RFID Solutions Evaluation in Industrial Container Access Control

TIAGO DUQUE LEITE VIEIRA DA SILVA
(Licenciado)

Dissertação para obtenção do grau de Mestre em Engenharia de Eletrónica e Telecomunicações, no Perfil de Telecomunicações

Orientador:

Doutor António João Nunes Serrador

Júri:

Presidente: Doutor Vitor Manuel de Oliveira Fialho

Vogais:

Doutor Nuno Miguel Soares Datia
Doutor António João Nunes Serrador

Novembro de 2025

RFID Solutions Evaluation in Industrial Container Access Control

TIAGO DUQUE LEITE VIEIRA DA SILVA

(Licenciado)

Dissertação para obtenção do grau de Mestre em Engenharia de Eletrónica e Telecomunicações, no Perfil de Telecomunicações

Orientador:

Doutor António João Nunes Serrador, ISEL

Júri:

Presidente: Doutor Vitor Manuel de Oliveira Fialho, ISEL

Vogais:

Doutor Nuno Miguel Soares Datia, ISEL
Doutor António João Nunes Serrador, ISEL

Novembro de 2025

Acknowledgements

First, I would like to thank my supervisor Prof. António Serrador for all the support in writing this thesis, as well as all the memorable academic experiences I've had over the last few years.

I wish to thank the Profs. António Couto Pinto, Fernando Azevedo, Helena Ramos, Pedro Vieira, Manuel Vieira, Vítor Costa and José Rocha for helping me grow both academically and personally during my university years at ISEL.

Acknowledgement also goes to all my classmates for helping me in several ways and for growing personally, academically and professionally along with me all these years. Thank you for the team spirit and the collaborative and stimulating environment we have created. It has been a privilege to learn alongside you.

And last but certainly not least, I would like to express my deepest love and gratitude to my family, who taught me that life's greatest achievements are built on hard work, humility, sacrifice, courage and persistence. Thank you for all your love, support and encouragement. Thank you for being my anchor in times of doubt and my greatest joy in times of achievement. This milestone is as much yours as it is mine.

Statement of integrity

I declare that this project work is the result of my personal and independent research. Its content is original, and all sources listed in the bibliographic references were consulted and are duly mentioned in the text. I further declare that all scientific and technical references relevant to the development of the work are duly cited and included in the bibliographic references.

The author

Assinado por: Tiago Duque Leite Vieira da Silva
Num. de Identificação: BI15382857
Data: 15-12-2025 15:11:09 +00:00

CHAVE MÓVEL

Resumo

Identificar e registar o fluxo de contentores de resíduos industriais através dos pontos de acesso pode representar um desafio significativo em ambientes industriais. Os métodos de registo manual podem levar a falhas de registo que representam riscos para uma empresa, particularmente para a segurança dos ativos e a eficiência operacional. Assim, a identificação da passagem de contentores pelos portões da instalação é essencial para reforçar as medidas de segurança e otimizar a gestão operacional em ambientes industriais.

Este trabalho investiga a aplicação da tecnologia RFID (Radio Frequency IDentification) passiva para enfrentar esses desafios. Foi desenvolvida uma arquitetura piloto, o hardware mais adequado foi selecionado e testado, e o sistema foi instalado numa empresa de gestão de resíduos, com o apoio de um serviço de fundo para processamento e registo de dados de eventos de etiquetas.

O sistema foi avaliado em testes de campo com vários cenários de passagem. As etiquetas RFID passivas foram instaladas nos contentores da empresa e monitorizadas nas suas passagens pelo portão. Foram analisadas as zonas de leitura e a qualidade da deteção pelas antenas. Por fim, avaliou-se o desempenho do middleware na interpretação dos eventos registados.

Os resultados mostram que as etiquetas rígidas passivas utilizadas no projeto melhoram significativamente o seu desempenho aplicadas numa superfície metálica, aumentando a sua capacidade de deteção de 64% para 100%. Concluiu-se também que uma empresa pode beneficiar significativamente em termos financeiros como resultado da melhoria da gestão operacional e do efeito dissuasor sobre o furto.

Palavras-chave: RFID, IoT, gestão de resíduos, controlo de acessos, sistemas de informação.

Abstract

Identifying and recording the flow of industrial waste containers through access points can pose significant challenges in industrial environments. Manual registration methods can lead to registration failures that pose risks for a company, particularly for the security of assets and operational efficiency. Thus, the identification of container crossings through the facility's gateways is essential for reinforcing security measures and optimising operational management in industrial environments.

This work investigates the application of passive RFID (Radio Frequency IDentification) technology to address these challenges. A pilot architecture was developed, the most suitable hardware was selected and tested, and the system was installed in a waste management company, supported by a background service for processing and recording tag event data.

The system was tested in real conditions with various crossing scenarios. RFID tags were installed on the company's containers, and their passages through the gateway were monitored. Detection quality and middleware performance were evaluated through transaction statistics.

The results show that the passive rigid tags used in the project significantly improve their performance when they have a metal background, increasing their detection capacity from 64% to 100%. It was also concluded that a company can benefit significantly in financial terms as a result of improved operational management and the deterrent effect on theft.

Keywords: RFID, IoT, waste management, access control, information systems.

Table of Contents

List of Figures

List of Tables

List of Equations

List of Symbols

Parameter	Symbol	Unit
Transmitted power	P_t	dBm
Received power	P_r	dBm
Transmit antenna gain	G_t	dBi
Receive antenna gain	G_r	dBi
Free space propagation distance	d	m
Hardware Losses	L	dB
Wavelength	λ	m
Speed of light	c	m/s
Frequency	f	MHz
Partial free space loss	PL	dB
Total free space losses	PL_{total}	dB
Fraunhofer distance	d_f	m
Antenna's largest physical linear dimension	D	m
Modulation Index	m	-
Losses due to ASK modulation	κ	dB
Power loss due to reflection	Γ	dB
Total attenuation on coaxial cables	Att_{coax}	dB
Coaxial cable length	l	m
Polarization Loss Factor	PLF	-
Tag antenna gain	G_{tag}	dBim

Parameter	**Symbol**	**Unit**
Fixed reader sensitivity	P_{sens}	dBm
Fixed reader transmitting power	P_{tx}	dBm
Fixed reader received power	P_{rx}	dBm
Fixed antenna transmission gain	G_{tx}	dBi
Fixed antenna receiving gain	G_{rx}	dBi
Total power losses	L_{total}	dB

List of Acronyms

ACL	Access Control List
AI	Artificial Intelligence
AIDC	Automatic Identification and Data Capture
ANPR	Automatic Number Plate Recognition
API	Application Programming Interface
ASK	Amplitude Shift Keying
BLE	Bluetooth Low Energy
BPM	Business Process Management
CAPEX	Capital Expenditures
CPS	Cyber-Physical Systems
CW	Continuous Wave
EMEA	Europe, Middle East and Africa
EMI	Electromagnetic Interference
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FTBR	Front-to-Back Ratio
FSPL	Free-Space Path Loss
FSPM	Free Space Propagation Model
GPS	Global Positioning System
HF	High Frequency
HID Global	Hughes Identification Devices Global
HPBW	Half-Power Beam Width
IC	Integrated Circuit
IFF	Identify Friend or Foe
IoT	Internet of Things
IP68	Ingress Protection 6-8

JSON	JavaScript Object Notation
LF	Low Frequency
M2M	Machine to Machine
MQTT	Message Queuing Telemetry Transport
OCR	Optical Container Recognition
OPEX	Operational Expenditures
PLF	Polarization Loss Factor
PSK	Phase Shift Keying
QoS	Quality of Service
QR Code	Quick Response Code
RFID	Radio-Frequency Identification
SHF	Super High Frequency
SLF4J	Simple Logging Facade for Java
TAPA	Transported Asset Protection Association
UHF	Ultra-High Frequency
UML	Unified Modeling Language
VDC	Volts of Direct Current
VM	Virtual Machine
VSWR	Voltage Standing Wave Ratio
Wi-Fi	Wireless Fidelity

1

Introduction

Industrial waste management represents a growing challenge for companies and entities responsible for sustainability and compliance with environmental standards [1]. Efficient control of waste flows not only promotes the safety of a company's assets, but also optimizes logistics processes and reduces operating costs, ultimately contributing to environmental preservation. In this context, automatic identification technologies have taken on a fundamental role, with RFID (Radio Frequency Identification) standing out as a versatile and effective solution.

RFID technology has been evolving since the mid-20th century, initially with military and logistics tracking applications, until it became a widely used tool in areas such as inventory management, access control, transportation, and healthcare. These topics are explored in more depth in 2.1 (Historical Context). In particular, passive UHF (Ultra High Frequency) RFID systems offer significant advantages, such as low cost per tag, high reading capability, and the ability to monitor multiple objects in real time, making them particularly suitable for industrial environments.

On the one hand, it has been demonstrated that fraud in industrial environments is a reality and that access control technologies are essential in preventing fraud. On the other hand, a good industrial access control method promotes better operational efficiency of a company's assets. This topic is explored in more depth in sections 2.4.2 and 5.3 (Case Studies and Financial Analysis Model, respectively).

As stated by [2], cargo theft poses the greatest risk to worldwide supply chains. According to a European Parliament report, cargo-related crime in Europe results in annual losses exceeding €8.2 billion for businesses. In 2020, TAPA (Transported Asset Protection Associ-

ation) recorded cargo theft incidents across 56 countries in the EMEA (Europe, Middle East and Africa) region, with major thefts averaging losses of €529,348 per incident. A joint study by TAPA and 12 industry associations revealed that German companies alone face over €2.2 billion in losses and damages yearly, stemming from roughly 26,000 truck attacks. In Europe, metals, vehicles, and empty containers rank among the most frequently targeted items by thieves.

According to [3], the most impactful strategies for preventing cargo theft and recovering stolen goods in supply chains include the adoption of advanced security technologies. As further stated by [4], implementing a strong loss prevention plan can significantly lower the risk of cargo theft and lessen its consequences. For logistics companies, this may involve enforcing strict cargo security protocols, adopting advanced tracking systems, and thoroughly vetting drivers and carriers.

Problem statement

Despite its advantages, the application of passive UHF RFID in the specific context of industrial waste container access control still faces technical and operational challenges. These challenges include reading reliability in adverse environments, electromagnetic interference and the need for efficient integration with existing management systems. In this sense, the central question that this research seeks to answer is: How can passive UHF RFID technology be applied efficiently and reliably in the access control of industrial waste containers? This study is justified by the growing need for technological solutions that support the circular economy and ensure the traceability and flow registration of company's assets. The expected contribution will be the demonstration of a system applicable in a real context, with the potential to improve operational efficiency, mitigate human error, and increase safety in the industrial waste management process.

Purpose and objectives of the study

The purpose of this dissertation is to develop and evaluate an access control solution based on passive UHF RFID, applied to industrial waste containers. The specific objectives include: Analysing the functional and technical requirements for implementing an RFID system in this context; Designing and implementing a functional access control prototype; Testing and validating the system's performance in experimental and industrial environments; Evaluating the advantages, limitations, and potential for integrating the solution into waste management systems.

Significance of the study

The main beneficiaries of this study will be industrial companies and waste management entities, which will be able to adopt a technological solution to improve the traceability and security of their processes. For the academic and scientific sector, this work contributes with an applied analysis of passive UHF RFID technology in real industrial scenarios, reinforcing the existing literature and opening perspectives for future research. From a social and environmental point of view, the implementation of effective solutions for the control and monitoring of waste containers contributes to more sustainable practices, in line with sustainable development goals and corporate environmental responsibility.

Scope and limitations of the study

This study focuses specifically on the application of passive UHF RFID technology in industrial waste containers. Other automatic identification technologies and other RFID frequency bands will not be explored in detail. Among the anticipated limitations are the influence of environmental factors, such as electromagnetic phenomena, on antenna performance, the limitation of reading range in practical situations, and the potential complexity of integration with existing information systems.

Methodology and approach

The methodology adopted in this dissertation combines an exploratory aspect with an experimental and applied approach. The work will be developed in five main phases:

1. Literature review and state-of-the-art analysis – survey of the main applications of passive UHF RFID technology, identification of best practices and limitations reported in industrial contexts;

2. Requirements gathering and definition – collection of technical and functional requirements through analysis of the context of use (industrial waste containers), including aspects such as required reading range, environmental conditions, and integration with existing management systems;

3. Development and implementation of the prototype – design of the passive UHF RFID-based access control system, covering the choice of equipment, the design of the communication architecture, and the practical implementation of the prototype;

4. Testing and validation – evaluation of the system in an experimental and/or semi-industrial environment, through the analysis of metrics such as reading rate, reliability, effective range, robustness in different scenarios, and possible interference;

5. Formulation of installation recommendations – based on the results obtained in the tests, practical guidelines were presented for the installation of the UHF RFID system in various

different industrial contexts, in order to maximize reading reliability, reduce interference, and ensure efficient integration with waste management processes.

Data analysis were conducted based on quantitative metrics and qualitative observations, allowing not only to validate the feasibility of the proposed solution, but also to substantiate recommendations applicable in real scenarios. At the same time as this document was being written, a paper on the project was presented and published at ”Inforum 2024: the 15th National Symposium on Informatics”, with the title ”Controlling Industrial Waste Containers Using RFID Tags” [5].

2

State-of-the-Art

When exploring how RFID technology can improve container access control in industrial settings, it's crucial to start with a detailed look at existing research. This initial step helps us understand what's already known and sets the stage for our own contributions to the field. As such, this chapter summarizes the historical development of RFID, current technological principles—including operating bands, readers, and tags—and recent trends in research and practical applications. It also analyses the main limitations and vulnerabilities, framing the challenges that drive the development of more robust and efficient solutions for industrial environments.

2.1 Historical Context

To understand and explore possible applications of RFID technology, it's useful to understand its origins and how it transitioned from a military use only technology to being present in our daily lives in several contexts.

2.1.1 RFID Technology Origins

As stated by [6], RFID technology has its origins in the radar systems used during World War II. These systems enabled the military to detect approaching aircraft, providing critical early warnings. However, accurately identifying whether the aircraft were allies or enemies posed a significant challenge. German pilots discovered that by turning their planes during their return, they could alter the radar signals, enabling ground crews to distinguish between friendly and hostile aircraft. This discovery laid the foundation for passive RFID systems. Subsequently,

the British developed the active IFF (Identify Friend or Foe) system, equipping aircraft with transmitters that responded to radar signals from the ground, confirming their identity as allies.

Modern RFID systems are based on principles similar to those of the IFF system. In 1999, MIT and other organizations began exploring a radio frequency-based automatic identification framework. This system features a reader device that emits radio waves to activate microchips Figure 2.1. In RFID systems, microchips can be passive or active: passive chips lack an internal battery and are powered by the reader's signal, responding through backscatter, while active chips contain their own power source, enabling them to transmit signals independently and reach greater distances. Furthermore, read/write systems not only allow reading the information stored on the chip but also updating it, making the technology highly versatile for applications in logistics, inventory management, and access control.

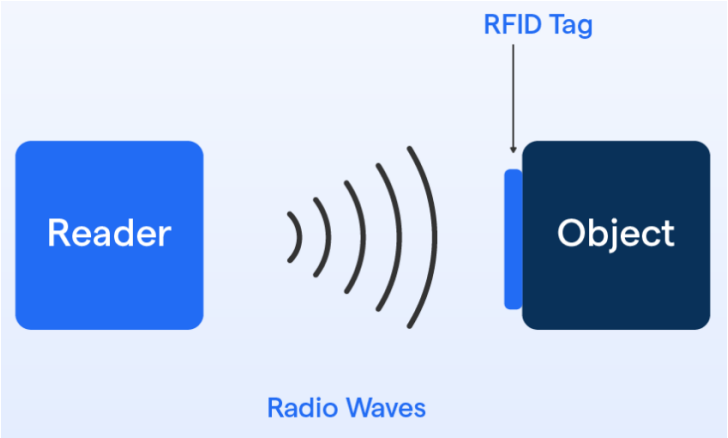


Figure 2.1: Basic RFID passive system (extracted from [7])

2.1.2 Industrial Revolutions

According to advancement of technology introduced new production methods designed to minimize human effort. This transformation in production techniques and technology is referred to as an Industrial Revolution (Figure 2.2). It was characterized by a dramatic rise in production, economic growth, and improved living standards. Technological progress not only boosted the economy but also fostered a wave of innovative thinking.

