albela, M.; Castedo, L. A methodology for evaluating security in commercial RFID systems. To be published in *Radio Frequency Identification*, 1st ed.; Crepaldi, P. C.; Pimenta, T. C.; INTECH: Rijeka, Croatia, 2016.

[59] Fraga-Lamas, P.; Fernández-Caramés, T. M. Reverse Engineering the Communications Protocol of an RFID Public Transportation Card. Accepted in 2017 IEEE International Conference on RFID (IEEE RFID 2017), Phoenix, AZ, USA, 9-11 May 2017.

[60] Roberts, C.M. Radio frequency identification (RFID), *Computers & Security*, **2006**, *25(1)*, pp. 18-26.

[61] Mednis, A.; Zviedris, R. RFID communication: How well protected against reverse engineering? In Proceedings of the Second International Conference on Digital Information Processing and Communications, Klaipeda City, Latvia, July 2012; pp. 59-61.

[62] Hutter, M.; Schmidt, J.M; Plos, T. Contact-based fault injections and power analysis on RFID tags. In Proceedings of the European Conference on Circuit Theory and Design, Antalya, Turkey, Aug. 2009; pp. 409-412.

[63] Vojtech, L.; Kahl, J. Power analysis of communication of RFID transponders with Password-Protected Memory. In Proceedings of the Eighth International Conference on Networks, Gosier, France, Mar. 2009; pp. 116-120.

[64] Oren, Y. Remote password extraction from RFID tags, *IEEE Trans. Comput.* **2007**, *56*, pp. 1292-1296. DOI: 10.1109/TC.2007.1050.

[65] Nohl, K.; Evans, D.; Plötz, S.; Plötz, H. Reverse-engineering a cryptographic RFID tag. In Proceedings of the 17th USENIX Security Symposium, San José, United States, July 2008; pp. 185-193.

[66] RFIDiot official webpage. Available online: www.rfidiot.org (accessed on 28 February 2017).

[67] Feldhofer, M.; Aigner, M.; Baier, T.; Hutter, M.; Plos, T.; Wenger, E. Semi-passive RFID development platform for implementing and attacking security tags. In Proceedings of the International Conference for Internet Technology and Secured Transactions, London, United Kingdom, Nov. 2010, pp. 1-6.

[68] Proxmark 3 Community webpage. Available online: www.proxmark.org (accessed on 28 February 2017).

[69] Tastic official webpage. Available online: www.bishopfox.com/resources/tools/rfid-hacking/attack-tools (accessed on 28 February 2017)

[70] OpenPCD Reader. Available online: http://www.openpcd.org (accessed on 28 February 2017)

[71] OpenPICC tag emulator. Available online: http://www.openpicc.org (accessed on 28 February 2017)

[72] Chameleon Project. Available online: https://github.com/skuep/ChameleonMini/wiki (accessed on 28 February 2017)

[73] McAffe's Proxbrute webpage. Available online: http://www.mcafee.com/es/downloads/free-tools/proxbrute.aspx (accessed on 28 February 2017)

[74] Paddington, J.; Tarry, S. *Study on Public Transport Smartcards Final Report*; Technical Report; European Commission DG MOVE, 2011.

[75] Nohl, K.; Plotz, H. MifareLittle Security, Despite Obscurity. In Proceedings of the 24th Chaos Communication Congress (24C3), Berlin, Germany, 2007.

[76] Siekerman, P.; Schee M. v. d. *Security Evaluation of the disposable OV-chipkaart v1.7*; Dept. System and Network Engineering, University of Amsterdam, 2008.

[77] Verdult, R. *Proof of concept, cloning the OV-Chip card*; Technical Report; Radboud University Nijmegen, 2008.

[78] Kasper, T.; Maurich, I. v.; Oswald, D.;Paar, C. Chameleon: A Versatile Emulator for Contactless Smartcards. In Proceedings of the 13th International Conference Information Security and Cryptology (ICISC 2010), Seoul, Korea, 1-3 December 2010.

[79] Oswald, D.; Paar, C. Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World. In Proceedings of Cryptographic Hardware and Embedded Systems (CHES 2011). *Lecture Notes in Computer Science*, vol 6917, Springer: Berlin, Heidelberg, pages 207-222, 2011.

[80] RIDAC RFID reverse-engineering methodology. Available online: https://www.ee.oulu.fi/research/ouspg/RFID%20Reverse%20Engineering (accessed on 28 February 2017)

[81] Open-source RFID audit framework RIDAC. Available online: https://www.ee.oulu.fi/research/ouspg/RIDAC (accessed on 28 February 2017)

[82] FCC ID search webpage. Available online: https://www.fcc.gov/general/fcc-id-search-page (accessed on 28 February 2017)

[83] Using the Agilent N9322C Basic Spectrum Analyzer (BSA). *Low Frequency RFID Tag Characterization*; Application Note; Agilent: United States, May 2013.

[84] USRP webpage. Available online: https://www.ettus.com (accessed on 28 February 2017)

[85] Kocatepe, Ü.; Için, O. Spectrum monitoring and demodulation using LabVIEW and USRP RIO software defined radio. In Proceedings of the 24th Signal Processing and Communication Application Conference (SIU), Zonguldak, Turkey, May 2016, pp. 517-520.

[86] Srivastava, S.; Hashmi, M.; Das, S.; Barua, D. Real-time blind spectrum sensing using USRP. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Lisbon, Portugal, May 2015, pp. 986-989.

[87] Nafkha, A.; Naoues, M.; Cichony, K.; Kliks, A.; Aziz, B. Hybrid spectrum sensing experimental analysis using GNU radio and USRP for cognitive radio. In Proceedings of the International Symposium on Wireless Communication Systems (ISWCS), Brussels, Belgium, Aug. 2015, pp. 506-510.

[88] Dobre, O. A.; Abdi, A.; Bar-Ness, Y.; Su, W. Survey of automatic modulation classification techniques: classical approaches and new trends. *IET Communications* **2007**, *1*, pp. 137-156. DOI:

[89] Bertoncini, C.; Rudd, K.; Nousain, B.; Hinders, M. Wavelet Fingerprinting of Radio-Frequency Identification (RFID) Tags, *IEEE Trans. Ind. Electron.* **2012**, *59*, pp. 4843-4850.

[90] Ma, L.; Yang, Y.; Wang, H. DBN based automatic modulation recognition for ultra-low SNR RFID signals, Proceedings of the 35th Chinese Control Conference (CCC), Chengdu, China, Aug. 2016, pp. 7054-7057.

[91] Han, J.; Qian, C.; Yang, P.; Ma, D.; Jiang, Z.; Xi, W.; Zhao, J. GenePrint: Generic and Accurate Physical-Layer Identification for UHF RFID Tags. *IEEE/ACM Transactions on Networking* **2016**, *24*, pp. 846-858.

[92] Zhu, F.; Xiao, B.; Liu, J.; Chen, L. J. Efficient Physical-Layer Unknown Tag Identification in Large-Scale RFID Systems. *IEEE Transactions on Communications* **2017**, *65*, pp.283-295.

[93] International Organization for Standardization (ISO); International Electrotechnical Commission (IEC). *Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards*; ISO/IEC 14443:2000; ISO: Geneva, Switzerland, 2008.

[94] M. Weiß. *Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment,* M.Sc. thesis, Germany, 2010.

[95] Suárez-Casal, P.; Carro-Lagoa, A.; García-Naya, J.A.; Fraga-Lamas, P.; Castedo, L.; Morales-Méndez, A. A Real-Time Implementation of the Mobile WiMAX ARQ and Physical Layer. *Journal of Signal Processing System* **2015**, *78*, 283-297.

[96] Carro-Lagoa, A.; Suárez-Casal, P.; García-Naya, J.A.; Fraga-Lamas, P.; Castedo, L.; Morales-Méndez, A. Design and Implementation of an OFDMA-TDD Physical Layer for WiMAX Applications. *EURASIP Journal on Wireless Communications and Networking* **2013**, *2013*, 243.

[97] Fraga-Lamas, P.; Castedo-Ribas, L.; Morales-Méndez, A.; Camas-Albar, J.M. Evolving military broadband wireless communication systems: WiMAX, LTE and WLAN. In Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 23–24 May 2016; pp. 1–8.

[98] Fraga-Lamas, P.; Camas, J.M.; Carro, A.; Suárez, P.; Castedo, L.; García-Naya, J.A.; Morales, A. Mobile WiMAX for next generation tactical wireless networks. In Proceedings of the Information Systems Technology Panel Symposium on Emerged/Emerging 'Disruptive' Technologies (NATO IST-099 / RSY-024), Madrid, Spain, 9–10 May 2011.

[99] Carro-Lagoa, A.; Suárez-Casal, P.; Fraga-Lamas, P.; García-Naya, J.A.; Castedo, L.; Morales-Méndez, A. Real-time validation of a SDR implementation of TDD WiMAX standard. In Proceedings of the 2013 Wireless Innovation Forum European Conference on Communications Technologies and Software Defined Radio (SDR-WInnComm-Europe 2013), Munich, Germany, 11–13 June 2013.

[100] Fraga-Lamas, P.; Castedo-Ribas, L.; Morales-Méndez, A.; Camas-Albar, J. M. Sistemas de comunicaciones militares de banda ancha basados en tecnologías inalámbricas 4G. In Proceedings of the DESEi+d 2015, III Congreso Nacional de I+D en Defensa y Seguridad, Pontevedra, Spain, 19–20 November 2015; pp. 925–932.