Industry 4.0 (Table 2.1) is a digital transformation of manufacturing and production, as well as related industries and processes for creating value. It mainly contains CPS (Cyber-Physical Systems), IoT (Internet of Things), and cloud computing but will also rely on smart devices in addition to CPS, IoT, cloud computing, and BPM (Business Process Management) [9]. Instead of looking at individual machines, look at networks of machines.

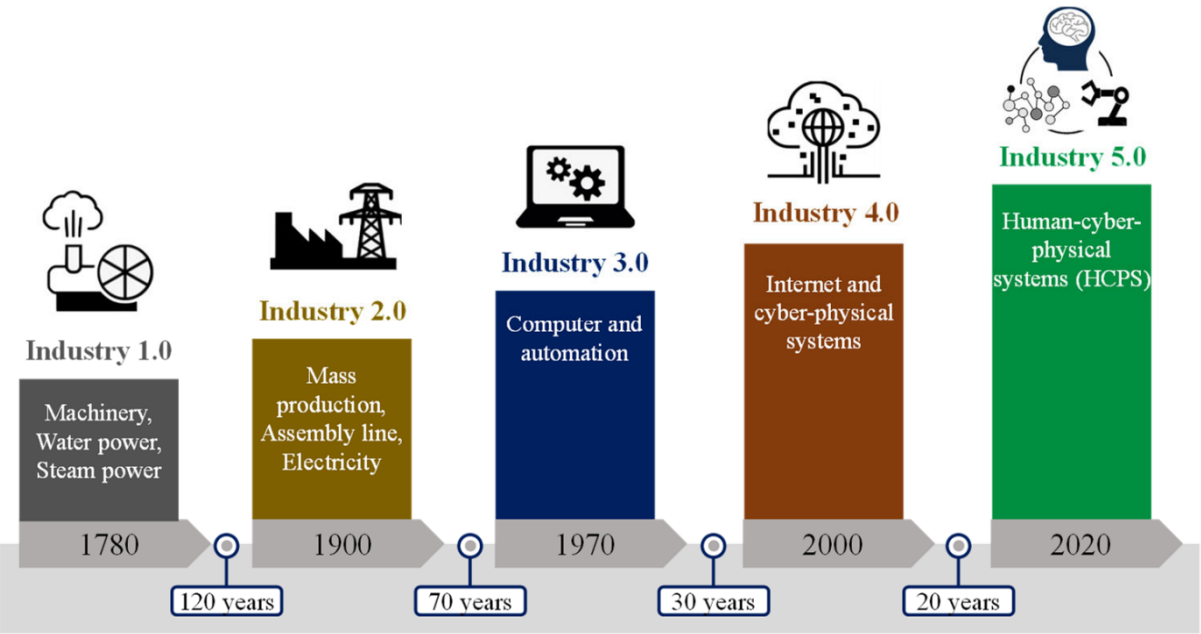


Figure 2.2: Industrial Revolutions (extracted from [8])

Table 2.1: Industrial Revolutions Overview

Industry	Time Period	Focus Area	Challenges
Industry 1.0	18th century	Steam and water plants, iron industries, mining, agriculture	Pollution, long working hours, poor working conditions
Industry 2.0	19th century	Iron, steel, railways, turbines. Telecommunication, petroleum	Costly, reduced the job opportunities
Industry 3.0	20th century	Renewable energy, telecommunication, wireless communication, ICs	E-waste, high power consumption
Industry 4.0	21st century	All production industries with intelligent systems	Risk of Cyber Attacks, long working hours, lack of skills
Industry 5.0	22nd century	Enabling people and machines to work together in all primary and secondary industries	Risk of Cyber Attacks, lack of skilled workers, difficulty in regulation.

2.2 Industrial Access Control

The initial stage of the project's work plan involved reviewing and updating the state of the art in access control technologies. Research was therefore carried out into different industrial access control methods, particularly their applicability to industrial containers. Of all the existing automatic access control methods, the following stand out.

RFID

RFID technology is widely used in the context of vehicle access control in industrial environments. RFID tags are placed on vehicles/containers and RFID readers and antennas are installed at strategic entry and exit points. When the vehicle approaches, the reader captures the information from the tag and validates its passage [5]. It is a reliable and versatile technology, allowing a good balance between quality of service and implementation cost (time, complexity and price).

ANPR (Automatic Number Plate Recognition)

According to [10], cameras are installed at strategic points where vehicles enter and exit, capturing images of license plates. A software system processes these images in real time, recognizing the number plate and comparing it with a list of authorized vehicles.

This method might offer a couple of advantages over RFID technology: ease of integration (it might be enough to integrate with the already existing video surveillance system). However, it has several disadvantages: visibility dependency (license plates with dirty or damaged plates compromise reading, as do bad weather conditions such as dense fog), security (license plates are more easily forged than RFID tags) and latency (the time it takes to process the image and identify the plate can cause the system to respond more slowly, especially in heavy traffic flows).

Although ANPR systems are effective for vehicle identification, their applicability to containers is limited. Unlike vehicles, containers do not carry standardized license plates designed for optical recognition. These codes are larger, alphanumeric, and not optimized for automated visual capture, which significantly reduces ANPR reliability. This distinction between vehicle license plates and container identification codes highlights a fundamental limitation of ANPR in logistics scenarios. In contrast, RFID technology overcomes this drawback, since it does not rely on optical visibility or standardized plate formats.

Shipping Container OCR (Optical Container Recognition)

As indicated by [11], Optical Character Recognition (OCR) is an automated text recognition technology that can intelligently recognize text in an image and convert it into an editable text string. The way this recognition system works is very similar to ANPR. Sea containers are marked with a unique ID, so that it is processed as if it were a car license plate. This type of

system could be applied to industrial containers.

However, according to [11], there are many factors that affect OCR, including light, font complexity, image blur, and background interference. The two main issues with the application of current OCR technologies for container terminal text recognition: irregularity of text, textual region cohesion.

BLE (Bluetooth Low Energy)

The use of BLE beacons can be applied in industrial environments to control vehicles. In this case, the vehicle is fitted with a device that communicates with sensors at access points, automatically checking that the vehicle is authorized to enter. However, these beacons contain a battery, limiting the device's autonomy and increasing the degree of device maintenance compared to passive RFID tags [12]. Compared to passive tags, the battery takes up more space and is much less resistant to high temperatures and physical impacts.

QR (Quick Response) Code or Bar Code

A unique QR code or bar-code is generated and printed on the container. When approaching the entrance, a scanner reads the code and validates the authorization [13]. This method requires sophisticated scanning equipment to guarantee scanning on the move and is only suitable in very close range. In addition, like ANPR, the level of security is much lower since QR or bar codes are easily forged and any physical wear or dirt on the code prevents it from being read.

GPS (Global Positioning System) Geo-fencing

Geo-fencing technology uses GPS data to define virtual geographical boundaries. Vehicles are fitted with GPS tracking devices, the system defines 'virtual fences' around the facility and access is granted or restricted when the vehicle crosses these boundaries. Actions can be automated, such as opening a gate or sending an alert if a vehicle enters a restricted area [14].

Since a gateway is a clearly delimited area, the use of geo-fencing is not justified, as this technology is more suitable for large and dispersed zones. Passive RFID proves to be more efficient, as it does not require batteries, unlike GPS devices, which increase both acquisition costs and maintenance needs. Moreover, GPS operation depends on mobile or satellite networks, generating additional costs, and may suffer signal loss in enclosed areas. Passive RFID

systems, supported by fixed readers and antennas, ensure reliable detection at the exact point of passage without these limitations.

Mixed Systems

The most sophisticated systems are made up of a set of technologies (including the ones already mentioned). These systems can even be controlled and monitored by AI (Artificial Intelligence), allowing for more informed automatic analysis based on a set of inputs from different sources. For instance, cameras equipped with deep learning algorithms are able to identify additional vehicle characteristics, in addition to reading and recognizing number plates (e.g. vehicle type, color, brand). Besides, artificial intelligence offers a promising solution for strengthening cybersecurity [15]. This type of solution is initially discarded because the physical appearance of the containers is very identical to each other. Also, economically, this type of solution is the least accessible. For the case under study, these methods are too sophisticated and expensive, although they could possibly serve as an improvement to the initial system of the pilot project.

2.3 RFID Technology

RFID is a technological family that belongs to the AIDC (Automatic Identification and Data Capture) category. AIDC methods detect objects, collect data about them, and enter the data straight into computer systems. Radio waves are used in RFID methods to accomplish this [5]. At its most basic, RFID systems consist of four components: a tag, an antenna, a reader and a back-end system (Figure 2.3) [16]. Using the antenna, the reader transmits an RF signal to the tag to ”wake it up” and then receives the target information from the tag. After performing initial filtering and signal processing, the reader extracts and analyzes the tag’s data. The processed information is then sent to data management systems via a network [17].

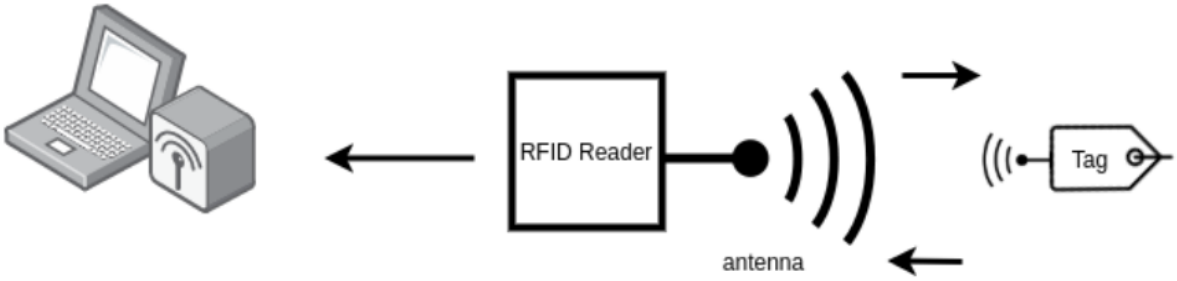


Figure 2.3: RFID General Architecture (extracted from [18])

When implementing an RFID system, it is essential to decide which equipment to buy. To do this, it’s crucial to choose which frequency band is the most suitable, depending on the context of the project.

2.3.1 Operating Bands

According to [19], four operating frequency bands can be used in this technology: LF (Low Frequency), HF (High Frequency), UHF (Ultra High Frequency) and SHF (Super High Frequency) also known as Microwaves. The UHF band offers the best performance in metallic environments and a fast data rate. It is the frequency band used in toll collection and provides a reading range of approximately 5 to 9 m (Table 2.2). For these reasons, it was the elected operating band for this project.

Table 2.2: RFID operating bands (extracted from [19])

Band + Frequency	**Read range**	**Advantages**	**Application**
Low Frequency (LF) 30–300 KHz	Up to 20 inches (∼0.5 m)	+ Good penetration in moist environments + No Anticollision – Slow data rate	○ Animal Tagging ○ Access control ○ Vehicle key-locks
High Frequency (HF) 3–30 MHz	Up to 3 feet (1 m)	+ Good penetration in moist environments – Poor performance in metal environment	○ Item level tagging, libraries ○ Smart cards ○ Airline baggage
Ultra High Frequency (UHF) 300–3000 MHz	Passive: Up to 16 feet Active: More than 30 feet (6 m)	+ Fast data rates + Good performance in metal environment	○ Supply chain use at WM and Metro ○ Baggage handling ○ Toll collection
Super High Frequency (SHF) "Microwave" 3–30 GHz	2+ meters	+ Fast data rates + Good performance in metal environment – Poor performance in moist environment – High cost	○ Item tracking ○ Toll collection

2.3.2 Readers and Antennas

Readers can be classified according to their mobility (mobile or fixed). Mobile readers (Figure 2.4) are portable devices with an integrated antenna, suitable for use over short distances [20].

Figure 2.4: Honeywell mobile RFID reader (extracted from [21])

Fixed readers are suitable for installation at strategic points of tags flow. They do not include an internally incorporated antenna, but can be connected to various externally connected antennas, via coaxial cable [20].

RFID fixed antennas are generally directional, as the aim is to capture the presence of tags in a relatively well-defined flow zone. By changing the transmission power configured in

Figure 2.5: RFID fixed reader (extracted from [22])

the reader, it is possible to increase or decrease the read range of each antenna in order to optimise its application.

Figure 2.6: RFID Fixed Antenna (Laird Technologies) (extracted from [23])

2.3.3 Tags

RFID tags are mainly categorised according to their type of technology. In this sense, there are three types of tag: passive, active and semi-passive [5]. Passive tags (Figure 2.7) do not contain an internal power source and are not capable of transmitting signals independently. Active and semi-passive tags contain a battery. Active tags (Figure 2.8) transmit constantly or periodically and semi-active tags transmit when they come into contact with an antenna and are detected by it. Within passive tags category, there are also printed tags (Figure 2.9), which can be manufactured more quickly and cheaply but have a shorter read range.

Figure 2.7: RFID passive tags (HID Global Corporation) (extracted from [24])

Figure 2.8: RFID active tags (SRK Innovations) (extracted from [25])

Figure 2.9: RFID printed passive tags (Zebra Technologies) (extracted from [26])

2.3.4 Link Budget

The propagation of radio signals in real environments is affected by various phenomena that cause variations in received power. The mechanisms behind the propagation of elec-

tromagnetic waves are diverse, but can generally be attributed to reflection, diffraction, and scattering. These variations are generally classified as large-scale fading and small-scale fading, as described by [27]. Large-scale fading refers to average variations in received power over relatively long distances, dominated by signal attenuation due to distance and shadowing introduced by natural or artificial obstacles. On the other hand, small-scale fading is associated with rapid variations in the received signal over distances of the order of the wavelength or over short time intervals. These fluctuations result mainly from multipath interference, which can cause significant signal reinforcement or attenuation at specific points.

Figure 2.10 depicts the dual fading effects in an indoor wireless environment: fast, short-term fluctuations (small-scale fading) superimposed on slower, distance-dependent signal attenuation (large-scale fading). The plot reveals rapid signal oscillations as the receiver changes position, while the underlying mean signal strength declines more smoothly over distance.

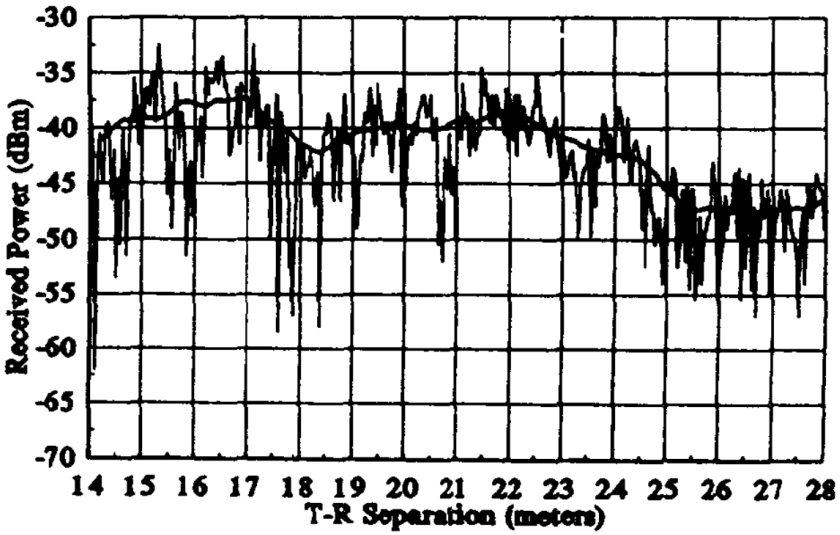


Figure 2.10: Small-scale and large-scale fading (extracted from [27])

In this work, small-scale fading will only be mentioned as an existing phenomenon, since the focus is mainly on the average power variations that condition the range and reliability of the RFID system under study. For initial estimates of RFID link performance and theoretical range, the FSPM (Free Space Propagation Model) was used in conjunction with the Friis equation. The FSPM allows the calculation of FSPL (Free-Space Path Loss) and, based on Friis' equation, it is possible to determine the power incident on the tag (forward link) and the power received by the RFID reader after reflection from the tag, based on the values of the power transmitted by the reader, the antenna gains, and the losses associated with the connection.