[101] Fraga-Lamas, P.; Castedo-Ribas, L.; Morales-Méndez, A.; Camas-Albar, J.M. Estudio comparativo de aplicabilidad de tecnologías inalámbricas de banda ancha civiles en entornos militares. In Proceedings of the DESEi+d 2013, I Congreso Nacional de I+D en Defensa y Seguridad, Madrid, Spain, 6–7 November 2013; pp. 565–573.

[102] Camas-Albar, J.M.; Morales-Méndez, A.; Castedo-Ribas, L.; Fraga-Lamas, P.; Brown, C.; Tschauner, M.; Hayri-Kucuktabak, M. NATO Task Group ET-IST-068, IST (Information Systems Technology) panel of NATO STO (Science

and Technology Organization). In *LTE vs. WiMAX for Military Applications*; Technical Report; North Atlantic Treaty Organization (NATO): Brussels, Belgium, 2015.

[103] IEEE 802.16: Broadband Wireless Metropolitan Area Networks (MANs). Available online: http://standards.ieee.org/about/get/802/802.16.html (accessed on 28 February 2017)

[104] LTE specifications. Release 10 onwards. Available online: http://www.3gpp.org/specifications/specifications (accessed on 28 February 2017)

[105] IEEE 802.11: Wireless LANs. Available online: http://standards.ieee.org/about/get/802/802.11.html(accessed on 28 February 2017)

[106] International Telecommunication Union Radiocommunication Sector (ITU-R). *Radiocommunication Objectives and Requirements for Public Protection and Disaster Relief (PPDR)*; Technical Report ITU-R M.2377-0 (07/2015); ITU: Geneva, Switzerland, July 2015.

[107] TETRA Association. *Public Safety Mobile Broadband and Spectrum Needs,16395-94, Analysis Mason*; Technical Report; Analysis Mason Limited: London, UK, March 2010.

[108] TETRA Critical Communications Association (TCCA). *The Strategic Case for Mission Critical Mobile Broadband: A Review of the Future Needs of the Users of Critical Communications*; Technical Report; TCCA: Newcastle Upon Tyne, UK, December 2013.

[109] European Telecommunications Standards Institute (ETSI). *Emergency Communications (EMTEL); Requirements for Communications from Authorities/Organizations to Individuals, Groups or the General Public During Emergencies*; Technical Report ETSI TS 102 182-V1.4.1; ETSI: Sophia Antipolis, France, July 2010.

[110] Telecommunications Industry Association (TIA). *APCO Project 25 Statement of Requirements (P25 SoR)*; Technical Report; TIA: Arlington, United States, December 2013.

[111] Office of Emergency Communications. *Fiscal Year 2016 SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance)*; Technical Report; Department of Homeland Security: Washington , D.C., USA, 2016.

[112] Baldini, G.; Karanasios, S.; Allen, D.; Vergari, F. Survey of wireless communication technologies for public safety. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 619–641.

[113] Favraud, R.; Apostolaras, A.; Nikaein, N.; Korakis, T. Toward moving public safety networks. *IEEE Commun. Mag.* **2016**, *54*, 14–20.

[114] Chudzikiewicz, J.; Furtak, J.; Zielinski, Z. Fault-tolerant techniques for the Internet of Military Things. In Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 12–14 December 2015; pp. 496–501.

[115] Yushi, L.; Fei, J.; Hui, Y. Study on application modes of military Internet of Things (MIOT). In Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 25–27 May 2012; Voloum 3, pp. 630–634.

[116] Butun, I.; Erol-Kantarci, M.; Kantarci, B.; Song, H. Cloud-centric multi-level authentication as a service for secure public safety device networks. *IEEE Commun. Mag.* **2016**, *54*, 47–53.

[117] Mariani, J.; Williams, B.; Loubert, B. *Continuing the March: The Past, Present, and Future of the IoT in The Military*; Technical Report; Deloitte University Press: Deloitte, UK, 2015.

[118] Eom, J. Security threats recognition and countermeasures on smart battlefield environment based on IoT. *Int. J. Secur. Appl.* **2015**, *9*, 347–356.

[119] Alqassem, I.; Svetinovic, D. A taxonomy of security and privacy requirements for the Internet of Things (IoT). In Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, Malaysia, 9–12 December 2014; pp. 1244–1248.

[120] Trusted Computing Group, Guidance for Securing IoT Using TCG Technology, Version 1.0, Revision 21. Available online: http://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf (Acessed on July 2016).

[121] Pérez-Expósito, J. M.; Fernández-Caramés, T.M.; Fraga-Lamas, P.; Castedo, L. VineSens: An Eco-Smart Decision Support Viticulture System. *Sensors* **2017**, *17*, 465.

[122] Blanco-Novoa, O.; Fernández-Caramés, T.M.; Fraga-Lamas, P.; Castedo, L. An Electricity-Price Aware Open-Source Smart Socket for the Internet of Energy. *Accepted in Sensors*. **2017**.

[123] Fraga-Lamas, P.; Suárez-Albela, M.; Fernández-Caramés, T. M.; Castedo, L.; González-López, M. A Review on Internet of Things for Defense and Public Safety. *Sensors* **2016**, *16*, 1644.

[124] Suárez-Albela, M.; Fraga-Lamas, P.; Fernández-Caramés, T.M.; Dapena, A.; González-López, M. Home Automation System Based on Intelligent Transducer Enablers. *Sensors* **2016**, *16*, 1595.

[125] Suárez-Albela, M; Fraga-Lamas, P.; Fernández-Caramés, González-López, M. Sistema domótico con auto-configuración y auto-detección rápida de transductores. In Proceedings of the XXXI Simposium Nacional de la Unión Científica Internacional de Radio (URSI), Madrid, Spain, 5–7 September 2016.

[126] Fraga-Lamas, P.; Fernández-Caramés, T. M.; Carro-Lagoa, A.; Escudero-Cascón, C. J.; González-López, M. IPT-20111006, Project CIUDAD2020: A new smart city model that is ecologically and economically sustainable. *Estndares para interoperabilidad de redes de sensores: IEEE 1451 y Sensor Web Enablement (SWE)/ Standards towards interoperability of wireless sensor networks: IEEE 1451 and Sensor Web Enablement (SWE)*; White Paper; Innpronta Ciudad2020: Madrid, Spain, January 2014.

[127] Aegis Combat System. Available online: http://www.lockheedmartin.com/us/products/aegis.html (accessed on 28 February 2017).

[128] Tomahawk Land Attack Missile (TLAM). Available online: http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=F4E98B0F-33F5-413B-9FAE-8B8F7C5F0766 (accessed on 28 February 2017).

[129] Calhoun, G.L.; Draper, M.H. Display and Control Concepts for Multi-UAV Applications. In *Handbook of Unmanned Aerial Vehicles*; Springer: Dordrecht, The Netherlands, 2015; pp. 2443–2473.

[130] Wang, P.; Ali, A.; Kelly, W. Data security and threat modeling for smart city infrastructure. In Proceedings of the International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 5–7 August 2015; pp. 1–6.

[131] Instrumented-Multiple Integrated Laser Engagement System (I-MILES). Available online: https://www.cubic.com/Global-Defense/Training-Systems-and-Solutions/Ground-Combat-Training/Multiple-Integrated-Laser-Engagement-System (accessed on 28 February 2017).

[132] Chang, J.M.; Ho, P.C.; Chang, T.C. Securing BYOD. *IT Prof.* **2014**, *16*, 9–11.

[133] U.S. Department of Defense. *Annual Energy Management Report*; Technical Report; Office of the Assistant Secretary of Defense (Energy, Installations, and Environment): Washington, D.C., USA, May 2015.

[134] OMA Lightweight M2M. Available online: http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-lightweightm2m-v1-0 (accessed on 28 February 2017).

[135] Perelman, V.; Schnwlder, J.; Ersue, M.; Watsen, K. Network configuration protocol for constrained devices (NETCONF Light). *IETF Draft* **2012**.

[136] Abeele, F.V.; Hoebeke, J.; Moerman, I.; Demeester, P. Fine-grained management of CoAP interactions with constrained IoT devices. In Proceedings of the IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 5–8 May 2014; pp. 1–5.

[137] OMA Device Management Working Group. Available online: http://openmobilealliance.org/about-oma/work-program/device-management/ (accessed on 28 February 2017).

[138] Program Executive Office Soldier, Portfolio 2014—The Soldier: Our Strength and Purpose. Available online: http://www.peosoldier.army.mil/portfolio/ accessed on 28 February 2017).

[139] U.S. Air Force: Programmers Earn Award for Innovative Tablet App. Available online: http://www.af.mil/News/ArticleDisplay/tabid/223/Article/518660/programmers-earn-award-for-innovative-tablet-app.aspx (accessed on 28 February 2017).

[140] Mitchell, P.T. *Network Centric Warfare and Coalition Operations—The New Military Operating System*, 1st ed.; Routledge: New York, NY, USA, 2009.

[141] Janes.com, U.S. Harris Corporation Readies New Tactical Radios for US Special Forces. Available online: http://www.janes.com/article/60812/harris-corporation-readies-new-tactical-radios-for-us-special-forces (accessed on 28 February 2017).

[142] Wood, T.; Ramakrishnan, K.K.; Hwang, J.; Liu, G.; Zhang, W. Toward a software-based network: Integrating software defined networking and network function virtualization. *IEEE Netw.* **2015**, *29*, 36–41.

[143] Salmanian, M.; Brown, J.D.; Watson, S.; Song, R.; Tang, H.; Simmelink, D. An architecture for secure interoperability between coalition tactical MANETs. In Proceedings of the Military Communications Conference, Tampa, FL, USA, 26–28 October 2015; pp. 37–42.

[144] Ward, J.R.; Younis, M. A cross-layer defense scheme for countering traffic analysis attacks in Wireless Sensor Networks. In Proceedings of the Military Communications Conference, Tampa, FL, USA, 26–28 October 2015; pp. 972–977.

[145] Amdouni, I.; Adjih, C.; Plesse, T. Network coding in military wireless ad hoc and sensor networks: Experimentation with GardiNet. In Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Cracow, Poland, 18–19 May 2015; pp. 1–9.

[146] Zambrano, A.; Perez, I.; Palau, C.; Esteve, M. Quake detection system using smartphone-based wireless sensor network for early warning. In Proceedings of the 2014 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Budapest, Hungary, 24–28 March 2014; pp. 297–302.

[147] Beal, J.; Usbeck, K.; Loyall, J.; Metzler, J. Opportunistic sharing of airborne sensors. In Proceedings of the 2016 International Conference on Distributed Computing in Sensor Systems (DCOSS), Washington, DC, USA, 26–28 May 2016; pp. 25–32.

[148] Ganz, F.; Li, R.; Barnaghi, P.; Harai, H. A resource mobility scheme for service-continuity in the internet of things. In Proceedings of the IEEE International Conference on Green Computing and Communications (GreenCom), Besanon, France, 20–23 November 2012; pp. 261–264.

[149] Fu, H.L.; Lin, P.; Yue, H.; Huang, G.M.; Lee, C.P. Group mobility management for large-scale machine-to-machine mobile networking. *IEEE Trans. Veh. Technol.* **2014**, *63*, 1296–1305.

[150] Yürür, O.; Liu, C.H.; Sheng, Z.; Leung, V.C.M.; Moreno, W.; Leung, K.K. Context-awareness for mobile sensing: A survey and future directions. *IEEE Commun. Surv. Tutor.* **2016**, *18* , 68–93.

[151] Etefia, B.; Gerla, M.; Zhang, L. Supporting military communications with Named Data Networking: An emulation analysis. In Proceedings of the IEEE Military Communications Conference, Orlando, FL, USA, 29 October–1 November 2012; pp. 1–6.

[152] Fongen, A.; Mancini, F. Integrity attestation in military IoT. In Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 12–14 December 2015; pp. 484–489.

[153] Defense Information Systems Agency (DISA) for Department of Defense (DoD). *Cloud Computing Security Requirements Guide*; Technical Report; DISA: Fort Meade, Maryland, USA, March 2016.

[154] lvarez, J.L.; Rice, M.; Samson, J.R.; Koets, M.A. Increasing the capability of CubeSat-based software-defined radio applications. In Proceedings of the IEEE Aerospace Conference, Big Sky, MT, USA, 4–11 March 2016; pp. 1–10.

[155] U.S. Department of Defense. *Unmanned Systems Integrated Roadmap FY2013–2038*; Technical Report; U.S. Department of Defense: The Pentagon, Arlington County, Virginia, USA, 2013.

[156] Maalel, N.; Natalizio, E.; Bouabdallah, A.; Roux, P.; Kellil, M. Reliability for emergency applications in internet of things. In Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems, Cambridge, MA, USA, 20–23 May 2013; pp. 361–366.

[157] Li, L.; Jin, Z.; Li, G.; Zheng, L.; Wei, Q. Modeling and analyzing the reliability and cost of service composition in the IoT: A probabilistic approach. In Proceedings of the IEEE 19th International Conference on Web Services (ICWS), Honolulu, HI, USA, 24–29 June 2012; pp. 584–591.

[158] Alsheikh, M.A.; Hoang, D.T.; Niyato, D.; Tan, H.P.; Lin, S. Markov decision processes with applications in wireless sensor networks: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *17* , 1239–1267.

[159] Defense Information Systems Agency (DISA). *Enabling the Joint Information Environment (JIE), Shaping the Enterprise for the Conflicts of Tomorrow*; Technical Report; DISA: Fort Meade, Maryland, USA, 2014.

[160] Lockheed Martin, Lockheed Martin-Led Team Demonstrates Interoperability with Legacy and Stealth Fighters Using Open Systems Architecture. Available online: http://www.lockheedmartin.com/us/news/press-releases/2014/march/140307ae_lockheed-martin-demonstrates-interoperability.html (accessed on 28 February 2017).

[161] U.S. Army CERDEC (Communications-Electronics Research, Development and Engineering Center) NVESD. Available online: http://www.cerdec.army.mil/inside_cerdec/ (accessed on 28 February 2017).

[162] Docking, M.; Uzunov, A.V.; Fiddyment, C.; Brain, R.; Hewett, S.; Blucher, L. UNISON: Towards a middleware architecture for autonomous cyber defence. In Proceedings of the 24th Australasian Software Engineering Conference (ASWEC), Adelaide, Australia, 28 September–1 October 2015; pp. 203–212.

[163] Cameron, A.; Stumptner, M.; Nandagopal, N.; Mayer, W.; Mansell, T. A rule-based platform for distributed real-time SOA with application in defence systems. In Proceedings of the Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 12–14 November 2013; pp. 1–7.

[164] Sarkar, C.; Nambi, S.N.A.U.; Prasad, R.V.; Rahim, A. A scalable distributed architecture towards unifying IoT applications. In Proceedings of the IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 508–513.

[165] Powers, B. A Multi-agent Architecture for NATO Network Enabled Capabilities: Enabling Semantic Interoperability in Dynamic Environments (NC3A RD-2376). In Proceedings of the 32nd Annual IEEE International Computer Software and Applications Conference, Turku, Finland, 28 July–1 August 2008; pp. 563–564.

[166] ASSIST Database. Available online: http://quicksearch.dla.mil/ (accessed on 28 February 2017).

[167] Al-Fuqaha, A.; Khreishah, A.; Guizani, M.; Rayes, A.; Mohammadi, M. Toward better horizontal integration among IoT services. *IEEE Commun. Mag.* **2015**, *53*, 72–79.

[168] Villaverde, B.C.; Alberola, R.D.P.; Jara, A.J.; Fedor, S.; Das, S.K.; Pesch, D. Service discovery protocols for constrained machine-to-machine communications. *IEEE Commun. Surv. Tutor.* **2014**, *16* , 41–60.

[169] Olyaei, B.B.; Pirskanen, J.; Raeesi, O.; Hazmi, A.; Valkama, M. Performance comparison between slotted IEEE 802.15.4 and IEEE 802.11ah in IoT based applications. In Proceedings of the IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 7–9 October 2013; pp. 332–337.

[170] Vahedi, E.; Ward, R.K.; Blake, I.F. Performance Analysis of RFID Protocols: CDMA Versus the Standard EPC Gen-2. *IEEE Trans. Autom. Sci. Eng.* **2014**, *11*, 1250–1261.

[171] Tsai, C.W.; Lai, C.F.; Chiang, M.C.; Yang, L.T. Data mining for internet of things: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16* , 77–97.

[172] MilCloud. Available online: http://www.disa.mil/computing/cloud-services/milcloud (accessed on 28 February 2017).

[173] Xu, X.; Huang, S.; Chen, Y.; Browny, K.; Halilovicy, I.; Lu, W. TSAaaS: Time series analytics as a service on IoT. In Proceedings of the IEEE International Conference on Web Services (ICWS), Anchorage, AK, USA, 27 June–2 July 2014; pp. 249–256.

[174] Xively. Available online: https://www.xively.com/ (accessed on 28 February 2017).

[175] Nimbits. Available online: http://bsautner.github.io/com.nimbits/ (accessed on 28 February 2017).

[176] Mazhelis, O.; Tyrvinen, P. A framework for evaluating Internet-of-Things platforms: Application provider viewpoint. In Proceedings of the IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 147–152.

[177] Vgler, M.; Schleicher, J.M.; Inzinger, C.; Dustdar, S. A scalable framework for provisioning large-scale IoT deployments. *ACM Trans. Internet Technol.* **2015**, *16*, 1–20.

[178] Satyanarayanan, M.; Lewis, G.; Morris, E.; Simanta, S.; Boleng, J.; Ha, K. The role of cloudlets in hostile environments. *IEEE Pervasive Comput.* **2013**, *12*, 40–49.

[179] Chang, H.; Hari, A.; Mukherjee, S.; Lakshman, T.V. Bringing the cloud to the edge. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 27 April–2 May 2014; pp. 346–351.

[180] Ponte: Connecting Things to Developers. Available online: http://www.eclipse.org/ponte/ (accessed on 28 February 2017).

[181] Celesti, A.; Fazio, M.; Giacobbe, M.; Puliafito, A.; Villari, M. Characterizing cloud federation in IoT. In Proceedings of the 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Crans-Montana, Switzerland, 23–25 March 2016; pp. 93–98.

[182] Chen, M.; Zhang, Y.; Hu, L.; Taleb, T.; Sheng, Z. Cloud-based wireless network: Virtualized, reconfigurable, smart wireless network to enable 5G technologies. *Mob. Netw. Appl.* **2015**, *20*, 704–712.

[183] Lee, C.A. Cloud federation management and beyond: Requirements, relevant standards, and gaps. *IEEE Cloud Comput.* **2016**, *3*, 42–49.

[184] Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. *J. Internet Serv. Appl.* **2013**, *4*, 1–13.