Friis Equation

The free space power received by an antenna, which is separated from a transmitting antenna by a distance d, is given by Friis' free space equation:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \tag{2.1}$$

where P_t is the transmitted power, $P_t(d)$ is the received power, which is a function of the transmitter-receiver separation distance, G_t is the transmit antenna gain, G_r is the receive antenna gain, d is the transmitter-receiver separation distance in meters, L is the system loss factor unrelated to propagation ($L \geq 1$), and λ is the wavelength in meters. λ is related to the carrier frequency by

$$\lambda = \frac{c}{f} \tag{2.2}$$

where f is the carrier frequency in Hertz and c is the speed of light expressed in meters per second. The values of P_t and P_r must be expressed in the same units, and G_t and G_r are dimensionless quantities. The various losses L ($L \geq 1$) are generally due to transmission line attenuation, filter losses, and communication system antenna losses. A value of $L = 1$ indicates that there are no losses in the system hardware.

Free Space Path Loss

Path losses, which represent signal attenuation as a positive quantity measured in dB, are defined as the difference (in dB) between the effective transmitted power and the received power, which may or may not include the effect of antenna gains. Path losses for the free space model, when antenna gains are included, are given by

$$PL(\text{dB}) = 10 \log \left(\frac{P_t}{P_r} \right) = -10 \log \left[\left(\frac{\lambda}{4\pi d} \right)^2 \right] \tag{2.3}$$

The Friis free space model is only a valid predictor for P_r values when d is in the far field region of the transmitting antenna. The far-field zone, or Fraunhofer region, of a transmitting antenna is defined as the region beyond the far-field distance d_f, which is related to the

largest linear dimension of the transmitting antenna aperture and the carrier wavelength. The Fraunhofer distance is given by

$$d_f = \frac{2D^2}{\lambda} \tag{2.4}$$

where D is the largest physical linear dimension of the antenna. Furthermore, to be in the far-field region, d_f must satisfy

$$d_f \gg D \tag{2.5}$$

and

$$d_f \gg \lambda \tag{2.6}$$

Although the analysis in this study was inspired by the free space propagation model and Friis equation presented by Rappaport, the equations were not used directly. This is because passive RFID links differ substantially from conventional mobile radio links. In a UHF RFID system, the tag does not have its own power source, depending entirely on the power received from the reader antenna to be activated and backscatter the signal. Thus, in addition to calculating the power received in the forward link, it is necessary to consider the particularities of the backscatter process and the minimum sensitivity of the tag chip, which makes the mathematical model distinct from that used to characterize traditional bidirectional radio communications.

According to [28], UHF RFID systems, the interrogation range stands out as the critical performance metric. This range can be compared to the cell coverage in wireless communication systems. Several factors influence this range, but three primary ones stand out: the power needed to activate a tag's IC (Integrated Circuit) chip, the reader's receiver sensitivity, and the surrounding propagation conditions. While the propagation environment is an external factor, the power required to activate the tag and the reader's sensitivity are inherent to the system. As a result, their impact on range can be efficiently analysed using a link budget—the standard method in wireless system design for assessing coverage.

Unlike conventional systems, RFID tags lack an internal power source, meaning the reader must provide all necessary energy—making the tag's activation threshold the dominant

factor in link budget calculations. A defining characteristic of conventional wireless networks is link symmetry. The forward and reverse links are balanced in coverage, despite minor variations in transmit power and receiver sensitivity. As a result, the effective range remains nearly identical for both directions. In a typical wireless communication setup, as shown in Figure 2.11, the systems are designed to maintain balance between the forward and reverse links, meaning that the difference in their power levels is minimal. As a result, the coverage area of the forward link is nearly identical to that of the reverse link, despite slight variations in transmission power and receiver sensitivity.

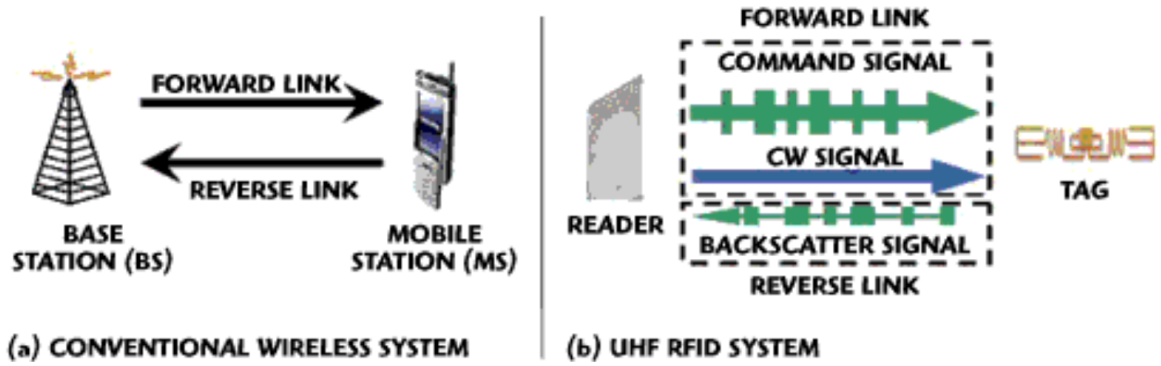


Figure 2.11: Comparison between a conventional system and a UHF RFID system (extracted from [28])

In contrast, RFID communication links operate differently from conventional wireless systems. In passive RFID systems, tags lack their own power supply and instead draw energy from the CW (Continuous Wave) signals emitted by the reader. Data transmission from passive tags relies solely on backscatter modulation, meaning that the tag reflects part of the reader's signal back to convey information. Consequently, an RFID link functions in half duplex mode—communication flows from reader to tag and then from tag back to reader. This results in an inherently unbalanced link, where the reverse transmission is strongly dependent on the forward link, as the tag's output power is determined by the reader's transmitted power.

In passive RFID systems, the power received by the tag's antenna is split into two parts: one is used to supply energy to the chip, while the other is allocated for backscatter communication. The parameter represents the power loss caused by backscatter modulation, which depends on the modulation technique employed by the tag, such as ASK (Amplitude Shift Keying) or PSK (Phase Shift Keying). This loss can be readily expressed using the following equation:

$$\kappa = \begin{cases} -10\log_{10}\left(\frac{1-m^4}{(1+m^2)^2}\right) & \text{for ASK} \\ -10\log_{10}\left(1-m^2\right) & \text{for PSK} \end{cases} \tag{2.7}$$

In the return path (reverse link), the tag first harvests the reader's CW (Continuous Wave) transmission, modulates the signal, and reflects a fraction of it back toward the reader's receive antenna. The power reflection loss (Γ) due to the ion factor is given, for both ASK and PSK, as

$$\Gamma = 10\log_{10}(m^2) \quad (4) \tag{2.8}$$

where m is the modulation index.

It is also essential to calculate power losses in coaxial cables, which depend directly on their length, and to take into account the PLF (Polarization Loss Factor) value. Both are analysed in greater depth in the implementation section, where the equipment used in the project is described.

2.4 Current Trends and Development

As mentioned by [29], the RFID industry is evolving with key trends shaping its applications. Integration with IoT enables real-time tracking and enhances operational efficiency. Technological advancements, including smart tags, blockchain, and cloud computing, expand RFID capabilities. Its adoption in supply chain and inventory management improves accuracy, reduces costs, and automates processes. Additionally, the COVID-19 pandemic has accelerated the growth of RFID-based contactless solutions, enhancing convenience and safety. These trends are expected to drive continued innovation and adoption in the industry.

2.4.1 Academic Research

There are several examples of academic research on passive RFID systems, showing that this technology sparks interest in the academic community. Current systems can be improved and therefore new applications can be found for this technology.

According to [30], passive RFID tags can be installed in metallic objects like vehicles and containers to optimize their reading range using an impedance matching technique. By placing

the tag in a metal cavity and adjusting the coupling effect, the tag's maximum reading range can be significantly improved, as shown in experimental results.

As shown by [31], the performance of RFID tag antennas is influenced by nearby materials, particularly metal surfaces, which can degrade radiation efficiency and affect the antenna's radiation pattern and impedance. To address this issue, a metal-mountable patch tag antenna was developed for UHF RFID systems. By placing the passive tag on a copper layer above a dielectric substrate, both matched to the antenna's impedance, the detection range was improved from 10 to 25 meters.

As reported by [32], a vehicle tracking and management system is proposed. This research proposes a vehicle tracking and management system that makes use of an electronic license plate (E-plate). The system employs passive RFID technology, which is more cost-effective. Furthermore, the proposed antenna is embedded within the e-plate tag and optimized to match the standard dimensions of vehicle license plates. This design not only improves antenna performance but also achieves significantly higher RFID reading efficiency compared to existing compact antennas. Because the vehicle e-plate contains an RFID chip with stored information, RFID readers placed at strategic locations can capture the vehicle's data. The collected information can then be processed and used for vehicle tracking, monitoring, and overall transportation management.

In accordance with [33], an e-plate is presented, that incorporates a slot antenna on a metallic license plate along with an attached active RFID module. By carefully designing and optimizing the notched slots at specific positions on the plate, a prototype e-plate was developed, capable of remote identification at 2.45 GHz. Results from both simulations and experiments show that the slot antenna achieves the requirements suitable for vehicle tracking. The proposed active e-plate also demonstrated a measured reading range exceeding 92 meters.

2.4.2 Case Studies

RFID technology has gained worldwide adoption across industries such as retail, healthcare, and logistics. Its applications are extensive, including supply chain and inventory management, cold chain monitoring, anti-counterfeiting measures, and more efficient asset management and inventory control. There are several contemporary examples of companies that have adopted RFID technology, optimising their management and service delivery.

According to [29, 34], Walmart stands out as a leading driver of RFID adoption in the retail sector, having initially implemented the technology experimentally in 2005 and, in 2022,

extending the mandatory use of UHF RFID tagging across various supply categories, including home goods, toys, electronics, and furniture. The integration of this technology enables real-time inventory tracking, contributing to reduced stock discrepancies, minimized theft, and fewer product shortages. Strategically, Walmart's use of RFID has enhanced supply chain visibility, improved operational efficiency, and consequently increased customer satisfaction. Additionally, it is stated that Pfizer employs RFID technology as a strategic tool to enhance security and traceability within the pharmaceutical supply chain, enabling rigorous monitoring of storage and transportation conditions for medications. This approach has been instrumental in mitigating risks associated with counterfeit products, safeguarding patient safety, and optimizing inventory management and regulatory compliance. Over more than a decade, the company has made significant investments in implementing RFID labels on individual packages, cases, and pallets, allowing detailed traceability of product origins and movement, as well as rapid detection of any discrepancies within the supply chain, thereby ensuring the authenticity and integrity of vaccines and medications delivered to consumers.

As stated by [35], in large-scale operations such as those managed by oil and gas service companies, efficient equipment tracking is crucial for maintaining efficiency, reducing costs, and minimizing errors. Traditionally, tracking tools and equipment in yards was performed manually, a process that was time-consuming and prone to errors, leading to operational inefficiencies and higher costs. RFID technology has been adopted to address these challenges, enabling more accurate and real-time asset management. The benefits of RFID in Yard Management include real-time tracking, which allows the location and status of equipment to be known at any time, as well as cost reduction, with one oil and gas service company saving millions annually by transitioning from time-based to usage-based certifications. Additionally, RFID has enabled some companies to reduce spare inventory by 50–75% and improve asset utilization by allowing more dynamic and precise equipment management, thereby reducing the risk of errors during operations. As a result, the adoption of RFID has transformed yard management, significantly enhancing operational efficiency, safety, and compliance in global operations. The technology also streamlines equipment maintenance and certification, ensuring that assets are always ready for use and fully compliant with regulations.

As per [36], Hera, one of the largest multi-utility companies in Italy, implemented an RFID-based solution to optimize the management of its waste containers. The objective was to increase operational efficiency, ensure full traceability of operations, and comply with regulatory requirements. To achieve this, more than 200,000 HID EXO PRO 800 RFID tags, designed

to withstand harsh environments, were installed on waste containers across the municipalities where Hera operates. These tags are automatically read by RFID devices installed on collection vehicles or handheld equipment, with the data integrated into geolocation (GPS) systems and central management platforms. The adoption of this technology enabled process automation, georeferencing of each container, improved data recording and processing, and real-time monitoring of operations. As a result, Hera achieved significant improvements in efficiency, transparency, and quality of environmental services, consolidating RFID technology as a strategic tool for urban waste management.

[37] explains the case of AMCS Group, which demonstrates how the application of RFID technology can transform urban waste management, addressing challenges related to wasted collection trips and the lack of reliable data for fair billing. The adopted solution consisted of attaching RFID tags to waste containers, combined with readers installed on collection vehicles, capable of automatically recording information such as weight, GPS location, and the status of the container, including situations of blockage, contamination, or missed collection. This integration made it possible to reduce unproductive trips, optimize fleet management, and lower operational costs, while also ensuring greater transparency in billing and tighter operational control, including the possibility of conditioning collection in cases of non-payment. Furthermore, process automation reduced the need for customer service interactions and improved overall service quality. Overall, this case study shows that the use of RFID not only generates operational and financial efficiency gains but also contributes to greater environmental sustainability by reducing fuel consumption and emissions associated with collection operations.

2.5 Gaps and Challenges

According to [38], despite progress in RFID technology, challenges remain for its widespread use, particularly in certain applications. While some areas are well-established, others require the development of new devices and security protocols. Within this reality, we can consider that the main challenges to be faced by technology are: costs, energy sources, reading distance, metal surfaces, norms and standards.

Costs

Although the cost of passive RFID tags has decreased significantly in recent years, their adoption might still not be advantageous for low value-added products, for which printed bar-

codes remain more competitive. However, the main challenge in implementing RFID solutions today does not lie in the cost of the tag, but rather in the investment required for system integration, including infrastructure, middleware, and the adaptation of business processes.

Energy sources

For active RFID devices, battery life is still a problem. The short charge life of current batteries limits the development of new devices and applications that require more processing power, which in turn requires a greater supply of energy. For passive devices, although they are only energised at the moment of use, the energy obtained is inversely proportional to the distance between them and the reader. The greater the distance, the less energy for the tag. As such, passive devices require less maintenance, less physical space and are economically cheaper.

Metal surfaces

Restrictions on use in environments subject to electromagnetic interference and metallic or conductive materials can hinder the transmission of radio frequency signals between the transponder and the RFID reader. As such, the right equipment should be chosen for such conditions.

Norms and standards

National and international regulations are still not compatible, and there is a lack of processes to streamline the integration of the microchip according to the type of product. For instance, the frequency bands used for RFID in the United States are not the same as those in Europe. For a company that works nation-wide, this shouldn't be an issue.

2.6 RFID Vulnerabilities

RFID technology enables data storage and tracking but poses security risks if not properly protected. According to [38], key vulnerabilities include integrity violations, where tags can be misplaced or altered, potentially causing harm; tag cloning, where attackers copy and replicate RFID data for fraudulent use; and tag monitoring, where sensitive information can be accessed and misused remotely. Without strong security measures, these risks can lead to significant

threats for individuals and organizations. For a more detailed analysis of the most apparent vulnerabilities in these applications, some of the examples mentioned above can be used:

RFID technology is used for object tracking, but it poses risks if tags store excessive information. Cloned or forged tags can carry viruses that infect reader systems and servers, potentially corrupting databases, compromising other tags, and enabling data theft. High costs make it challenging to implement advanced security protocols to mitigate such attacks. Even passive tags, with limited range, can be intercepted, while active tags amplify security concerns.