[185] Li, W.; Zhao, Y.; Lu, S.; Chen, D. Mechanisms and challenges on mobility-augmented service provisioning for mobile cloud computing. *IEEE Commun. Mag.* **2015**, *53*, 89–97.

[186] Chang, V.; Ramachandran, M. Towards achieving data security with the cloud computing adoption framework. *IEEE Trans. Serv. Comput.* **2016**, *9*, 138–151.

[187] Wei-bing, M.; Wen-guang, W.; Yi-fan, Z.; Wei-bing, M.; Fa-yi, Y. Semantic Web services description based on command and control interaction user context. In Proceedings of the 2014 IEEE 7th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 20–21 December 2014; pp. 541–544.

[188] Gómez, M.; Preece, A.; Johnson, M.P.; de Mel, G.; Vasconcelos, W.; Gibson, C.; Bar-Noy, A.; Borowiecki, K.; La Porta, T.; Pizzocaro, D.; et al. An ontology-centric approach to sensor-mission assignment. In *Knowledge Engineering: Practice and Patterns*; Springer: Berlin, Germany; Heidelberg, Germany, 2008; pp. 347–363.

[189] W3 PROV. Available online: https://www.w3.org/TR/prov-overview (accessed on 28 February 2017).

[190] McKinsey & Company. *Manufacturing's Next Act*; White Paper; Cornelius, B., Wee, D., Eds.; McKinsey & Company: New York, NY, USA, 2015.

[191] PricewaterhouseCoopers (PwC). *2016 Global Industry 4.0 Survey. Industry 4.0: Building the Digital Enterprise*; Technical Report; PwC: London, UK, 2016.

[192] Wang, S.; Wan, J.; Li, D.; Zhang, C. Implementing smart factory of industrie 4.0: An outlook. *Int. J. Distrib. Sens. Netw.* **2016**, *2016*, 1–10.

[193] Navarro, P.J.; Muro, J.S.; Alcover, P.M.; Fernández-Isla, C. Sensors systems for the automation of operations in the ship repair industry. *Sensors* **2013**, *13*, 12345–12374.

[194] Navantia's web page. Available online: https://www.navantia.es/index.php (accessed on 28 February 2017).

[195] Fraga-Lamas, P.; Noceda-Davila, D.; Fernández-Caramés, T. M.; Díaz-Bouza, M.; Vilar-Montesinos, M. Smart Pipe System for a Shipyard 4.0. *Sensors* **2016**, *12*, 2186.

[196] Fraga-Lamas, P.; Fernández-Caramés, Noceda-Davila, D.; Vilar-Montesinos, M. RSS Stabilization Techniques for a Real-Time Passive UHF RFID Pipe Monitoring System for Smart Shipyards. Accepted in 2017 IEEE International Conference on RFID (IEEE RFID 2017), Phoenix, AZ, USA, 9-11 May 2017.

[197] Fraga-Lamas, P.; Fernández-Caramés, Noceda-Davila, D.; Díaz-Bouza, M. A Real-Time Pipe Monitoring Cyber-Physical System for the Shipyard of the Future. Accepted in 2017 IEEE International Conference on RFID (IEEE RFID 2017), Phoenix, AZ, USA, 9-11 May 2017.

[198] Faíña, A.; Souto, D.; Deibe, A.; López-Peña, F.; Duro, R.J.; Fernández, X. Development of a climbing robot for grit blasting operations in shipyards. In Proceedings of the ICRA'09 2009 IEEE International Conference on Robotics and Automation, New York, NY, USA, 12–17 May 2009; pp. 200–205.

[199] Kuss, A.; Schneider, U.; Dietz, T.; Verl, A. Detection of assembly variations for automatic program adaptation in robotic welding systems. In Proceedings of the ISR 2016 47th International Symposium on Robotics, Munich, Germany, 21–22 June 2016; pp. 1–6.

[200] Mun, S.; Nam, M.; Lee, J.; Doh, K.; Park, G.; Lee, H.; Kim, D.; Lee, J. Sub-assembly welding robot system at shipyards. In Proceedings of the 2015 IEEE International Conference on Advanced Intelligent Mechatronics (AIM), Busan, Korea, 7–11 July 2015; pp. 1502–1507.

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

[202] Kim, M.Y.; Cho, H.S.; Kim, J. Neural network-based recognition of navigation environment for intelligent shipyard welding robots. In Proceedings of the 14th IEEE/RSJ International Conference on Intelligent Robots and Systems, Maui, HI, USA, 29 October–3 November 2001; pp. 446–451.

[203] Kim, M.Y.; Ko, K.; Cho, H.S.; Kim, J. Visual sensing and recognition of welding environment for intelligent shipyard welding robots. In Proceedings of the 13th IEEE/RSJ International Conference on Intelligent Robots and Systems, Takamatsu, Japan, 31 October–5 November 2000; pp. 2159–2165.

[204] Kawakubo, S.; Chansavang, A.; Tanaka, S.; Iwasaki, T. Wireless network system for indoor human positioning. In Proceedings of the 1st International Symposium on Wireless Pervasive Computing, Phuket, Thailand, 16–18 January 2006.

[205] Pérez-Garrido, C.; González-Castaño, F.J.; Chaves-Díeguez, D.; Rodríguez-Hernández, P.S. Wireless remote monitoring of toxic gases in Shipbuilding. *Sensors* **2014**, *14*, 2981–3000.

[206] Yang, J.; Zhou, J.; Lv, Z.; Wei, W.; Song, H. A real-time monitoring system of industry carbon monoxide based on Wireless Sensor Networks. *Sensors* **2015**, *15*, 29535–29546.

[207] Do Amaral Bichet, M.A.; Hasegawa, E.K.; Solé, R.; Núñez, A. Utilization of hyper environments for tracking and monitoring of processes and supplies in construction and assembly industries. In Proceedings of the Symposium on Computing and Automation for Offshore Shipbuilding (NAVCOMP), Rio Grande, Brazil, 14–15 March 2013; pp. 81–86.

[208] Wong, S.F.; Zheng, Y. The effect of metal noise factor to RFID location system. In Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management, Bangkok, Thailand, 10–13 December 2013; pp. 310–314.

[209] Deavours, D.D. Improving the near-metal performance of UHF RFID tags. In Proceedings of the IEEE International Conference on RFID, Orlando, FL, USA, 14–16 April 2010; pp. 187–194.

[210] Arumugan, D.D.; Engels, D.W. Characterization of RF propagation in helical and toroidal metal pipes for passive RFID Systems. In Proceedings of the IEEE International Conference on RFID, Las Vegas, NV, USA, 16–17 April 2008; pp. 269–276.

[211] Rao, K.V.S.; Lam, S.F.; Nikitin, P.V. UHF RFID tag for metal containers. In Proceedings of the Asia-Pacific Microwave Conference, Yokohama, Japan, 7–10 December 2010; pp. 179–182.

[212] Bovelli, S.; Neubauer, F.; Heller, C. Mount-on-Metal RFID transponders for automatic identification of containers. In Proceedings of the 36th European Microwave Conference, Manchester, UK, 10–15 September 2006; pp. 726–728.

[213] Jeong, S.H.; Son, H.W. UHF RFID tag antenna for embedded use in a concrete floor. *IEEE Antennas Wirel. Propag. Lett.* **2011**, *10*, 1536–1225.

[214] Heiss, M.; Hildebrant, R. High-temperature UHF RFID sensor measurements in a full-metal environment. In Proceedings of the 2013 European Conference on Smart Objects, Systems and Technologies (SmartSysTech), Nuremberg, Germany, 11–12 June 2013.

[215] He, S.; Chan, S. H. G. Wi-Fi Fingerprint-Based Indoor Positioning: Recent Advances and Comparisons. *IEEE Commun. Surv. Tutor.* **2016**, 18, 466-490.

[216] Aguilar-Garcia, A.; Fortes, S.; Barco, R.; Colin, E. Enhancing localization accuracy with multi-antenna UHF RFID fingerprinting. In Proceedings of the 2015 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Banff, AB, 2015; pp. 1-9.

[217] He, S.; Chan, S. H. G.; Yu, L.; Liu, N. Fusing noisy fingerprints with distance bounds for indoor localization. In Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM), Kowloon, Hong Kong, 26 April-1 May 2015; pp. 2506-2514.

[218] Mustika, I. W.; Phimmasean, S. Reorganizing fingerprint information using intersection technique for RFID-based indoor localization system. In Proceedings of the 2014 6th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, 7-8 October 2014; pp. 1-5.

[219] Ge, Y.; Wang, A.; Cheng, J. A spatial scheduling strategy for irregular workplace in shipbuilding. In Proceedings of the 2016 IEEE International Conference on Mechatronics and Automation, Harbin, China, 7-10 August 2016; pp. 12-16.

[220] Pinha, D. C.; de Queiroz, M. H.; Cury, J. E. R. Optimal scheduling of a repair shipyard based on Supervisory Control Theory. In Proceedings of the 2011 IEEE International Conference on Automation Science and Engineering, Trieste, Italy, 24-27 August 2011; pp. 39-44.

[221] Chen, N.; Liu, W. Ship Construction Program of Visual Simulation. In Proceedings of the 2012 Second International Conference on Intelligent System Design and Engineering Application, Sanya, Hainan, 6-7 January 2012; pp. 921-927.

[222] Santos, R.; Botelho, S.; Amaral, M.; Duarte, N.; Espíndola, D. Toogle: A CPS Platform for Equipment Tracking in Shipyards. In Proceedings of the 2014 Symposium on Automation and Computation for Naval, Offshore and Subsea (NAVCOMP), Rio Grande, Brazil, 11-13 March 2014; pp. 5-9.

[223] Choi, S. G.; Ryu, S. H.; Park, I. Y. Development of web-based control and monitoring system for facility in shipbuilding yard. In Proceedings of the 2011

11th International Conference on Control, Automation and Systems, Gyeonggi-do, South Korea, 26-29 October 2011; pp. 815-817.

[224] Kaminski, L.; Kulawiak, M.; Cizmowski, W.; Chybicki, A.; Stepnowski, A.; Orlowski, A. Web-based GIS dedicated for marine environment surveillance and monitoring. In Proceedings of OCEANS 2009-EUROPE, Bremen, Germany, 11-14 May 2009; pp. 1-7.

[225] Tarjan, L.; Senk, I.; Tegeltija, S.; Stankovski, S.; Ostojic, G. A readability analysis for QR code application in a traceability system. *Comput. Electron. Agric.* **2014**, *109*, 1–11.

[226] Zhong, R.Y.; Dai, Q.Y.; Qu, T.; Hu, G.J.; Huang, G.Q. RFID-enabled real-time manufacturing execution system for mass-customization production. *Robot. Comput. Integr. Manuf.* **2013**, *29*, 283–292.

[227] Barro-Torres, S.J.; Fernández-Caramés, T.M.; Pérez-Iglesias, H.J.; Escudero, C.J. Real-time personal protective equipment monitoring system. *Comput. Commun.* **2012**, *36*, 42–50.

[228] Fernández-Caramés, T.M. An intelligent power outlet system for the smart home of the Internet of Things. *Int. J. Distrib. Sensor Netw.* **2015**, *2015*, 1.

[229] Ozdenizci, B.; Coskun, V.; Ok, K. NFC internal: An indoor navigation system. *Sensors* **2015**, *15*, 7571–7595.

[230] Kitazawa, M.; Takahashi, S.; Takahashi, T.B.; Yoshikawa, A.; Terano, T. Improving a cellular manufacturing system through real time-simulation and-measurement. In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; pp. 117–122.

[231] Makki, A.; Siddig, A.; Saad, M.; Cavallaro, J.R.; Bleakley, C.J. Indoor localization using 802.11 time differences of arrival. *IEEE Trans. Instrum. Meas.* **2016**, *65*, 614–623.

[232] Mousa, M.; Zhang, X.; Claudel, C. Flash flood detection in urban cities using ultrasonic and infrared sensors. *IEEE Sens. J.* **2016**, *16*, 7204–7216.

[233] Ijaz, F.; Yang, H.K.; Ahmad, A.W.; Lee, C. Indoor positioning: A review of indoor ultrasonic positioning systems. In Proceedings of the 2013 15th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 27–30 January 2013; pp. 1146–1150.

[234] Alarifi, A.; Al-Salman, A.; Alsaleh, M.; Alnafessah, A.; Al-Hadhrami, S.; Al-Ammar, M.A.; Al-Khalifa, H.S. Ultra wideband indoor positioning technologies: Analysis and recent advances. *Sensors* **2016**, *16*, 707.

[235] Ruan, Q.; Xu, W.; Wang, G. RFID and ZigBee based manufacturing monitoring system. In Proceedings of the 2011 International Conference on Electric Information and Control Engineering (ICEICE), Wuhan, China, 25–27 March 2011; pp. 1672–1675.

[236] Ergeerts, G.; Nikodem, M.; Subotic, D.; Surmacz, T.; Wojciechowski, B.; de Meulenaere, P.; Weyn, M. DASH7 alliance protocol in monitoring applications. In Proceedings of the 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Krakow, Poland, 4–6 November 2015; pp. 623–628.

[237] Belchior, R.; Júnior, D.; Monterio, A. ANT+ medical health kit for older adults. In *Wireless Mobile Communication and Healthcare*; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Berlin/Heidelberg, Germany, 2013; Volume 61, pp. 20–29.

[238] Horvath, P.; Yampolskiy, M.; Koutsoukos, X. Efficient evaluation of wireless real-time control networks. *Sensors* **2015**, *15*, 4134–4153.

[239] Augustin, A.; Yi, J.; Clausen, T.; Townsley, W.M. A study of LoRa: Long range & low power networks for the internet of things. *Sensors* **2016**, *16*, 1466.

[240] Margelis, G.; Piechocki, R.; Kaleshi, D.; Thomas, P. Low Throughput Networks for the IoT: Lessons learned from industrial implementations. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 181–186.

[241] Boukhtouta, A.; Berger, J. Improving in-transit and in-theatre asset visibility of the Canadian Armed Forces supply chain network. In Proceedings of the 2014 International Conference on Advanced Logistics and Transport (ICALT), Hammamet, Tunisia, 1–3 May 2014; pp. 149–154.

[242] B&W Pantex. *Advanced Inventory and Materials Management at Pantex*; White Paper; B&W Pantex: Amarillo, TX, USA, 2011.

[243] Rappaport, T.S. *Wireless Communications: Principles and Practice*, 2nd ed.; Prentice Hall: Upper Saddle River, NJ, USA, 2002.

[244] Grewal, M.H.; Andrews, A.P. *Kalman Filtering: Theory and Practice using Matlab*, 3rd ed.; John Wiley & Sons: Hoboken, NJ, USA, 2008.

[245] Bulten, W.; Rossum, A.C.V.; Haselager, W.F.G. Human SLAM, indoor localisation of devices and users. In Proceedings of the IEEE First International Conference on Internet-of-Things Design and Implementation, Berlin, Germany, 4–8 April 2016; pp. 221–222.

[246] Clerckx, B.; Oestges, C. *MIMO Wireless Networks: Channels, Techniques and Standards for Multi-Antenna, Multi-User and Multi-Cell Systems*, 2nd ed.; Academic Press: Cambridge, MA, USA, 2013.

[247] Fernández, T.M.; Rodas, J; Escudero, C.J.; Iglesia, D.I. Bluetooth sensor network positioning system with dynamic calibration. In Proceedings of the 4th IEEE International Symposium on Wireless Communication Systems, Trondheim, Norway, 16–19 October 2007; pp. 45–49.

[248] Speedway Revolution R420 from Impinj. Available online: http://www.impinj.com/products/readers/speedway-revolution (accessed on 28 February 2017).

[249] A6-UHFLongRange. Available online: http://www.nextpoints.com/es/productos-rfid/item/196-rugged-pda-a6-rfid-uhf.html (accessed on 28 February 2017).

[250] Omni-ID Products. Available online: https://www.omni-id.com/industrial-rfid-tags (accessed on 28 February 2017).

[251] NPR ActiveTrack-2 New Edition. Available online: http://www.nextpoints.com/es/productos-rfid/item/187-npr-active-track-2-new-edition.html (accessed on 28 February 2017).

[252] Active RuggedTag-175S. Available online: http://www.nextpoints.com/es/productos-rfid/item/319-tag-rfid-activo-active-rugged-tag-175s.html (accessed on 28 February 2017).

[253] Mascharka, D.; Manley, E. LIPS: Learning Based Indoor Positioning System using mobile phone-based sensors. In Proceedings of the 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2016; pp. 968–971.

[254] Lim, H.; Kung, L.-C.; Hou, J.C.; Luo, H. Zero-configuration indoor localization over IEEE 802.11 wireless infrastructure. *Wirel. Netw.* **2010**, *16*, 405–420.

[255] Park, J.-G.; Charrow, B.; Curtis, D.; Battat, J.; Minkov, E.; Hicks, J.; Teller, S.; Ledlie, J. Growing an organic indoor location system. In Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services, San Francisco, CA, USA, 15–18 June 2010; pp. 271–284.

[256] Chintalapudi, K.; Padmanabha Iyer, A.; Padmanabhan, V.N. Indoor localization without the pain. In Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking, Chicago, IL, USA, 20–24 September 2010; pp. 173–184.

[257] Goswami, A.; Ortiz, L.E.; Das, S.R. WiGEM: A learning-based approach for indoor localization. In Proceedings of the Seventh Conference on emerging Networking Experiments and Technologies ACM CoNEXT, Tokyo, Japan, 6–9 December 2011; pp. 1–12.

[258] Wu, C.; Yang, Z.; Liu, Y.; Xi, W. WILL: Wireless indoor localization without site survey. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 839–848.

[259] Wang, H.; Sen, S.; Elgohary, A.; Farid, M.; Youssef, M.; Choudhury, R. R. No need to war-drive: Unsupervised indoor localization. In Proceedings of the ACM 18th Annual International Conference on Mobile Computing and Networking (MobiCom 2012), Istambul, Turkey, 22–26 August 2012; pp. 197–210.

[260] Rai, A.; Chintalapudi, K.K.; Padmanabhan, V.N.; Sen, R. Zee: Zero-effort crowdsourcing for indoor localization. In Proceedings of the ACM 18th Annual International Conference on Mobile Computing and Networking (MobiCom 2012), Istambul, Turkey, 22–26 August 2012; pp. 293–304.

[261] Yang, Z.; Wu, C.; Liu, Y. Locating in fingerprint space: Wireless indoor localization with little human intervention. In Proceedings of the ACM 18th Annual International Conference on Mobile Computing and Networking (MobiCom 2012), Istambul, Turkey, 22–26 August 2012; pp. 269–280.