Privacy concerns with RFID arise when tags remain active outside business premises. For instance, if hidden contents are tagged, a malicious person could use a reader to inventory items from the street and plan a burglary.

Protection Alternatives

RFID and wireless identification technologies present significant privacy concerns. However, studies and projects are being developed to ensure secure deployment, making large-scale use feasible and more convenient. While these solutions don't guarantee complete security, they make RFID technology more reliable and less vulnerable.

One way to protect the system's integrity is by using key-based encryption. Only the sender and receiver have access to the content of the information on the tag. Anyone trying to obtain this data illicitly will have to decipher a cryptographic standard that has already been proven to be reliable.

3

System Architecture and Requirements

Being familiar with the state of the art of the main access control technologies, particularly in industrial environments, a passive UHF RFID system was proposed to monitor access to the company's industrial containers. This chapter presents the pilot architecture of the system, justifies its choice, and describes its hardware and software requirements.

3.1 Hardware and Software Requirements

As explained in section 2.3, the UHF and SHF frequency bands offer better performance in metallic environments. However, the UHF band allows for greater reading range, so it was decided to work in this frequency band.

Given that this project focuses on access control for industrial containers, the most appropriate strategy is to install fixed RFID equipment at industrial vehicle access points, such as a main gate. The use of mobile equipment is not at all suitable for several reasons, mainly because of its much shorter read range and it requires manual handling by a person each time a container passes through, defeating the purpose of the project, which is to automate the recording of container passages.

As mentioned in section 2.3, RFID architectures contain a back-end system that processes tag events sent by the fixed reader. Therefore, it is necessary to adopt an appropriate IoT protocol for sending information in the context of the project. The MQTT (Message Queuing Telemetry Transport) protocol was chosen, since tag events occur asynchronously, i.e., tag reading is constant and the publication of tag events in the broker is independent of the timestamp of the events or the order in which they occur [39]. On the other hand, according to [40],

the MQTT protocol is valued for low overhead, scalability, and real-time communication, so if it is necessary to expand the system, namely to monitor or control access at more flow points, this protocol supports such expansion. Finally, through the publish/subscribe operating model, this protocol prevents each device from having to communicate directly with all the others.

Figure 3.1 illustrates the layout (top view) of an industrial vehicle access point, the proposed RFID architecture and its tag event data flow, in which the objects are not to scale. The green lines represent physical connections via coaxial cable, and the red lines represent MQTT connections. The fixed reader must be installed in a secure location, such as a security booth.

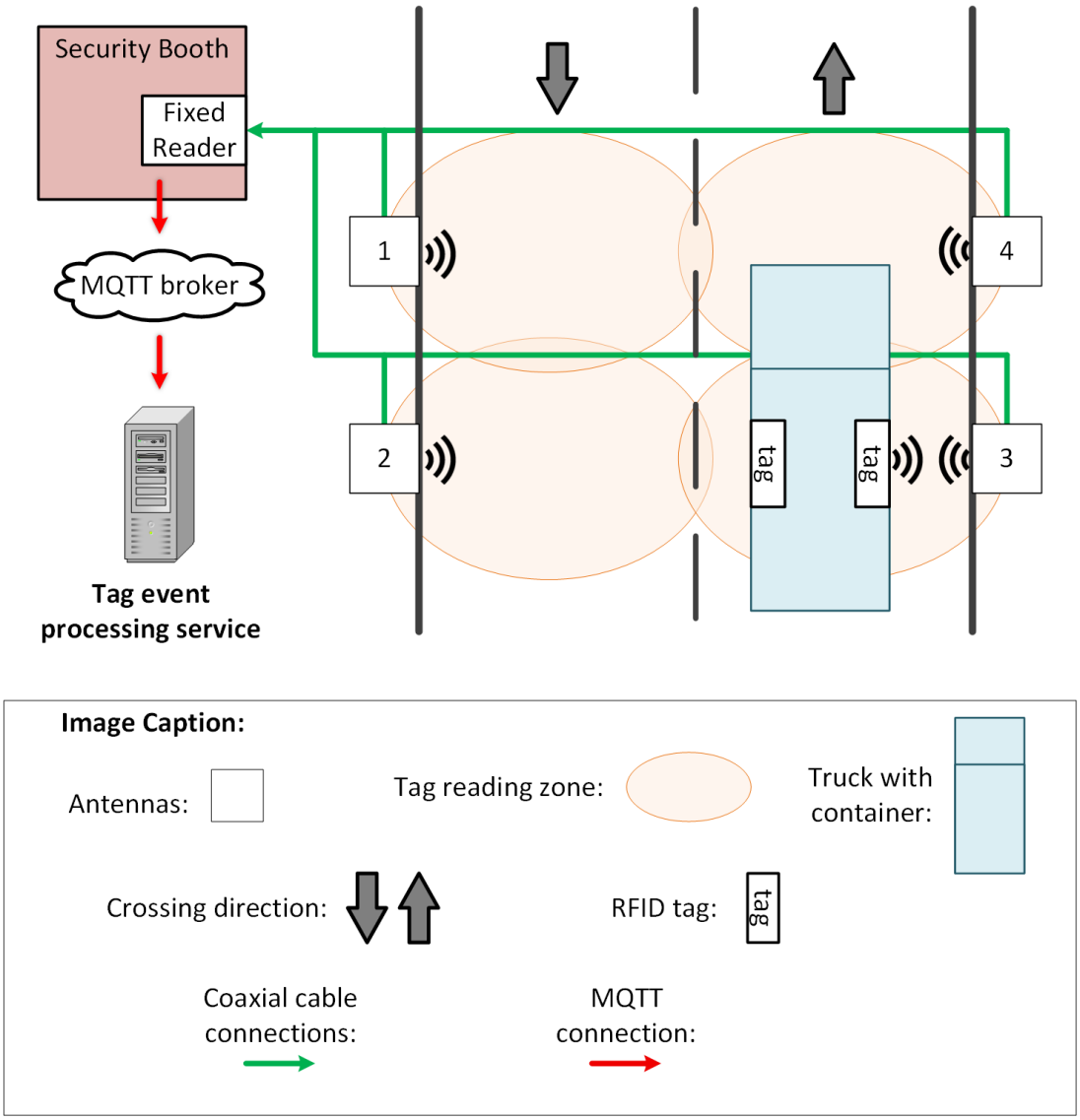


Figure 3.1: Proposed Architecture for RFID system

When an RFID tag is detected inside each antenna's range, the fixed reader publishes a tag event message in the MQTT broker. The middleware has subscribed all the necessary topics to communicate with the fixed reader and receives the tag event messages, extracting its essential parameters (tag ID, time stamp, antenna ID). The back-end system consists of an

information processing service that receives and interprets tag events published by the fixed reader by subscribing to the respective topic.

All RFID equipment must operate on the European UHF band (865 to 868 MHz [41]). The fixed reader must meet several requirements, namely: have coaxial cable ports for at least four antennas, allow connection via MQTT protocol and Ethernet and/or Internet communication interface. Fixed antennas must be directional and resistant to contact in outdoor industrial environments (dust, liquids, temperature variations). Coaxial cables should have the lowest possible attenuation (dB/m), be as short as possible to reduce signal attenuation and connectors should be compatible with the reader and fixed antennas.

Additional structures may be required. The fixed reader must be installed in such a way that it is protected, for example, in a security booth. The antennas should be installed on a pole so that their height and direction can be adjusted, it is recommended for a mounting structure to be acquired for each antenna.

As for battery use, it was decided to use passive technology. The use of batteries, namely in tags, brings several disadvantages to the implementation and maintenance of the project, both financially and in terms of maintenance complexity. Firstly, the acquisition of passive tags is more affordable, especially considering that a large inventory of tags is to be purchased [42]. In addition to the acquisition cost, the use of active or semi-active tags involves higher maintenance costs due to the use of battery, namely: more frequent technical labour and periodic monitoring of the battery level of each tag. Thirdly, batteries are sensitive to various factors present in industrial environments, namely temperature values and aggressive physical impacts. Finally, the use of batteries implies a larger physical tag size [43], making it more prominent when installed in a container and more vulnerable to physical damage.

Also regarding tags, they must be suitable for installation on metal surfaces and resistant to aggressive contact in urban environments (physical impacts, dust, liquids, and temperature variations). The reading range allowed by the tag and the attachment method must also be taken into account. In order to protect the integrity of the tag, riveting or welding should be used for attachment. Screwing can compromise the tag more easily, as it can be easily unscrewed, and strong types of glues such as epoxy are more suitable for attachment to fibrous surfaces, not metal ones.

Finally, in relation to the software, it is necessary to implement a middleware that receives data from tag events and processes this information. This program runs on a local machine or on a company VM and, in practice, converts tag events into industrial container passage events.

3.2 Link Budget Requirements

As already mentioned, the performance of an RFID system is mainly defined by its tag reading range, which in turn is closely related to the system's link budget. To ensure reliable system operation, it is necessary to develop a link budget that allows estimating whether the power received by the tag is sufficient for its activation and, subsequently, whether the backscattered signal is detected by the reader. Thus, the fundamental requirements of the link budget were defined, which will serve as the basis for analyzing the theoretical range of the system and for formulating the installation recommendations presented in the following chapters. Figure 3.2 illustrates the link budget model considered for the passive RFID system.

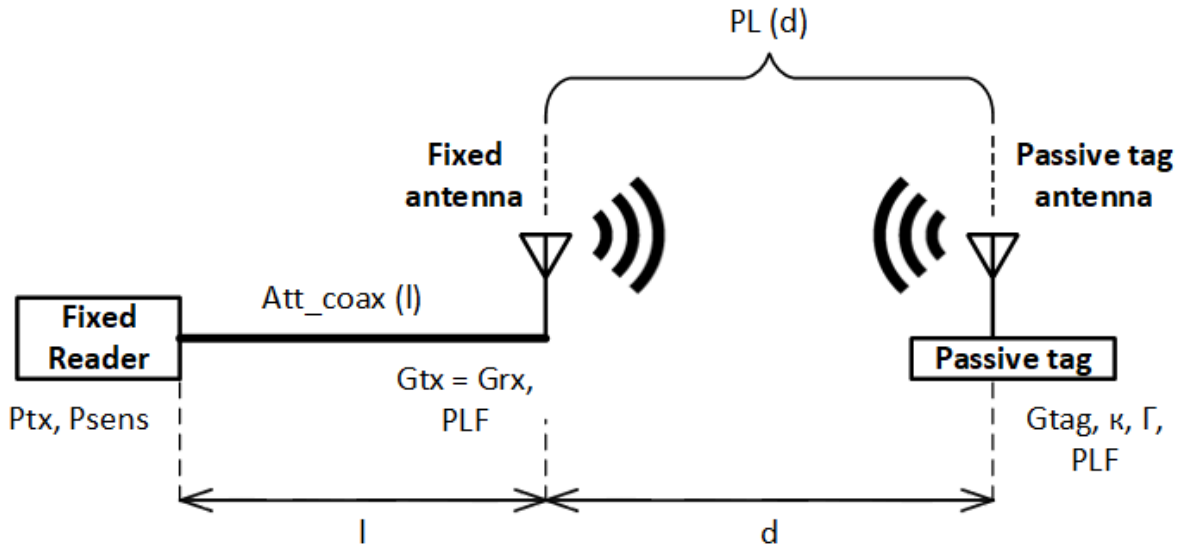


Figure 3.2: Link budget diagram

The process begins at the fixed reader, which transmits a signal with power P_{tx} through a coaxial cable subject to attenuation $Att_{coax}(l)$ directly proportional to the length of the cable l [m]. This signal is applied to a fixed antenna with gain G_{tx}, responsible for radiating the electromagnetic wave into free space. Propagation in free space to the passive tag suffers a path loss $PL(d)$, dependent on the distance d [m]. Upon reaching the passive tag antenna, there is a power loss due to polarization mismatch PLF. The tag contains an antenna with gain G_{tag} and is also characterized by losses associated with its passive behavior, namely power loss due to modulation κ and power loss due to reflection Γ. The tag then responds by backscattering, modulating the incident wave and sending it back along the same inverse path to the reader antenna. The propagation of the tag response in free space again implies, once again, losses $PL(d)$. The fixed antenna receiving responses from the tag by the reader is the same one that transmits the interrogation signal, so $G_{rx} = G_{tx}$. The signal reaches the reader

through the coaxial cable, again suffering losses $Att_{coax}(l)$. Finally, the balance between all these gains and losses determines whether the received power is above the reader's sensitivity P_{sens}, defining the reliability of RFID communication.

3.3 Event Interpretation and Decision Process

This section delves into the decision and interpretation logic used to program the system middleware's program. As illustrated in Figure 3.1, the system's data process begins with a tag event. Whenever a tag is detected, a message is sent from the fixed reader to the machine where the middleware is running, via MQTT. The content of this message includes the three essential parameters for processing the passage of each tag: its ID, the antenna on which it was detected and the event time-stamp. Thus, whenever it receives a tag event message, the machine records this event in hash-maps, as illustrated in the example of Figure 3.3.

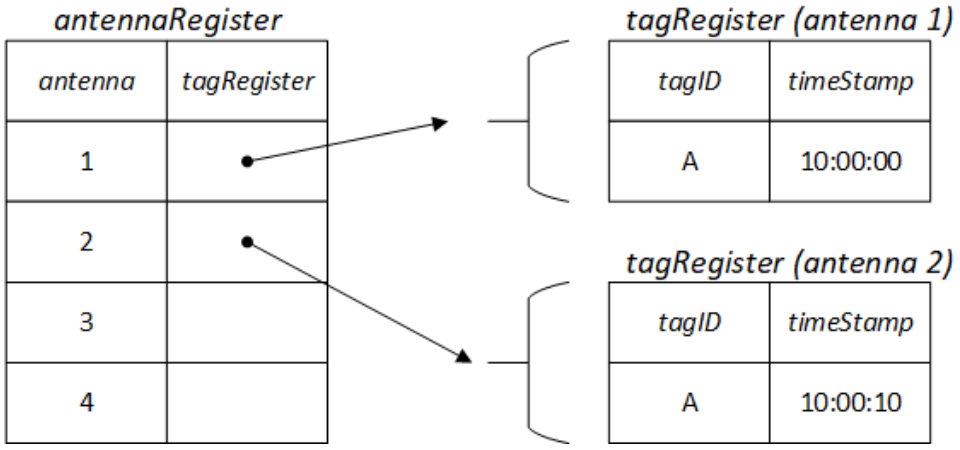


Figure 3.3: Example of the registration of the crossing of a tag A

This example illustrates the registration of an 'A' tag passage that is detected by antenna 1 at 10:00:00 and by antenna 2 at 10:00:10. In the antennaRegister hash-map, the moment of the first detection of a tag in each antenna is recorded, with each key-value pair corresponding to an antenna-tagRegister pair. Thus, each antenna is associated with the set of tags that were detected by it. In turn, each tagRegister is a hash map whose key-value pairs correspond to tagID-timestamp, which represent each tag that passed through the respective antenna and the timestamp of the event.

Figure 3.4 shows the flowchart that reflects the entire process of recording a tag event in the hash-maps. Multiple consecutive readings of the same tag may occur for each antenna, so it is essential to filter tag events to obtain the first occurrence. The most important moment when a tag passes through the gate is the first moment it is detected by each antenna, as this

is the only way to determine the direction in which it passed.

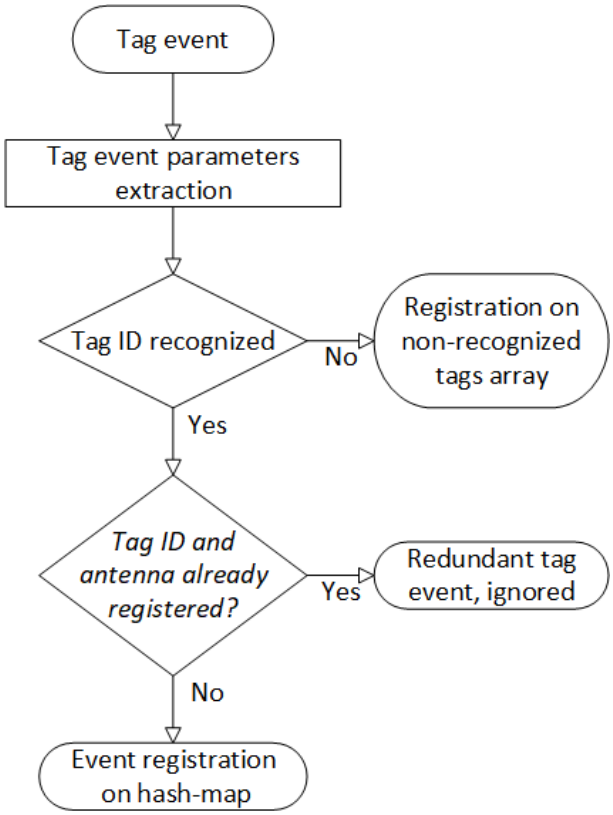


Figure 3.4: Flowchart of the process for registering tag events in hash-maps

The middleware program involves the execution of several threads. The threads dedicated to subscribing to MQTT topics are constantly running, so that tag event information can be received, as well as maintenance events such as the MQTT connection heartbeat. These connections also allow commands to be sent to the fixed reader and feedback from those commands to be received by the reader (success, failure).

Each time a tag event occurs, the dedicated program receives several parameters from the respective event via the MQTT connection. From these parameters, the tag ID, the antenna which detected the tag, and the timestamp of the occurrence are extracted.

Next, it checks whether the tag ID belongs to the company's inventory. If it is an unknown ID, it is recorded in an array of unknown tags. If it is recognised as a company tag, another check is performed: whether the tag is already being processed or not, in order to ensure that duplicate tag events are not processed. The records in the aforementioned hash maps are scanned and each record is compared with the event being processed. If it is a duplicate tag event, it is ignored; otherwise, it is recorded in the hash map.

The middleware carries out a periodic verification process (Figure 3.5) on the hash-maps, using a thread that runs asynchronously in relation to tag events threads. The purpose of this

verification process is to evaluate the hash-map records in order to interpret and determine the passage (or lack thereof) of each tag that has been detected by the antennas.

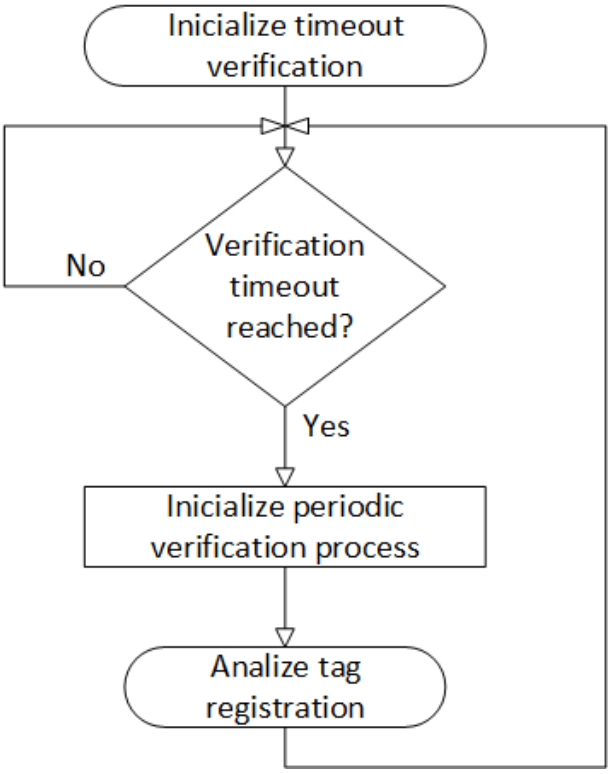


Figure 3.5: Flowchart of the process for the hash-maps periodic check

In order to interpret the tag passage records, various checks are made, including whether or not a tag has passed through and in which direction (Figure 3.6). The first check to be made is whether the tag has passed from one side of the gate to the other. For example, according to the position of the antennas in Figure 3.1, if a tag has been read by antenna 1 but has not been read by antennas 2 or 3, this means that no crossing has taken place.

If no tag crossings took place, there are two possibilities: 1) The vehicle carrying the container is waiting; 2) The vehicle was not allowed to pass and had to back off. The type of situation is determined on the basis of pre-established timers. For example: if a tag was read on an antenna 5 minutes ago but no further tag events have occurred since then, it is fairly safe to assume that the vehicle carrying the container was not allowed passage, so the tag is removed from the processing logs and a message is sent by the program informing it of what has happened.

The proposed system architecture establishes a solid foundation for the implementation of an automated access control solution using passive UHF RFID technology. With the main hardware and software requirements defined, the implementation phase follows.

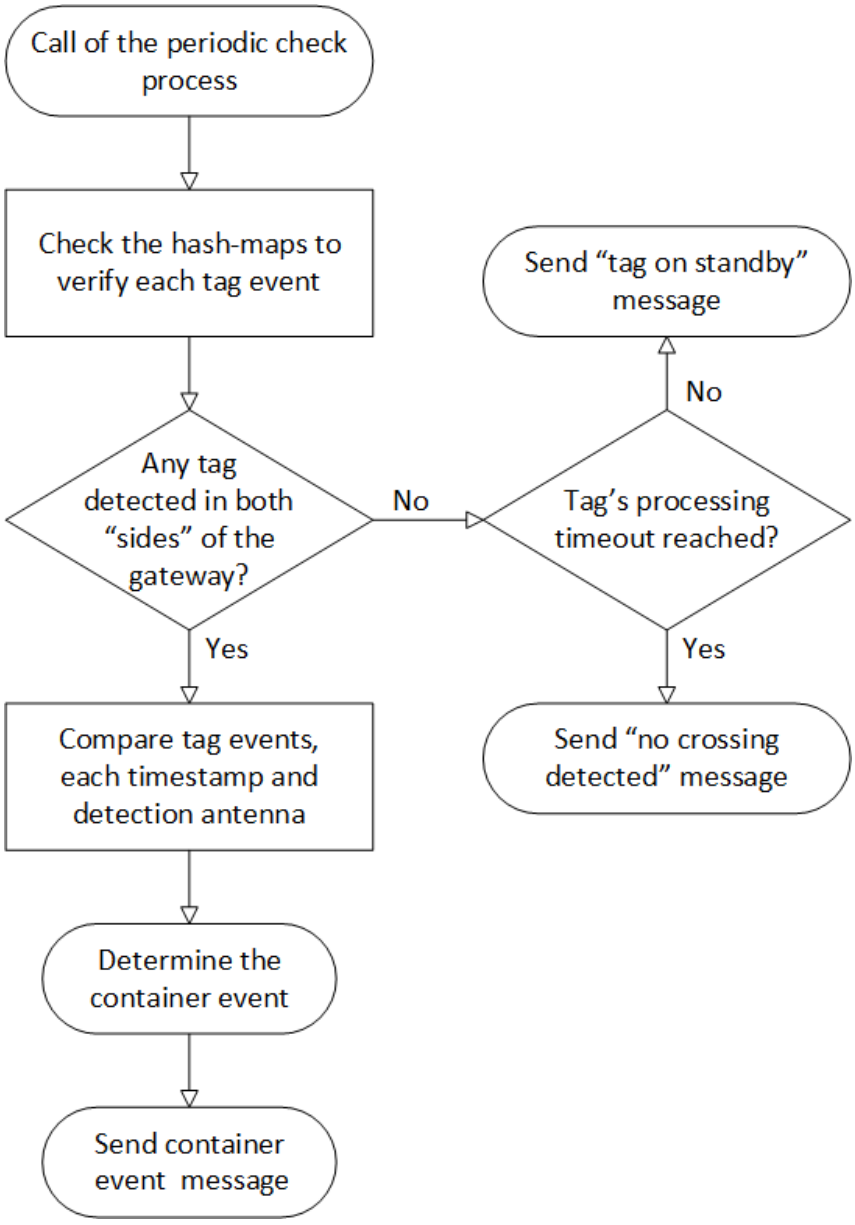


Figure 3.6: Flowchart of the process for interpretation of the registered tag events

4

Implementation

This chapter describes the practical implementation of the system defined in the architecture, based on the functional and technical requirements defined in the previous chapter. It details the equipment chosen, the software tools used, and the configurations adopted to ensure communication between the various components of the system. The implementation covers both the hardware and software sides. The aim is to demonstrate how the concepts defined in the architecture phase were implemented in a functional and integrated manner in the real context of the installation.

4.1 Hardware Implementation

There are several RFID equipment suppliers on the market, including companies such as Zebra, Inpinj, Honeywell International, Alien Technology, Avery Dennison, HID Global, and CAEN RFID [44–48]. In this project, it was decided to use RFID fixed equipment from Zebra Technologies and HID passive tags. This company is a market leades with reliable equipment that complies with European standards. In addition, it has good documentation available online that enables more effective implementation of both hardware and software. Therefore, in terms of hardware, it's important to highlight the main features and performance of the acquired RFID devices.

4.1.1 Fixed Reader and Antennas

The Zebra FX9600 fixed reader (Figure 4.1) is extremely customisable in terms of operating mode settings, which makes it versatile and adaptable to various scenarios. As can be seen in Table 4.1, this reader is available in two versions: global and US-only. Logically, the global reader was used in this project, as it allows operation in Europe's UHF frequency bands.

It complies with ISO 18000-63 (EPC Class 1 Gen 2 V2) standard, integrating an anti-collision mechanism. This means that it implements a protocol that, when coming into contact with several tags simultaneously, allows the reader to identify and communicate with one tag at a time in an orderly manner, even in the presence of many tags. In in terms of radio characteristics, it is also essential to mention that the reader has a maximum signal receiving sensitivity of -86 dBm and it is monostatic, which means it uses the same antenna to send and receive signals, together with a circulator. According to [28], the circulator is a non-reciprocal three-port device, where the signals travel from the transmitter port to the antenna port or from the antenna port to the receiving port.

Finally, this reader has a maximum read capacity of 1200 tags per second [49–54], it supports internet connection via Ethernet or Wi-Fi and connects to at least four antennas simultaneously via coaxial cable [55]. The technical information from the Zebra FX9600 data sheet is included in the attachments (Figures 6-12).

Table 4.1: Zebra FX9600 fixed reader specifications (extracted from [55])

Max Receive Sensitivity	-86 dBm monostatic
Air Protocols	ISO 18000-63 (EPC Class 1 Gen 2 V2)
Frequency (UHF Band)	Global Reader: 902 MHz - 928 MHz (Also supports countries that use a part of this band), 865 MHZ - 868 MHz US (only) Reader: 902 - 928 MHz
Transmit Power Output	0dBm to +33.0dBm: PoE+, 24V External DC, Universal 24 VDC Power Supply; 0dBm to +31.5dBm: PoE, 12V External DC (4-port-models only), 24V External DC, Universal 24 VDC Power Supply

The Zebra AN480 antenna (Figure 4.2) is a directive antenna, compatible with all UHF RFID bands worldwide (operates between 865 MHz and 956 MHz). Due to its physical size it

Figure 4.1: Zebra FX9600 fixed reader (extracted from [55])

can be used indoors or outdoors, depending on the configuration of its transmission power [56]. The specifications of this antenna can be found in Table 4.2.

Figure 4.2: Zebra AN480 fixed antenna (extracted from [56])

Table 4.2: Zebra AN480 fixed antenna specifications (extracted from [56])

PHYSICAL CHARACTERISTICS	
Polarization	Left-hand circular or Right-hand circular
Dimensions	259.1 mm x 259.1 mm x 33.5 mm/ 10.2 in. x 10.2 in x 1.32 in.
Connector	N-Type Female
Connector Location	Rear
Mounting Options	Mounting studs provided
Weight	2.5 lbs./1.13 kg
Casing/Materials	Aluminum with white plastic cover
Frequency Ranges	865 – 956 MHz
VSWR (Return Loss)	1.3:1

Gain	6.0 dBiL
Front to Back Ratio	18 dB
3 dB Beam Width	65° in both planes
Maximum Power	2 Watts
Axial Ratio	1.5 dB typical
Operating Temperature	-25° to +70°C/-13° to +158°F
Storage Temperature	-40° to +70°C/-40° to +158°F
IP Sealing	IP54
Vibration	IEC-68 series
Humidity	IEC-68-2-30

It operates with circular polarisation, which is the most common polarisation in UHF RFID antennas. Passive tags, on the other hand, usually operate with linear polarisation. Although European standards do not impose a specific polarisation for each device, there are reasons for using this practice worldwide. According to [57], generally, the polarization of the receiving antenna will not be the same as the polarization of the incoming (incident) wave. This is commonly stated as ”polarization mismatch.” The amount of power extracted by the antenna from the incoming signal will not be maximum because of the polarization loss, which can be taken into account using the PLF (Polarization Loss Factor):

$$PLF = |\cos \psi_i|^2 \quad \text{(dimensionless)} \tag{4.1}$$

where ψ_i is the angle between the transmitted wave's polarization direction of the electric field unit vector and the receiving antenna's polarization direction of the electric field unit vector. Therefore, coherence between the polarizations of the incident wave and the receiving antenna is essential. In extreme cases there may be a theoretically zero power transfer (PFL=0), depending on the position of the receiving antenna. Ideally, the system must be capable of detecting the tag regardless of its position.

As further stated by [57], when an electromagnetic wave transmitted with circular polarisation reaches a linearly polarised receiving antenna, the PLF is 0.5, regardless of the angle of linear polarisation or whether the circular polarisation is right or left handed. Thus, by using fixed antennas with circular polarisation and tags with linear polarisation, it is possible to en-

sure that the tags do not go ‘unnoticed’ due to polarisation mismatch. However, this practice requires some compromises.

As stated by [58], circularly polarized antennas do not require precise alignment between the reader and the tag to operate effectively. Due to the rotating nature of the signal, there is an increased likelihood of successfully ”capturing” the tag, regardless of the tag’s orientation. However, these antennas typically have a shorter read range compared to linearly polarized antennas and can be more susceptible to interference. Despite these limitations, the flexibility provided by circularly polarized antennas in unpredictable environments often makes them the preferred choice for many real-world RFID applications.

As a directive antenna (Figure 4.3), it is important to highlight the following parameters: 6 dBi gain, 65º HPWB (Half-Power Beam Width) and 18 dB FTBR (Front-to-Back Ratio). HPBW (Half Power Beam Width) characterizes the aperture of its main lobe [59]. The HPBW value is 65°(in both the horizontal and vertical planes), which means that the angular width of the antenna beam is 65°between the points at which the radiated power drops to 50% of the maximum value. FTBR (Front to Back Ratio) characterizes the radiation intensity of the main lobe in relation to the back lobe [59]. This parameter is essential in this case because there is a secondary rear lobe concentrated approximately 180° from the main lobe. The FTBR is 18 dB, which means that for every 18 dB radiated from the front of the antenna, only 1 dB is radiated to the rear. The technical information from the Zebra AN480 data sheet is included in the attachments (Figures 13-15).