[262] Shen, G.; Chen, Z.; Zhang, P.; Moscibroda, T.; Zhang, Y. Walkie-Markie: Indoor pathway mapping made easy. In Proceedings of the 10th USENIX Conference on Networked Systems Design and Implementation, Berkeley, CA, USA, 2–5 April 2013; pp. 85–98.

[263] Bahl, P.; Padmanabhan, V.N. RADAR: An in-building RF-based user location and tracking system. In Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2000), Piscataway, NJ, USA, 26–30 March 2000; Volume 2, pp. 775–784.

[264] Youssef, M.; Agrawala, A. Handling samples correlation in the horus system. In Proceedings of the Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004), Hong Kong, China, 7–11 March 2004; Volume 2, pp. 1023–1031.

[265] AiRISTA. Available online: https://www.airistaflow.com/hardware/ (accessed on 28 February 2017).

[266] IZat. Available online: https://www.qualcomm.com/products/izat (accessed on 28 February 2017).

[267] Ubisense. Available online: https://ubisense.net/en (accessed on 28 February 2017).

[268] Dart system. Available online: https://www.zebra.com/us/en/solutions/location-solutions/enabling-technologies/dart-uwb.html (accessed on 28 February 2017).

[269] Prieto, J.C.; Jiménez, A.R.; Guevara, J.; Ealo, J.L.; Seco, F.; Roa, J.O.; Ramos, F. Performance evaluation of 3D-LOCUS advanced acoustic LPS. *IEEE Trans. Instrum. Meas.* **2009**, *58*, 2385–2395.

[270] Elpas (Gdsystems). Available online: http://www.gdsystems.com/staff-attack-alarms/elpas/ (accessed on 28 February 2017).

[271] Hightower, J.; Want, R.; Borriello, G. *SpotON: An Indoor 3D Location Sensing Technology Based on RF Signal Strength*; UW CSE 00-02-02 Technical Report; University of Washington: Seattle, WA, USA, 2000.

[272] Topaz Local Positioning (Tadlys). Available online: http://www.tadlys.co.il/pages/Product_content.asp?iGlobalId=2 (accessed on 28 February 2017).

[273] Ni, L.M.; Liu, Y.; Lau, Y.C.; Patil, A.P. LANDMARC: Indoor location sensing using active RFID. *Wirel. Netw.* **2004**, *10*, 701–710.

[274] Yang, P.; Wu, W.; Moniri, M.; Chibelushi, C.C. Efficient object localization using sparsely distributed passive RFID Tags. *IEEE Trans. Ind. Electron.* **2013**, *60*, 5914–5924.

[275] Seco, F.; Plagemann, C.; Jiménez, A.R.; Burgard, W. Improving RFID-based indoor positioning accuracy using Gaussian processes. In Proceedings of the 2010 International Conference on Indoor Positioning and Indoor Navigation, Zurich, Switzerland, 15–17 September 2010; pp. 1–8.

[276] Ladd, A.M.; Bekris, K.E.; Rudys, A.; Kavraki, L.E.; Wallach, D.S. Robotics-based location sensing using wireless ethernet. *Wirel. Netw.* **2005**, *11*, 189–204.

[277] Prasithsangaree, P.; Krishnamurthy, P.; Chrysanthis, P. On indoor position location with wireless LANs. In Proceedings of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Lisbon, Portugal, 15–18 September 2002; pp. 720–724.

[278] Luoh, L. ZigBee-based intelligent indoor positioning system soft computing. *Soft Comput.* **2014**, *18*, 443–456.

[279] Gwon, Y.; Jain, R. Error characteristics and calibration-free techniques for wireless LAN-based location estimation. In Proceedings of the Second International Workshop on Mobility Management & Wireless Access Protocols, Philadelphia, PA, USA, 1 October 2004; pp. 2–9.

[280] Faragher, R.; Harle, R. Location fingerprinting with bluetooth low energy beacons. *IEEE J. Sel. Areas Commun.* **2015**, *33*, 2418–2428.

[281] Otsason, V.; Varshavsky, A.; LaMarca, A.; de Lara, E. Accurate GSM indoor localization. *UbiComp 2005: Ubiquitous Computing*; Lecture Notes Computer Science; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3660, pp. 141–158.

[282] Optotrak Certus System. Available online: http://www.ndigital.com/msci/products/optotrak-certus/ (accessed on 28 February 2017).

[283] Aitenbichler, E.; Mühlhäuser, M. An IR local positioning system for smart items and devices. In Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems Workshops (IWSAWC03), Providence, RI, USA, 19–22 May 2003.

[284] Bat System. Available online: http://www.cl.cam.ac.uk/research/dtg/attarchive/bat/ (accessed on 28 February 2017).

[285] Priyantha, N.B. The Cricket Indoor Location System. PhD Thesis, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, 2005.

[286] Sonitor. Available online: http://sonitor.com/ (accessed on 28 February 2017).

[287] King, T.; Kopf, S.; Haenselmann, T.; Lubberger, C.; Effelsberg, W. COMPASS: A probabilistic indoor positioning system based on 802.11 and digital compasses. In Proceedings of the First ACM International Workshop on Wireless Network Testbeds, Experimental evaluation and CHaracterization (WiN-TECH), Los Angeles, CA, USA, 29 September 2006; pp. 34–40.

[288] An, X.; Wang, J.; Prasad, R.V.; Niemegeers, I.G.M.M. OPT: Online person tracking system for context-awareness in wireless personal network. In Proceedings of the 2nd International Workshop on Multi-hop Ad Hoc Networks: From Theory to Reality (REALMAN '06), Florence, Italy, 26 May 2006; pp. 47–54.

[289] Brumitt, B.; Meyers, B.; Krumm, J.; Kern, A.; Shafer, S. Easyliving: Technologies for intelligent environments. In Proceedings of the 2nd International Symposium on Handheld and Ubiquitous Computing, Bristol, UK, 25–27 September 2000; pp. 12–29.

[290] Lopes, C.V.; Haghighat, A.; Mandal, A.; Givargis, T.; Baldi, P. Localization of off-the-shelf mobile devices using audible sound: Architectures, protocols and performance assessment. *ACM SIGMOBILE Mob. Comput. Commun. Rev.* **2006**, *10*, 2.

Anexo A

Resumen de la tesis

In accordance with the Regulations of the Ph.D. studies passed by the Governing Council of the University of A Coruña at its meeting of July 17^{th} 2012, a summary in Spanish of this thesis is reproduced below.

Los sistemas de transporte fiables, la defensa, la seguridad pública y el control de los activos principales de las empresas son esenciales para la sociedad moderna. El terrorismo, los conflictos, los incidentes y los desastres naturales están presentes en este momento en algún lugar del mundo. Como consecuencia, el término misión crítica es común en las discusiones de seguridad pública con numerosas definiciones ofrecidas por múltiples fuentes. Existen referencias a escenarios de misión crítica, situaciones, soluciones, servicios, operaciones, infraestructuras, usuarios, profesiones, información, entre otras. En estos escenarios, un fracaso de la misión podría poner en peligro vidas humanas y poner en riesgo activos cuyo deterioro o pérdida podrían perjudicar seriamente a la sociedad o a los resultados de una empresa. Incluso pequeñas degradaciones en las comunicaciones que soportan la misión podrían tener consecuencias importantes y posiblemente nefastas. Los escenarios de misión crítica juegan un papel de creciente importancia en la sociedad, tanto aumentando la productividad de las empresas como directamente relacionados con el mantenimiento de la seguridad nacional.

Por tanto, los usuarios involucrados en una misión crítica son los responsables de la salud, la seguridad y el bienestar de los ciudadanos. El término PPDR (*Public Protection & Disaster Relief*) incluye seguridad pública (policía, bomberos/rescate y servicios médicos de emergencia), las agencias gubernamentales y de la defensa civil, los servicios públicos (electricidad, petróleo y gas, el agua, la generación de energía) y los sistemas de transporte inteligentes, incluyendo tráfico por carretera, puertos, trenes... los cuales forman parte de la infraestructura crítica nacional.

Las comunicaciones de misión crítica incluyen hardware, software, así como los recursos de comunicación, incorporando la suficiente capacidad de espectro de frecuencias radio para transmitir y compartir información entre los usuarios de campo y los

centros de mando. Las organizaciones y grupos de interés involucrados en misiones críticas (gobiernos, reguladores, usuarios, proveedores y operadores) desean utilizar los sistemas de comunicaciones móviles más modernos e innovadores y, sin embargo, necesitan soluciones que son muy diferentes a las comerciales y civiles. Además, en la provisión de los servicios necesarios interaccionan aspectos técnicos, legales, económicos y regulatorios.

Debido al gran número de escenarios de misión crítica y a su creciente complejidad, en el aspecto técnico es necesario recurrir a la evolución continua de las tecnologías de la información, los paradigmas de *Internet of Things* (IoT), *Cyber-Physical Systems* (CPS), tecnologías de comunicaciones inalámbricas como *Radio Frequency IDentification* (RFID) o comunicaciones de banda ancha 4G / 5G como *Worldwide Interoperability for Microwave Access* (WiMAX), *Long-Term Evolution* (LTE) y *Wireless Local Area Network* (WLAN). Estas tecnologías podrían ser utilizadas para servicios de misión crítica con el adecuado marco legal, regulatorio y contractual pero sólo si sus requisitos operativos y técnicos se cumplen totalmente.

A día de hoy, las redes de seguridad pública están adaptadas a las necesidades de misión crítica incluyendo mayoritariamente servicios que han sido tradicionalmente orientados a voz, con redes dedicadas con espectro exclusivo. Sin embargo, la banda ancha está emergiendo rápidamente como una necesidad para proporcionar nuevos servicios que sólo se puede obtener hoy en día a través de las redes civiles de misión no crítica. La tecnología comercial aún no está lista para soportar banda ancha de misión crítica de datos o voz. Esta situación será temporal durante algunos años y esta transición plantea cuestiones tales como: en qué medida la banda ancha puede usarse en escenarios de misión crítica; puede proporcionar el nivel necesario de disponibilidad, priorización, seguridad, eficiencia, fiabilidad, resistencia, escalabilidad, interoperabilidad, calidad de servicio y cobertura; las tecnologías emergentes en el ámbito civil pueden dar lugar a nuevos servicios, de qué tipo y cómo se implementarían en este tipo de escenarios. El objetivo de esta tesis es resolver estas cuestiones y analizar el potencial de las tecnologías citadas para optimizar tanto su diseño como su implementación en escenarios de misión crítica.

Considerando además que la distinción entre misión crítica y no crítica depende del contexto, y que puede cambiar de forma inesperada, lo más adecuado es estudiar los requisitos operativos y técnicos de los sectores concretos en situaciones específicas. Con esto en mente, esta tesis ha seleccionado tres líneas de investigación en tres sectores diferentes: transporte, defensa y seguridad pública, y la industria de la construcción naval. Como conclusión, en esta tesis se investiga el pasado, el presente y el futuro de las comunicaciones y los paradigmas IoT y CPS en sectores relevantes de misión crítica, analizando el papel potencial que podrían desempeñar para garantizar la

misión. No obstante, es importante señalar que los hallazgos, resultados y metodologías presentadas en esta tesis también pueden servir para optimizar e innovar en sistemas no necesariamente de misión crítica.

A.1 Transporte

La primera línea de investigación de esta tesis se dedica al análisis del sector del transporte, concretamente el ferroviario. En este sector, un incidente o accidente puede tener un impacto significativo. Por otro lado, las interrupciones y retrasos en el servicio causan un detrimento económico si muchas personas se ven afectadas o la duración es larga. En particular, el sector ferroviario puede beneficiarse de los enlaces inalámbricos en su servicio de formas que todavía se están empezando a explorar. Es importante tener en cuenta que, para los usuarios de misión crítica existentes, es absolutamente necesaria una hoja de ruta de migración hacia la banda ancha móvil con continuidad del servicio.

Teniendo en cuenta estas premisas, esta línea analiza el progreso de las tecnologías de comunicaciones en el dominio ferroviario desde la implantación de GSM-R. Además, se describen las motivaciones de las diferentes alternativas a lo largo del tiempo y la evolución de los requisitos ferroviarios con sus principales especificaciones y recomendaciones. El objetivo de este trabajo es analizar la posible contribución de LTE para proporcionar características adicionales que GSM-R nunca podría soportar. Los servicios que podría mejorar LTE son las comuniciones de voz punto a punto y punto-multipunto, los servicios de proximidad y los basados en localización, las llamadas *push-to-talk* y las de emergencia, la gestión de prioridad y el soporte IP multi-servicio. Asimismo, se presenta la capacidad de la IoT industrial y el paradigma de Internet de los Trenes para revolucionar la industria y afrontar los desafíos actuales. Por ejemplo, se describen los principales desarrollos industriales actuales, exponiendo las posibilidades de los principales servicios que IoT permitirá ofrecer a corto y medio plazo: mantenimiento predictivo, infraestructuras inteligentes (monitorización avanzada de los activos, sistemas de video-vigilancia y control de las operaciones), control de la información tanto relativa al pasajero como a la carga, eficiencia energética y avances en los sistemas de control de los trenes.

Otro aspecto crítico en el sector del transporte son las tarjetas de identificación y acceso. Su función primaria actualmente es el pago de los distintos medios de transporte (e.g., tren, metro, tranvía y bus) incluyendo también funcionalidades adicionales relativas al turismo o servicios al ciudadano. En este contexto, se analiza su seguridad y la privacidad de sus datos proporcionando además una revisión detallada de las vulnerabilidades más comunes encontradas en sistemas IoT basados en RFID, incluyendo asimismo los últimos

ataques descritos en la literatura. La tecnología RFID es extremadamente popular hoy en día en múltiples aplicaciones pero es fácil encontrar sistemas comerciales con fallos de seguridad que permiten clonar tarjetas, emular las comunicaciones, acceder a ciertos servicios u obtener y alterar información personal. Con el objetivo de incrementar su seguridad, se presenta una metodología innovadora que facilita la detección de vulnerabilidades y permite mitigar los posibles ataques.

Además, tras analizar las últimas herramientas de seguridad RFID, se aplica la metodología propuesta a través de una de ellas (Proxmark 3) para validarla. Por lo tanto, se realizan pruebas en un escenario real en donde las etiquetas se utilizan comúnmente para el acceso y el pago de servicios. En tales sistemas es posible extraer información, capturar las comunicaciones lector-etiqueta para realizar ataques *Man-in-the-Middle* (MitM) y emular tanto lectores como etiquetas.

Durante la investigación, se ha observado que aunque muchas aplicaciones pueden hacer uso de medidas avanzadas de seguridad, algunos desarrolladores han adoptado la tecnología sin tener en cuenta estos mecanismos. En el caso de la etiqueta de transporte analizada, su seguridad podría mejorarse mediante la adición de una capa de seguridad más alta (por ejemplo, cifrar datos internos), habilitar algunos de los protocolos de seguridad ya existentes o simplemente reemplazarla por una versión más segura. De esta forma, se concluye que la metodología propuesta demuestra ser útil para la auditoría de la seguridad y la ingeniería inversa de comunicaciones RFID en aplicaciones de transporte. Igualmente, la metodología podría ayudar a los desarrolladores de aplicaciones IoT a realizar auditorías y determinar el nivel de seguridad de un sistema RFID antes de pasar de un entorno de prueba a un escenario de misión crítica. Cabe señalar que, si bien sólo se ha detallado cómo fomentar la seguridad de las comunicaciones RFID en el transporte, la metodología puede aplicarse a cualquier otro protocolo de comunicaciones RFID en cualquier otro sector.

A.2 Defensa y seguridad pública

La segunda línea de investigación está impulsada por las nuevas necesidades operativas y los retos derivados de los despliegues militares modernos. Los subsistemas de distribución de datos militares del ejército de tierra presentan gran similitud con las tecnologías inalámbricas comerciales en términos de alcance de las comunicaciones, los servicios y las capacidades de la red de apoyo. El objetivo de esta investigación es analizar las ventajas estratégicas de las tecnologías de banda ancha 4G masivamente desplegadas en escenarios civiles. Mediante el uso de una metodología propuesta basada en escenarios, se diseña un nuevo Sistema de Comunicación Inalámbrica de Banda Ancha Militar (MBWCS)

que permitirá aumentar la interoperabilidad entre las redes actuales verificando tanto las recomendaciones de la OTAN como las necesidades operacionales nacionales.

El análisis realizado es capaz de determinar las tecnologías necesarias a medio y largo plazo para cumplir con los requisitos operativos del ejército terrestre y los equipos militares comerciales de última generación que cubren tales necesidades. El primer paso en la metodología utilizada es la definición de los escenarios de la OTAN. Posteriormente, se realiza un análisis de los requisitos operativos. En un segundo paso, se derivan sus correspondientes requisitos técnicos y se utilizan como entrada para el análisis de aplicabilidad de las tecnologías 4G LTE, WiMAX y Wi-Fi. Para este trabajo, fue necesario caracterizar los requisitos de implementación técnica de los estándares 4G, y analizar capacidades, aptitudes y desafíos al desplegar una red táctica. También se identificaron y evaluaron las modificaciones y las técnicas necesarias para los tres estándares. El estudio confirmó que el desarrollo de un MBWCS innovador sería claramente optimizado si se tomaran como base las tecnologías 4G. Igualmente, debido a la velocidad en la evolución de los estándares, los sistemas 5G deben revisarse bajo la metodología presentada para ver el grado de cumplimiento de los requisitos.

En el marco de esta línea de investigación, por otro lado, se analiza el gran potencial de aplicación de las tecnologías IoT (en concreto, aplicaciones basadas en datos o sistemas de automatización integrados y sistemas adaptativos inteligentes) para revolucionar la guerra moderna y proporcionar beneficios similares a los obtenidos en la industria. Para ello, se identificaron escenarios en los que la defensa y la seguridad pública podrían aprovechar mejor las capacidades de IoT comercial para ofrecer una mayor capacidad de supervivencia al combatiente o los servicios de emergencia, a la vez que reduce los costes y aumenta la eficiencia y efectividad de las operaciones. Para llevar a cabo el estudio, se analizaron diferentes escenarios relevantes tales como: *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance* (C4ISR), sistemas de control de fuego, logística (gestión de flotas y suministros individuales), operaciones en ciudades inteligentes, sensado personal y entrenamiento, gestión de la energía o vigilancia, entre otras.