4.1.2 Industrial Passive Tags and Coaxial Cables

Still with regard to the hardware, it is important to mention the choice of passive tags, mentioning some of their characteristics. Two different models of passive rigid RFID tags were acquired and tested: HID Exo Pro InLine (Figure 4.4) and HID Exo Keg (Figure 4.5). As stated by [60], HID is a leading brand of RFID equipment, particularly in the field of access control. According to [24, 61], both are designed for mounting on metal and operate in the UHF band, specifically between 865 and 928 MHz. They support anti-collision protocols and operate within a temperature range of -40 to 85 ºC. The manufacturer guarantees IP68 protection (Ingress Protection 68), offering complete protection against dust and the possibility of submersion in water at depths greater than 1 metre for a prolonged period. They are also guaranteed to be resistant to physical impact according to IEC (International Electrotechnical Commission) 60068-2-27:2008 and resistant to vibration according to IEC 60068-2-6.

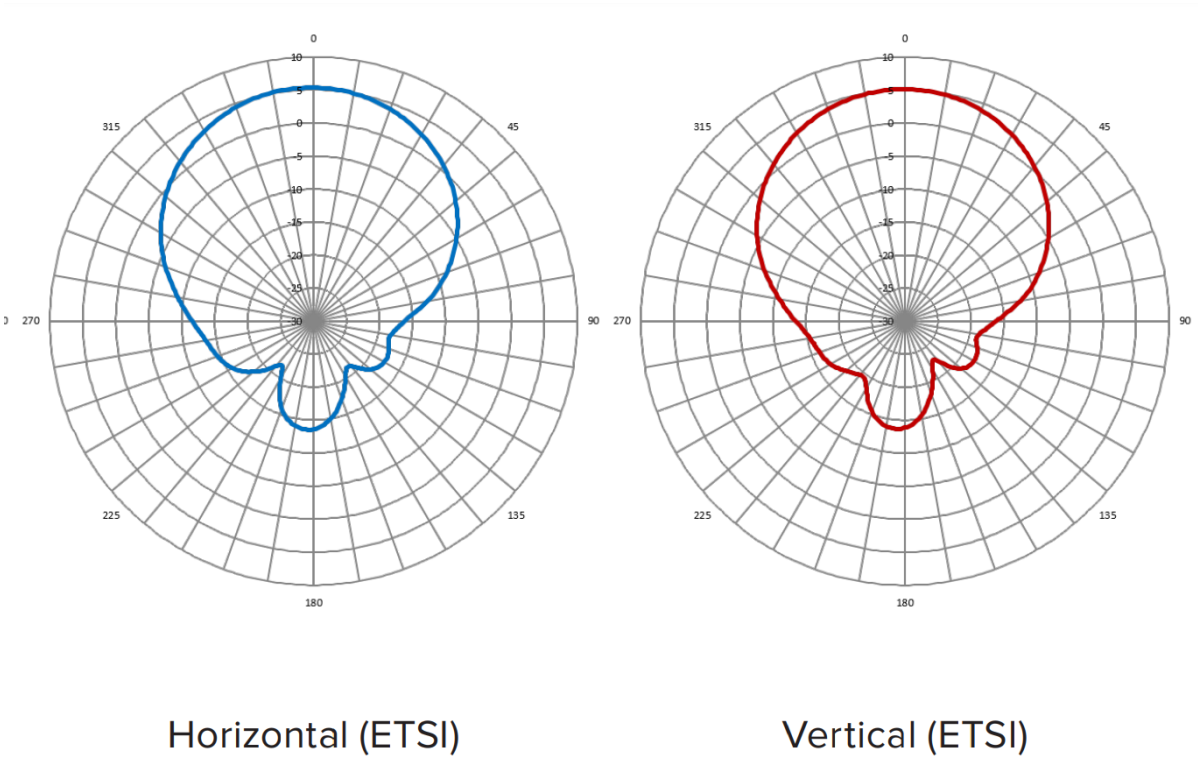


Figure 4.3: Zebra AN480 fixed antenna radiation pattern (extracted from [56])

There are some differences between the two tag models. Still according to [24, 61], the Exo Pro model is designed for mounting on flat surfaces (metal, plastic, wood), can be mounted by welding, screw or rivet, has a reading range of up to 11 m, and its housing material is thermoplastic. The Exo Keg model, on the other hand, is designed for mounting on curved surfaces, prepared for welding installation, has a reading range of up to 9 m, and its housing material is PA (polyamide). Different models were acquired to enable performance comparison tests between them. Despite their differences, these models were chosen for their physical durability, suitable detection range, and because they are specifically manufactured for mounting on metallic surfaces.

Figure 4.4: HID Exo Pro InLine tag

These tags are lightweight, waterproof and resistant to high-pressure and high-temperature washing conditions. They are highly resistant to aggressive liquids and physical impact. This

Figure 4.5: HID Exo Keg tag

tag model can be assembled in various ways. It was decided that the tags would be fitted by welding or riveting, since screws are easier to remove and resins (such as epoxy) are more suitable for fibrous surfaces such as wood, plywood or fibreglass. The technical information from the both chosen tags data sheets is included in the attachments (Figures 16-22).

Finally, Times Microwave Systems LMR240 coaxial cables were chosen. This cable has 24.8 dB/100 m attenuation @900 MHz and 50 ■ [62] input impedance, which corresponds to the input impedance of RFID equipment [41], minimising signal reflections (low VSWR (Voltage Standing Wave Ratio)). Regarding this cable model, it is stated by [63] that LMR240 is ideal for medium-length runs where signal preservation is crucial and the LMR series are widely used for outdoor antennas applications.

As explained by [64–66], the three most important parameters to consider when choosing a coaxial cable are: length, insulation rating and connectors. Length affects signal loss because no cable has perfect insulation, so the longer the cable, the greater the loss. The higher the insulation rating, the thicker and more protected the cable. The most commonly used UHF coaxial cables are the 195, 240 and 400 series. The downside of thicker, more insulated cable is that it is less flexible and can be difficult to install in tight spaces that require bending.

Therefore, although the length of the cable varies depending on the scenario in which it is used, it is highly recommended to use cables that are as short as possible. Looking now at insulation rating, according to [67], the LMR240 cable belongs to the group of flexible, low-loss coaxial cables. Low-loss coaxial cables are designed to minimise signal attenuation over long distances whereas flexible coaxial cables are easy to install and manoeuvre in tight or confined spaces without compromising electrical performance. Thus, this cable stands out for being suitable for RFID applications. As for the cable connectors, they must match the connectors on the other RFID equipment. The FX9600 fixed reader has RP-TNC (Reverse Polarity - Threaded Neill–Concelman) female connectors and the AN480 fixed antenna has N-Type female connectors. Therefore, the coaxial cable must have a RP-TNC male connector

on one end and a N-Type male connector on the other (Figures 4.6 and 4.7). The technical information from the LMR240 data sheet is included in the attachments (Figures 23-26).

Connectors

Interface	Description	Part Number	Stock Code	VSWR** Freq. (GHz)	Coupling Nut	Inner Contact Attach	Outer Contact Attach	Finish* Body /Pin	Length in (mm)	Width in (mm)	Weight lb (g)
1. F Male	Straight Plug	TC-240-FM-X	3190-2891	<1.25:1 (2.5)	Knurl	Solder	Crimp	N/G	1.1 (28)	0.45 (11.4)	0.014 (6.4)
2. N Male	Straight Plug	EZ-240-NMH-X	3190-2893	<1.25:1 (2.5)	Hex/Knurl	Spring Finger	Crimp	A/G	1.5 (38.1)	0.78 (19.8)	0.086 (39.0)
3. N Male	Right Angle	EZ-240-NMH-RA-X	3190-6143	<1.35:1 (6)	Hex	Spring Finger	Crimp	A/G	1 (25.1)	1.04 (26.4)	0.115 (52.0)

Figure 4.6: LMR240 connectors (part 1/2) (extracted from [62])

Connectors

Interface	Description	Part Number	Stock Code	VSWR** Freq. (GHz)	Coupling Nut	Inner Contact Attach	Outer Contact Attach	Finish* Body /Pin	Length in (mm)	Width in (mm)	Weight lb (g)
4. N Male	Right Angle	TC-240-NMH-RA-D	3190-2426	<1.35:1 (6)	Hex/Knurl	Solder	Crimp	A/G	1.2 (32.4)	1.22 (31.0)	0.091 (41.7)
5. N Male	Straight Plug	TC-240-NMH-X	3190-2887*	<1.25:1 (2.5)	Hex/Knurl	Solder	Crimp	N/S	1.5 (38)	0.75 (19.1)	0.086 (39.0)
6. N Male	Straight Plug	TC-240-NMC	3190-244	<1.25:1 (2.5)	Knurl	Solder	Clamp	S/G	1.5 (38)	0.75 (19.1)	0.082 (37.2)
7. 1.0/2.3 DIN	Straight Plug	EZ-240-1023M	3190-6283	<1.35:1 (2.5)	knurl	Spring Finger	Crimp	N/G	1.1 (228.5)	0.33 (8.5)	0.014 (6.63)
8. N Female	Bulkhead Jack	TC-240-NF-BH-X	3190-2888	<1.25:1 (2.5)	NA	Solder	Crimp	A/G	1.7 (44)	0.88 (22.2)	0.115 (52.2)
9. N Female	Panel Mount	TC-240-NF-PM-X	3190-2889*	<1.25:1 (6)	NA	Solder	Crimp	A/G	1.7 (44)	0.88 (22.2)	0.115 (52.2)
10. N Female	Straight Jack	EZ-240-NF-X	3190-2795	<1.25:1 (6)	NA	Spring Finger	Crimp	A/G	1.4 (35.4)	0.62 (15.8)	0.040 (18.0)
11. BNC Male	Straight Plug	TC-240-BMC	3190-242	<1.25:1 (2.5)	Knurl	Solder	Clamp	S/G	1.7 (43)	0.56 (14.2)	0.040 (18.1)
12. BNC Male	Straight Plug	EZ-240-BM-X	3190-6120	<1.25:1 2.5	Knurl	Spring Finger	Crimp	A/G	1.3 (34)	0.58 (14.7)	0.043 (19.5)
13. BNC Male	Straight Plug	TC-240-BM-X	3190-2890	<1.25:1 (2.5)	Knurl	Solder	Crimp	A/G	1.3 (34)	0.58 (14.7)	0.043 (19.5)
14. BNC Male	Right Angle	TC-240-BM-RA-D	3190-2869	<1.25:1 (2)	Knurl	Solder	Crimp	A/G	1.0 (25.1)	0.57 (14.5)	0.115 (52.0)
15. BNC Male	Right Angle	EZ-240-BM-RA-X	3190-2868	<1.30:1 (4)	KNURL	Spring Finger	Crimp	A/G	1.3 (33.6)	1.19 (30.1)	0.091 (41.7)
16. TNC Male	Straight Plug	EZ-240-TM-X	3190-2725	<1.25:1 (2.5)	Knurl	Spring Finger	Crimp	N/G	1.4 (34.3)	0.59 (15.0)	0.043 (19.5)
17. TNC Male	Straight Plug	TC-240-TM-X	3190-2797	<1.25:1 (2.5)	Knurl	Solder	Crimp	N/G	1.7 (43)	0.59 (15.0)	0.043 (19.5)
18. TNC Male	Reverse Polarity	EZ-240-TM-RP-X	3190-2892	<1.25:1 (6)	Knurl	Spring Finger	Crimp	A/G	1.4 (36)	0.59 (15.0)	0.043 (19.5)
19. TNC Male	Right Angle	TC-240-TM-RA-D	3190-2798	<1.25:1 (6)	Hex	Solder	Crimp	A/G	1.0 (25.1)	0.62 (15.7)	0.115 (52.0)
20. TNC Female	Straight Jack	EZ-240-TF-X	3190-6204	<1.25:1 (6)	NA	Spring Finger	Crimp	A/G	1.1 (27.2)	0.87 (22.0)	0.033 (15.0)
21. TNC Female	Reverse Polarity	EZ-240-TF-RP-X	3190-6167	<1.35:1 (6)	NA	Spring Finger	Crimp	A/G	1.1 (27.2)	0.87 (22.0)	0.033 (15.0)
22. QMA Male	Straight Plug	EZ-240-QM-X	3190-2894	<1.25: (6)	Knurl	Spring Finger	Crimp	N/G	1.2 (30.0)	0.41 (10.5)	0.014 (6.35)
23. QMA Male	Right Angle	EZ-240-QM-RA-X	3190-2895	<1.25: (<6)	Knurl	Spring Finger	Crimp	N/G	0.8 (20.3)	0.65 (16.5)	0.019 (8.62)
24. SMA Male	Straight Plug	EZ-240-SM-X	3190-2897	<1:25: (6)	Hex	Spring Finger	Crimp	N/G	1.0 (25.4)	0.32 (8.1)	0.016 (7.26)
25. SMA Male	Straight Plug	TC-240-SM-SS-X	3190-2898*	<1.25:1 (10)	Hex	Solder	Crimp	SS/G	1.0 (25)	0.32 (8.1)	0.016 (7.3)
26. SMA Male	Right Angle	TC-240-SM-RA-SS-X	3190-2900*	<1.35:1 (6)	Hex	Solder	Crimp	SS/G	0.8 (20)	0.65 (16.5)	0.019 (8.6)
27. SMA Male	Right Angle	EZ-240-SM-RA-X	3190-2899	<1.25:1 (6)	Hex	Spring Finger	Crimp	A/G	0.9 (22.8)	0.31 (7.9)	0.019 (8.6)
28. SMA Male	Reverse Polarity	TC-240-SM-RP	3190-326	<1.25:1 (2.5)	Hex	Solder	Crimp	SS/G	1.0 (25)	0.32 (8.1)	0.016 (7.3)
29. SMA Female	Bulkhead Jack	TC-240-SF-SS-BH-X	3190-2896*	<1.25:1 (2.5)	NA	Solder	Crimp	SS/G	1.1 (29)	0.31 (7.9)	0.019 (8.6)
30. Mini-UHF	Straight Plug	TC-240-MUHF	3190-445	<1.25:1 (2.5)	Knurl	Solder	Crimp	N/G	1.1 (28)	0.45 (11.4)	0.014 (6.4)
31. 7/16 Din Male	Straight Plug	TC-240-716M	3190-2982	<1.35:1 (3)	Hex	Spring Finger	Crimp	A/S	2.0 (50.5)	1.26 (32.0)	0.186 (84.4)
32. 7/16 Din Male	Right Angle	TC-240-716M-RA-D	3190-2983	<1.35:1 (3)	Hex	Solder	Crimp	A/S	1.4 (34.3)	1.60 (40.6)	0.239 (108.5)

*Finish metals: N=Nickel, S=Silver, G=Gold, SS=Stainless Steel, A=Alballoy **VSWR spec based on 3 foot cable with a connector pair *Available in bulk pack

Figure 4.7: LMR240 connectors (part 2/2) (extracted from [62])

RFID equipment was purchased and tested at ISEL's campus facilities. This was an important step in familiarising myself with the equipment before installing it at a company's premises and testing it in an industrial context. Zebra provides two essential tools for testing, monitoring and configuring its equipment: its web interface and the 123RFID desktop application. Initially, in order to familiarise ourselves with these tools, the 123RFID application was used to test tag readings in real time and the Zebra web interface to configure the reader's MQTT connection to the broker.

4.2 MQTT Implementation

The proposed system includes the use of the MQTT protocol for communication between the fixed reader and the developed middleware. Thus, as a starting point for the pilot project, it was decided to connect the FX9600 reader to an MQTT broker. Therefore, an EMQX public broker was set up.

EMQX is a high-performance public MQTT broker developed by EMQ Technologies, widely used in IoT projects due to its ability to handle large volumes of connections and messages. This MQTT broker is compatible with QoS 0, 1, and 2 and supports retained messages, will messages, and session persistence.

It offers high performance in terms of scalability, as it can handle millions of simultaneous connections in distributed clusters, allowing multiple nodes to be added to the cluster to support more devices, and has low latency even with high traffic.

When it comes to security, EMQX uses TLS/SSL for message encryption in transit, username/password authentication, and certificates. In order to protect MQTT topics, ACL (Access Control List) based authorisation is used to control who can publish/subscribe to topics.

In terms of integration capabilities, EMQX allows connection to different types of databases, such as MySQL, PostgreSQL, MongoDB, and Redis. It also allows integration with Kafka, RabbitMQ, and MQTT Bridge (to interconnect brokers) and has plugins for routing rules, persistence, and message transformation.

Once the EMQX broker was set up, it was necessary to configure the MQTT connection to this broker in the reader. To do this, Zebra's web interface was used, as already mentioned. The first step is to ensure that the computer and the reader are connected to the same LAN. Secondly, access the reader via its unique ID or IP address (if a specific address has been assigned) using the browser. The device is protected by a factory username/password, which can be changed by the customer who purchases it. After logging in, you can access the Zebra IoT Connect settings (REFERENCE X), where you will find the options related to the MQTT connection.

The FX9600 fixed reader can be monitored and controlled via MQTT command messages. To this end, these messages must be sent via specific topics and comply with a specific format, which is why several topics have been created in the broker. In order to test the functionality of the MQTT connection between the fixed reader and the EMQX broker, command messages were sent and the reader's responses were observed.

Postman was used to test the MQTT link, connecting to the EMQX broker as an endpoint.

According to [68], Postman is a development tool that helps to build, test and modify APIs. Almost any functionality that could be needed by any developer is encapsulated in this tool, and it is widely used by developers to test, debug, and document APIs. This way, it was possible to test sending commands to the FX9600 fixed reader and receiving its response.

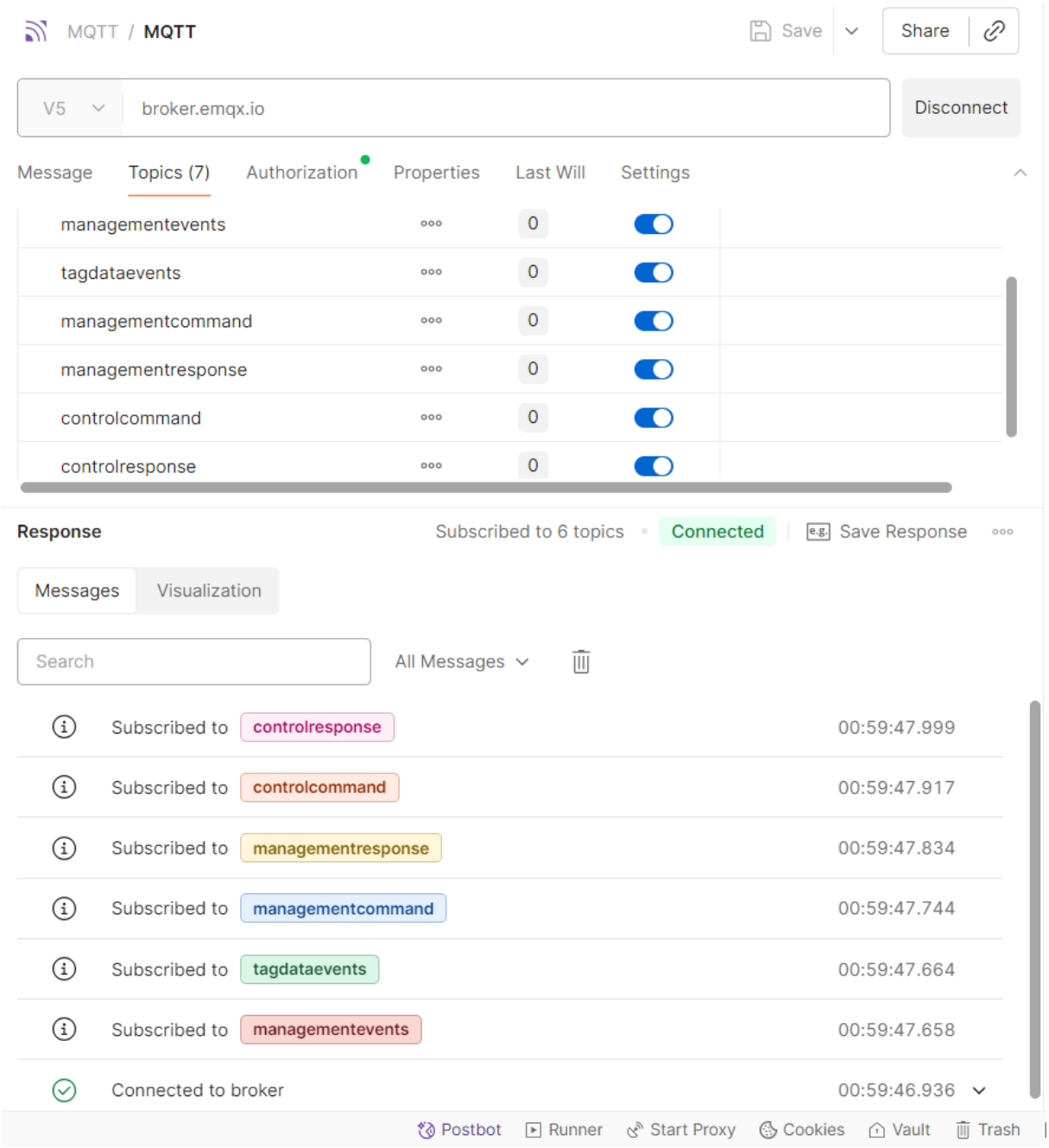


Figure 4.8: Postman desktop application (topic subscriptions)

As mentioned earlier, messages must be sent via specific topics. The ‘controlcommand’ topic allows command messages to be sent to the reader, for example: start/stop tag reading, change operating mode, control LEDs or GPIs. The ‘managementcommand’ topic allows commands related to device monitoring to be sent, for example: obtain configuration, update firmware, change parameters. The ‘controlresponse’ and “managementresponse” topics are

used by the reader to respond to received commands, for example: success, failure, or payloads from 'get' commands. The 'tagdataevents' topic is used by the reader to send tag event messages. Tag events are sent in JSON format with various event parameters, including the time stamp, the ID of the tag read, and the antenna that read the tag. Finally, the managementevents topic is used for asynchronous events related to the device status, for example, reader health status (temperature, memory usage), errors, alerts, or hardware signals such as GPO. It is the ideal topic for monitoring, alerting, and diagnosing reader operation. It is through this topic that the reader sends heartbeat messages.

Having defined the RFID equipment and implemented an IoT platform that meets the requirements set out in Chapter 3, it is also necessary to comply with the defined software requirements.

4.3 Middleware Implementation

The defined architecture requires middleware, i.e., a software service that processes and filters data sent by one or more RFID readers [69–71]. In the context of this project, the middleware consists of a service that runs in background on a local server or VM (Virtual Machine) belonging to the company. Its main purpose is to receive, process and filter tag event messages sent by the fixed reader and convert them into container passage events, as well as to detect anomalous situations in the reading zone. It was decided that the middleware would be developed in Java language.

According to [72–75], there are strong advantages in using Java for developing IoT middleware. In terms of platform independence, it follows the principle "write once, run anywhere", meaning this middleware can run on multiple devices, as long as they have a JVM (Java Virtual Machine). Regarding scalability, Java's strong multi-threading model and ecosystem of scalable frameworks make it well-suited for handling large numbers of connected devices and high volumes of real-time data. When it comes to security, Java comes equipped with built-in mechanisms for secure coding, cryptographic libraries, and authentication systems, helping protect against cyber threats. Java-based platforms support functionality for device provisioning, configuration, monitoring, and updates—simplifying the administration of large-scale IoT device fleets. It also supports edge computing, allowing processing to happen close to the data source (IoT device) for lower latency, real-time analytics, and better bandwidth utilization. Java allows for great interoperability With extensive libraries and protocol support (including MQTT,

CoAP, HTTP), enabling smooth interoperability across varied device ecosystems. Last, not least, Java benefits from a large, active developer community, accelerating development and troubleshooting. As further stated by [76], Java is the best suited programming language for data organization and processing.

Program's structure

Before explaining the structure and content of the Java code developed in greater depth and detail, it is important to mention the context in which it was tested. Field tests were carried out at an urban waste collection and management company, so the system has adaptations that are due to compliance with the requirements established by the company. One of the requirements imposed on the project was to ensure that the results of each container passage detection are published on the company's Kafka server. Another requirement was that the program had to run on a company VM, where it could be monitored remotely and in real time. It was therefore necessary to adapt the original system architecture to meet these requirements. Figure 4.9 shows the architecture adapted for implementation in the company, as well as the flow of information from tag events. Therefore, the middleware's program was developed in Java, using the InteliJ development environment, from which the executable could be generated in '.jar' format and sent to the company's local server or VM to run in the background.

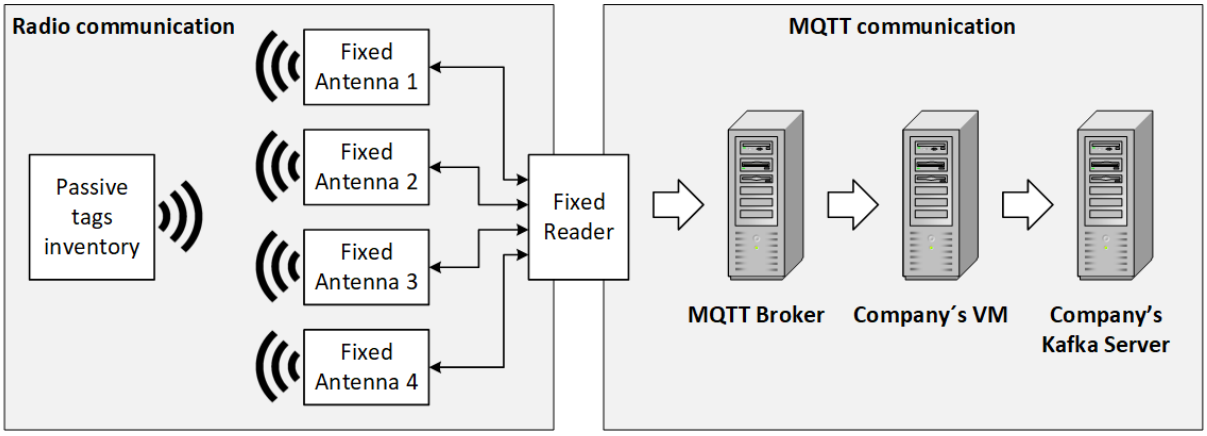


Figure 4.9: Tag events information flow

With the initial architecture modified to adapt to the company's requirements, the middleware program was developed in Java, in the IntelliJ development environment.

Java Libraries

The program must be able to make MQTT connections to the fixed reader, manipulate JSON files, and connect to the company's Kafka server. Therefore, it was necessary to use

Java libraries available online via Maven:

- org.eclipse.paho.client.mqttv3 [77]
- org.apache.kafka.clients [78]
- org.slf4j [79, 80]
- org.json [81]

The Paho project provides code implementations of messaging and standardised protocols aimed at new, existing and emerging applications for M2M (Machine to Machine) and IoT [82]. This library enabled the implementation of MQTT connections between the data processing service and the EMQX broker, as well as the subscription to the topics necessary for communication with the fixed reader.

Apache Kafka is an open source distributed event streaming platform used for high-performance data pipelines, streaming analytics, data integration and applications. Thus, implementations of the Kafka client have been developed, which support publishing messages in topics and inspecting them [83]. This library enabled the implementation of connections between the data processing service and the company's Kafka server, allowing container crossing messages to be sent.

SLF4J (Simple Logging Facade for Java) serves as an interface or abstraction for various logging frameworks (e.g. java.util.logging, logback, log4j) allowing the end user to switch on the desired logging framework at deployment time [84]. This solution was chosen because SLF4J acts as a logging facade, providing a simple and consistent API that can be integrated with different underlying implementations, such as Logback or Log4j. This approach ensures the application's independence from a specific logging technology, increasing flexibility and facilitating future maintenance or migrations. In addition, SLF4J is widely supported by frameworks used in the project, namely Spring and Apache Kafka.

JSON (JavaScript Object Notation) is a lightweight data exchange format and is language independent, most commonly used for client-server communication. Furthermore, it's both easy to read/write and language-independent [85]. It was crucial for the project, given its simple and straightforward implementations for constructing and reading JSON objects, in particular with the JSONObject class. This approach made it simple to parse responses from the FX9600 reader and send JSON messages to Apache Kafka. On the other hand, it is also stated that although json.org provides a way to serialize a Java object to JSON string, there is no way to convert it back using this library. To reach that kind of flexibility, there's a need to switch to other libraries such as Jackson [86, 87].

4.3.1 Java Classes

The list of classes implemented for the middleware's program is shown in the UML (Unified Modeling Language) diagram, in Figure 4.10. The ”Main” class begins by instantiating and executing the threads associated with each topic in the MQTT connections, both Kafka and EMQX. It's important to bear in mind that 'the MQTT client programming model uses threads extensively [88].

The classes dedicated to subscribing to MQTT topics are implemented using callback functions. In many programming languages, particularly when dealing with asynchronous code, callback functions are highly useful [89].

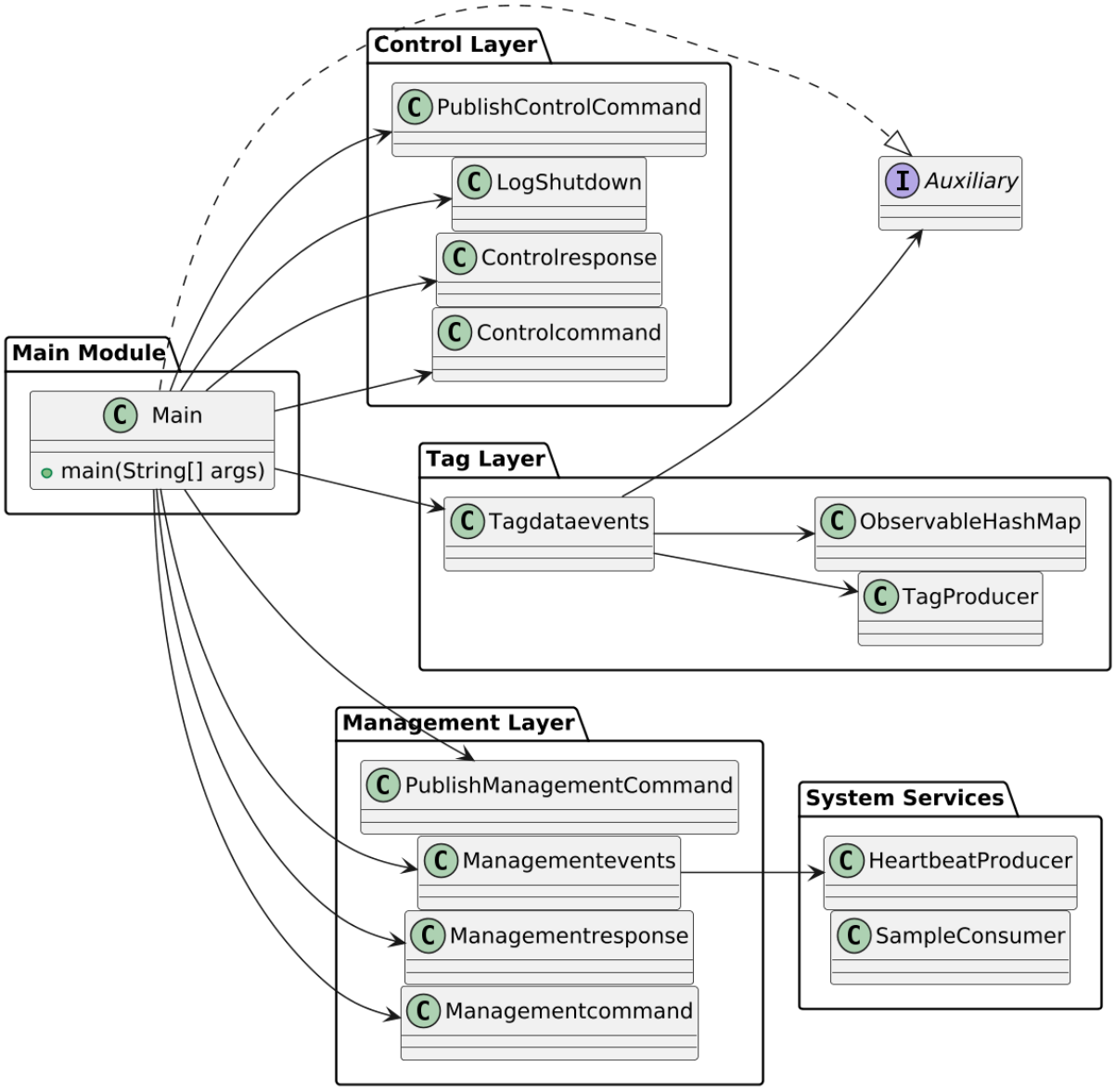


Figure 4.10: Java classes UML diagram

The ControlCommand class subscribes to the controlcommand MQTT topic, enabling

the VM service to send control commands to Zebra's FX9600 reader. The Controlresponse class's function is to subscribe to the controlresponse MQTT topic, which informs the middleware whether each command sent to the reader has been accepted or rejected, and how.