Tras el análisis de los requisitos operativos y técnicos, como resultado del estudio, se concluye que la IoT comercial e industrial todavía debe confrontar muchos retos, como la estandarización, la escalabilidad, la interoperabilidad y la seguridad. Tres diferencias principales sobresalen en estos escenarios: la complejidad de los despliegues, las limitaciones de recursos (básicamente las relacionadas con el consumo de energía y las comunicaciones) y el uso de arquitecturas centralizadas basadas en la nube. Las transiciones orgánicas como la gestión de la cadena de suministro y la logística migrarán de forma natural a entornos de misión crítica. Pero, más allá de las primeras innovaciones militares usando IoT, cubrir complejos campos de batalla requerirá avances adicionales

de investigación para abordar las demandas específicas. Además de abordar varios desafíos técnicos, esta tesis también identifica áreas vitales de investigación en el periodo 2017-2020.

A.3 Industria 4.0: construcción naval

La última línea de investigación presenta el concepto de Astillero 4.0 como una traslación de los principios de la Industria 4.0 al sector naval. En concreto, Navantia, uno de los diez astilleros más grandes del mundo, está llevando a cabo esta transformación conjuntamente con la Universidade da Coruña en el marco de una unidad mixta de investigación. La Industria 4.0 plantea el uso de los últimos avances tecnológicos (por ejemplo, en IoT, robótica o realidad aumentada) con el objetivo de aumentar la eficiencia e integración de los procesos para optimizar su ciclo de vida.

La construcción de un buque en un astillero es una tarea compleja en la que intervienen multitud de procesos. Uno de ellos es la fabricación de tubos, los cuales constituyen una parte fundamental de un buque. Los tubos representan el 'sistema circulatorio' del buque transportando combustible y refrigerante para los motores, el agua potable para consumo, conduciendo los residuos a las plantas de tratamiento, así como otros muchos servicios. En concreto, dependiendo del tipo, es habitual que un buque cuente con entre 15,000 y 40,000 tubos, los cuales difieren en su tamaño, material, y en los accesorios que los constituyen. Debido a esta diversidad y a la importancia de los tubos, el control de su trazabilidad y de los procesos a los que son sometidos constituye un tema de alto interés para Navantia.

Esta necesidad de control de los tubos puede cubrirse mediante un CPS, en el que la información que pueden proporcionar tubos inteligentes interconectados permite acelerar su localización facilitando los procesos de construcción, instalación y mantenimiento. El CPS propuesto consiste en una red de balizas que recoge continuamente información sobre la ubicación de las tuberías que, además, realiza una estimación de su posición mediante algoritmos matemáticos y cuyo diseño permite a los astilleros hacer un mejor uso de las mismas. Con este sistema funcionando, el desarrollo de aplicaciones innovadoras relacionadas con la monitorización de elementos diferentes a las tuberías (por ejemplo, los dispositivos portátiles para operadores, herramientas, máquinas compartidas) es sencilla. Por lo tanto, nuevas aplicaciones permitirán al Astillero 4.0 un consumo de energía más inteligente, una logística óptima de entrada/salida y de almacenamiento de información, una mayor seguridad laboral, y una optimización del rendimiento en tiempo real.

Un aspecto relevante en la construcción del CPS ha sido conocer con detalle cómo funciona un taller de tuberías de un astillero y cuáles son los requisitos para construir

un sistema de tuberías inteligentes. Tras un estudio del estado del arte, se analizó la viabilidad de las tecnologías de identificación disponibles comparando de forma detallada las prestaciones de más de quince tecnologías. Posteriormente, una vez realizada la definición de los requisitos operativos y técnicos, se seleccionó UHF RFID como la tecnología que mejor se adapta a las necesidades de un taller de tuberos.

La arquitectura del sistema consta de diversos módulos que permiten adquirir los niveles de *Received Signal Strength* (RSS) transmitidos por las etiquetas electrónicas adheridas a los tubos y realizar su procesado para estimar la ubicación de estos. Igualmente, el sistema consta de un módulo de *Business Intelligence* para la detección de eventos, de un módulo para conectarse a sistemas externos (SAP y MES), y de un módulo para la visualización de toda la información relevante.

Una vez seleccionadas las tecnologías, se adquirió el hardware necesario para llevar a cabo pruebas en un entorno real. Dicho hardware incluyó lectores de sobremesa para etiquetas RFID activas y pasivas, y lectores móviles UHF. Además, se seleccionaron un amplio rango de etiquetas pasivas y activas que, gracias a su diversa naturaleza y objetivos, permitieron una correcta validación de las tecnologías. Las etiquetas elegidas tienen en común su tolerancia a entornos con una alta presencia de metales. Igualmente, todas ellas tienen una buena resistencia a golpes, presiones externas y factores medioambientales (e.g., ácidos, salinidad, alta humedad, ...).

Posteriormente, se indica cómo construir un sistema de posicionamiento desde cero en un entorno tan hóstil como un astillero, mostrándose un ejemplo de su implementación y su arquitectura. A través de múltiples pruebas se confirmó que el sistema RFID UHF activo permite la monitorización constante de las etiquetas en áreas amplias. Además, se propone el uso de técnicas de diversidad espacial y el filtrado de Kalman para estabilizar los valores de la señal recibida.

El sistema propuesto facilita la visualización en tiempo real de la ubicación de los tubos del taller. Una vez instalado el sistema software y hardware, los resultados obtenidos pueden verse por los operarios gracias a un interfaz web que puede ser accedido a través de cualquier dispositivo con un navegador (i.e., desde PCs, Mac, smartphones, tablets). Considerando que se visualizan múltiples tubos mientras se mueven a través del taller, se puede usar un filtro para mostrar un tubo específico o un subconjunto que cumple ciertos criterios. Adicionalmente, los operarios pueden hacer zoom en el mapa del taller para observar áreas específicas o acceder a información específica de los tubos (i.e., identificador del tubo, área o material).

Como punto de partida de un sistema de *data mining* que analice el recorrido de un tubo a lo largo de su vida en el taller, se ha implementado también un módulo de seguimiento. Este módulo permite conocer en tiempo real la posición en la que el sistema sitúa al tubo pero, a diferencia del módulo de visualización, su objetivo es generar una

traza del estado del tubo a lo largo del tiempo. Además, se han implementado cálculos que permiten conocer el error cometido por el sistema. Por otro lado, el módulo de *Business Intelligence* desarrollado es actualmente capaz de monitorizar constantemente la posición de los tubos y determinar cuándo se produce un cambio de una zona a otra. Este módulo ha sido verificado in-situ en el taller y se ha comprobado su perfecto funcionamiento que, obviamente, se ve condicionado por la precisión del sistema para ofrecer estimaciones sobre la ubicación. En el momento en el que un tubo cambia de área, se muestra un pop-up en la parte derecha de la pantalla que indica el evento. Este sistema representa tan sólo un ejemplo de las funcionalidades que aportaría un sistema de posicionamiento de los tubos que automatice las tareas del taller. Con los datos adecuados, dicho sistema sería capaz de ofrecer eventos relacionados con la ubicación concreta, y obtener métricas sobre el tiempo de procesado real por tubo, o de determinar si un tubo sigue la ruta adecuada en el taller en función de su tipología. En este sentido, las posibilidades que ofrece el sistema desarrollado suponen una fuente valiosa de datos de cara a optimizar los procesos del taller de tuberos de Navantia.

A.4 Contribuciones

Las principales contribuciones originales derivadas de esta tesis pueden resumirse con los siguientes puntos:

- Análisis del estado del arte de IoT, CPS y las comunicaciones inalámbricas en entornos de misión crítica como el transporte, la defensa y la industria de construcción naval.

- Estudio de las características específicas de las comunicaciones ferroviarias. Se introducen tanto los requisitos operativos como los servicios necesarios. Se analiza la viabilidad de LTE y la IoT industrial para dar soporte a estos servicios.

- Revisión de las vulnerabilidades más comunes y los últimos ataques en sistemas IoT que utilicen la tecnología RFID. Formulación de una metodología para auditar la seguridad y hacer ingeniería inversa de etiquetas comerciales RFID en aplicaciones de IoT. Evaluación de la seguridad de una etiqueta de transporte usada en la actualidad mediante las herramientas de seguridad RFID más recientes (Proxmark 3) y la metodología propuesta.

- Análisis y definición de un sistema de comunicación militar inalámbrico de banda ancha (MBWCS) basado en las tecnologías de comunicación 4G WiMAX, LTE y Wi-Fi.

- Estudio del potencial del paradigma IoT para revolucionar la guerra moderna. Identificación de escenarios en los que la defensa y la seguridad pública podrían aprovechar las capacidades de la IoT industrial para ofrecer una mayor capacidad de supervivencia al combatiente aumentando la eficiencia y eficacia de las operaciones. Análisis crítico de las capacidades operativas más relevantes (seguridad, robustez, topología de red, interoperabilidad, entre otras), definición de los principales requisitos tácticos y arquitecturas, y examen de las deficiencias de los sistemas IoT existentes en los escenarios de defensa y de seguridad pública, incluyendo la revisión de las tecnologías emergentes civiles actuales.

- Definición del concepto de Astillero 4.0 como un astillero construido sobre la aplicación de los principios de la Industria 4.0. Descripción del funcionamiento de un taller de tuberías de un astillero y los requisitos operativos y técnicos necesarios para construir un sistema de tuberías inteligentes.

- Diseño e implementación de un sistema de posicionamiento en un entorno hóstil como lo es un astillero. Debe señalarse que no se ha encontrado en la literatura ningún análisis práctico sobre la aplicación de la tecnología RFID en ningún escenario similar.

- Aplicación de técnicas de diversidad espacial para estabilizar los valores de señal recibida en sistemas RFID. Evaluación de la monitorización en tiempo real del CPS propuesto mediante simulaciones y mediciones.