The purpose of the Managementcommand class is to subscribe to the managementcommand MQTT topic, which allows the middleware to send the reader commands to manage its operating status. The Managementresponse class is able to subscribe to the managementresponse MQTT topic, which allows the reader to inform the middleware whether each managementcommand sent to the reader has been accepted or rejected, and how.

The ManagementEvents class makes it possible to subscribe to the topic of managing events the device's operating status, such as the heartbeat. The heartbeat is a mechanism for monitoring the reader's operating status. This monitoring indicates whether the reader is running, how many antennas it is connected to, how many events it has recorded, and more.

The PublishControlCommand class allows control commands to be sent to the reader via the controlcommand MQTT topic, namely the stop and start commands that orders the reader to read or stop reading tags. The PublishManagementCommand class allows management commands to be sent to the reader via the managementcommand MQTT topic. Although not used in this project, this topic must be configured for the reader to accept the connection to the MQTT endpoint.

The SampleConsumer class makes use of the Apache Kafka project's libraries to implement a connection from the project's server to the company's Kafka server and consume a topic's messages. Likewise, the SampleProducer also makes use of the Apache Kafka project libraries to implement a connection to the company's Kafka server. However, its purpose is to produce messages for a topic.

The LogShutdown class creates an utility (LogShutdown) that monitors program termination by registering a shutdown hook—a thread triggered when the JVM exits, whether gracefully (e.g., via Ctrl+C) or abruptly (e.g., system failure). Upon shutdown, it appends a timestamped entry to a log file stating ”Program shutdown intentionally” and echoes the message to the console. It allows to get more information when the program fails.

The ObservableHashMap class implements an ObservableHashMap¡K, V¿, a thread-safe map that combines the functionality of a ConcurrentHashMap with an observer pattern to notify registered listeners whenever the map is modified. It supports standard map operations like put, remove, get, and containsKey, while allowing external code to subscribe to changes via addListener(Runnable). Whenever an entry is added or removed, all listeners are auto-

matically executed through notifyListeners(), enabling real-time reactions—such as updating a UI, logging changes, or triggering RFID-related actions in the container access system. This mechanism allows synchronization between writing and reading in hash maps, preventing failures and crashes related to the lack of this type of synchronization.

The Auxiliary class was used to support the development of the middleware's program. It contains the tag inventory array used for the first field tests, the ArrayList where tags that have been read but don't belong to the company's inventory are registered, a method for printing the commands accepted by the program and the macros used to identify two different company installations. In the long term, this class will no longer be necessary. For example, when the company's tag inventory is registered in a database, the tag inventory array will no longer be used.

The Tagdataevents class is the most relevant, in the sense that it fulfils the main objective of the project, which is to convert the information from tag events into useful information on the passage of waste containers. The class begins by instantiating the three timeouts that are essential to the logic of processing tag events, instantiating them as variables. The ”processtimeout” corresponds to the time interval between the tag being read and the start of its processing. When a tag is read and registered in the hash-maps, it is only processed after 5 seconds, giving the vehicle time to pass through the gate. The ”checktimeout” corresponds to the time interval between each periodic check of the hash-map records, which in this case is set at 10 seconds. The ”removetimeout” is the time interval after which it is assumed that, despite having been detected on one side of the gate, the tag has not completed its passage, and its status is changed from ‘on standby’ to ‘no crossing occurred’. After instantiating these three timeouts, the tag event registration hash-maps are instantiated: ”antennaRegister” and ”tagRegister”.

After the development and testing of the middleware program, the code was uploaded to a GitHub repository as a means of transferring knowledge to the company. Having acquired the necessary equipment and developed the middleware program, it was possible to proceed with installation in the field, beginning testing of the pilot project.

5

Test Scenarios and Results Analysis

The equipment was installed in the company's reception area (Figure 5.1) and the middleware's program was executed to run in the background independently on the company's virtual machine. The project moved on to the field testing phase, thus becoming a pilot prototype. Through various experiments, the system's performance and reliability in real-world industrial environments are evaluated.

Figure 5.1: Company's gateway (view from outside the facility)

Figures 5.2 and 5.3 show the measurements of the gatehouse, to scale, from an oblique

view (3D) and top view (2D) respectively. Measurements up to 5 metres were taken using a tape measure, and measurements over 5 metres were taken using Google Earth.

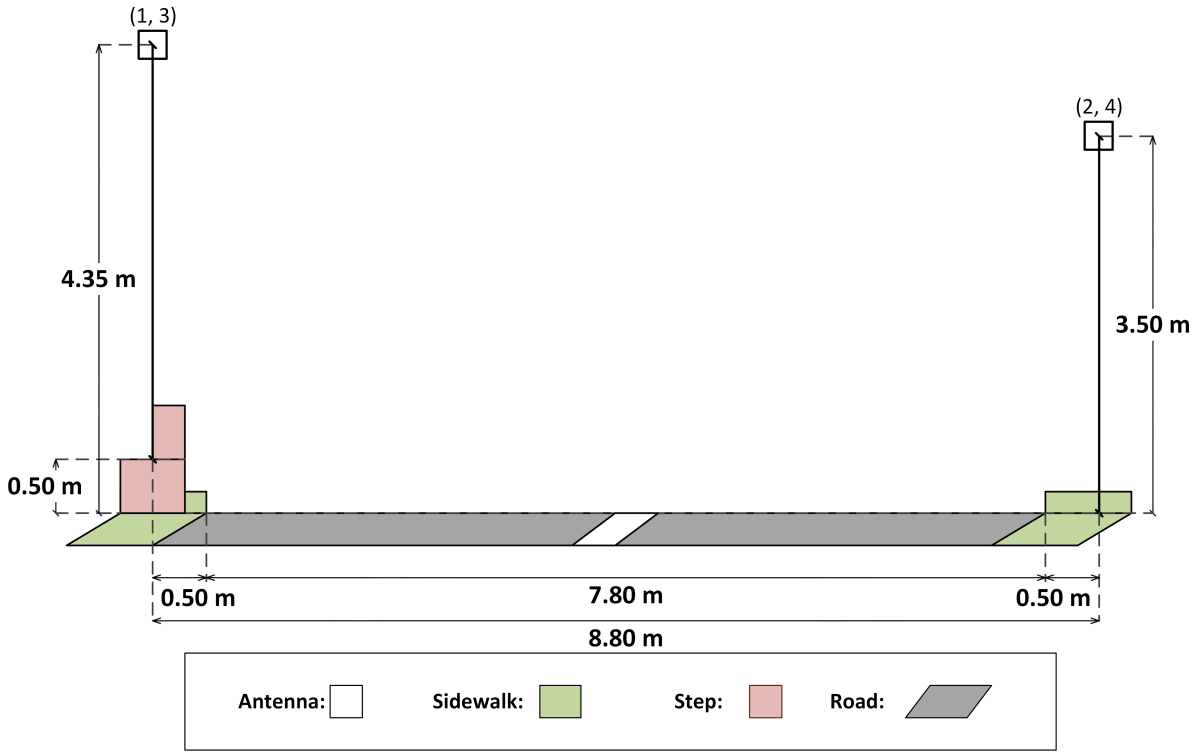


Figure 5.2: Measurements of the gatehouse (outside view, in oblique perspective)

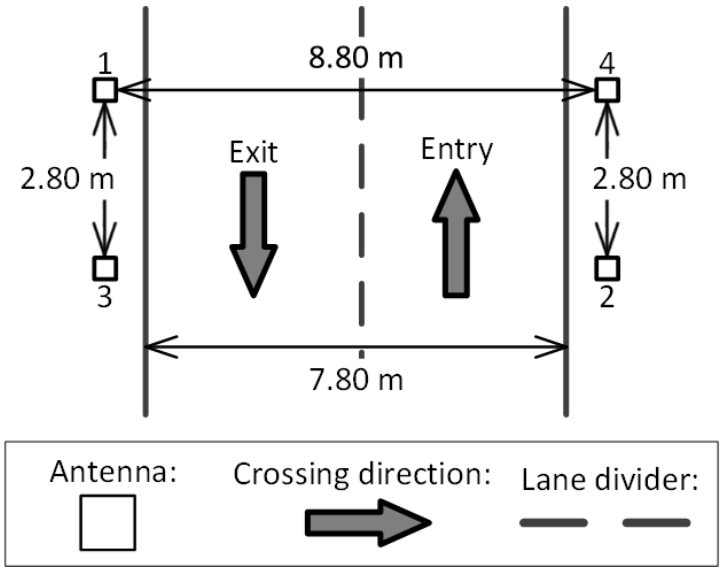


Figure 5.3: Measurements of the gatehouse (view from above)

The developed middleware receives the heartbeat messages from the fixed reader (Figure 5.4) and the information from the tag crossing events sent by the Zebra equipment. After processing this information, it publishes the results of the events on the company's Kafka server (Figures 5.5, 5.6, 5.7, 5.8). Different scenarios were tested, including crossings considered normal, crossings with a pause at the gate and a 'false crossing' in which the tag was only read on

one side of the gate.


```
{
  "Antenna 2: ": "connected",
  "Antenna 1: ": "connected",
  "Time-Stamp: ": "2025-03-11T03:32:24.750+0000",
  "Antenna 4: ": "connected",
  "Antenna 3: ": "connected",
  "Radio Activity: ": "active",
  "Radio Connection: ": "connected"
}
```


Figure 5.4: Message on Kafka server: reader heartbeat


```
{
  "tagType: ": "container tag",
  "tagID": "E2801191A50300617D847815",
  "Instalação": "Blueotter Circular Sacavém",
  "Antenna Time-Stamps: ": [
    "Antenna 1: 2025-03-04T14:32:30.628+0000",
    "Antenna 3: 2025-03-04T14:32:28.592+0000"
  ],
  "Estado da Passagem": "Entrada",
  "TimeStamp": "2025-03-04 14:32:28.592"
}
```


Figure 5.5: Message on Kafka server: entry


```
{
  "tagID": "E200001D1706023411170D3EA",
  "Instalação": "Blueotter Circular Sacavém",
  "Antenna Time-Stamps: ": [
    "Antenna 1: 2025-03-05T10:04:02.381+0000",
    "Antenna 3: 2025-03-05T10:04:03.100+0000"
  ],
  "Estado da Passagem": "Saída",
  "TimeStamp": "2025-03-05 10:04:02.381"
}
```


Figure 5.6: Message on Kafka server: exit


```
{
  "tagType: ": "container tag",
  "tagID": "E2801191A50300617D847815",
  "Instalação": "Blueotter Circular Sacavém",
  "Antenna Time-Stamps: ": [
    "Antenna 1: 2025-03-06T07:44:07.708+0000"
  ],
  "Estado da Passagem": "Em Espera",
  "TimeStamp": "2025-03-06 07:44:07.708"
}
```


Figure 5.7: Message on Kafka server: on standby

```
{
  "tagType: ": "container tag",
  "tagID": "E2801191A50300617D847815",
  "Instalação": "Blueotter Circular Sacavém",
  "Antenna Time-Stamps: ": [
    "Antenna 1: 2025-03-06T07:44:07.708+0000"
  ],
  "Estado da Passagem": "Não Ocorreu Passagem",
  "TimeStamp": "2025-03-06 07:44:07.708"
}
```


Figure 5.8: Message on Kafka server: no crossing occurred

Based on the previously defined requirements and the propagation models adopted, the path losses and received power were calculated for the scenario in question, assessing the feasibility of communication between the reader and the passive tags. Analysis of these results allows the theoretical range of the system to be estimated.

5.1 Link Budget and Detection Range

First, it is necessary to verify whether Friis' free space propagation model is valid in this context. The distance from the Fraunhofer region df depends directly on the working wavelength λ and the largest linear dimension of the antenna D:

$$\lambda = \frac{c}{f} = \frac{3 \times 10^8}{865 \times 10^6} \approx 0.347\ [m] \tag{5.1}$$

$$d_f = \frac{2D^2}{\lambda} = \frac{2 \times (259.1 \times 10^{-}3)^2}{347 \times 10^{-}3} = 0.387\ [m] \tag{5.2}$$

Thus, we can conclude that Friis' model is only valid for distances between the fixed antenna and the tag greater than 0.387 m. In addition to the Fraunhofer zone requirement, the 2.5 and 2.6 must also be verified.

$$d_f = 0.387 \gg D = 0.2591 \tag{5.3}$$

and

$$d_f = 0.387 \gg \lambda = 0.347 \tag{5.4}$$

Therefore, in this context, Friis' free space propagation model is valid. It remains, then, to collect the values of power losses and gains and estimate the range of reliable detection and reading in this context. Therefore, the total propagation losses (uplink and downlink) in free space are given by:

$$PL_{\text{total}} = -10\log_{10} \times \left(\frac{\lambda^2}{(4\pi)^2 \times d^2}\right) \approx -10\log_{10} \times \left(\frac{0.12}{157.914 \times d^2}\right) \tag{5.5}$$

where distance d is the total distance of the RF signal free space propagation and the variable that determines the reading range.

Since manufacturers do not explicitly state whether the modulation of the reader and FX9600 passive tags is ASK or PSK, nor the modulation index used, ASK with a modulation index of 0.8 is assumed, as suggested by [28]. Therefore, the losses due to ASK modulation (κ) are 7.39 dB and the losses due to reflection (Γ) are 1.94 dB.

The length of the coaxial cables differs because the antennas are at different distances from the reader. Therefore, to calculate the attenuation losses in the coaxial cables, the length of the longest cables (20 m) was used. Since the attenuation of coaxial cables is 24.8 dB/100m, the total attenuation (uplink and downlink) introduced by the coaxial cable will be given by:

$$Att_{coax} \times l = \frac{24.8}{100} \times 40 = 9.92\, dB \tag{5.6}$$

Thus, the total loss expression is given by:

$$L_{\text{total}} = PL_{\text{total}} + 2 \times Att_{\text{coax}} - \Gamma - \kappa_{\text{ASK}} \tag{5.7}$$

The transmission power configured in the reader Ptx is 29.2 dBm and the gain of the fixed antennas Gtx (downlink) and Grx (uplink) is 6 dBi in both cases because, as already mentioned in section 4.1, the reader is monostatic. Industrial hard tags typically have a gain of 3 dBi, which is the value used in link budget calculations.

Finally, it is necessary to take into account losses due to polarization mismatch. This effect occurs in both the uplink and downlink, with the loss effect being applied twice in the total link budget path. Thus, the total expression of the link budget is given by:

$$P_r = P_{tx} + G_{tx} + G_{rx} + 2 \times G_{tag} - L_{total} + 2 \times PLF \tag{5.8}$$

Figure 5.9 represents the total losses of the system and the estimated power received by the reader. In order to verify the range of the connection between the fixed antenna and the passive tags, the link distance was varied, comparing the value of the power received by the reader Pr with its sensitivity ($Psens$).

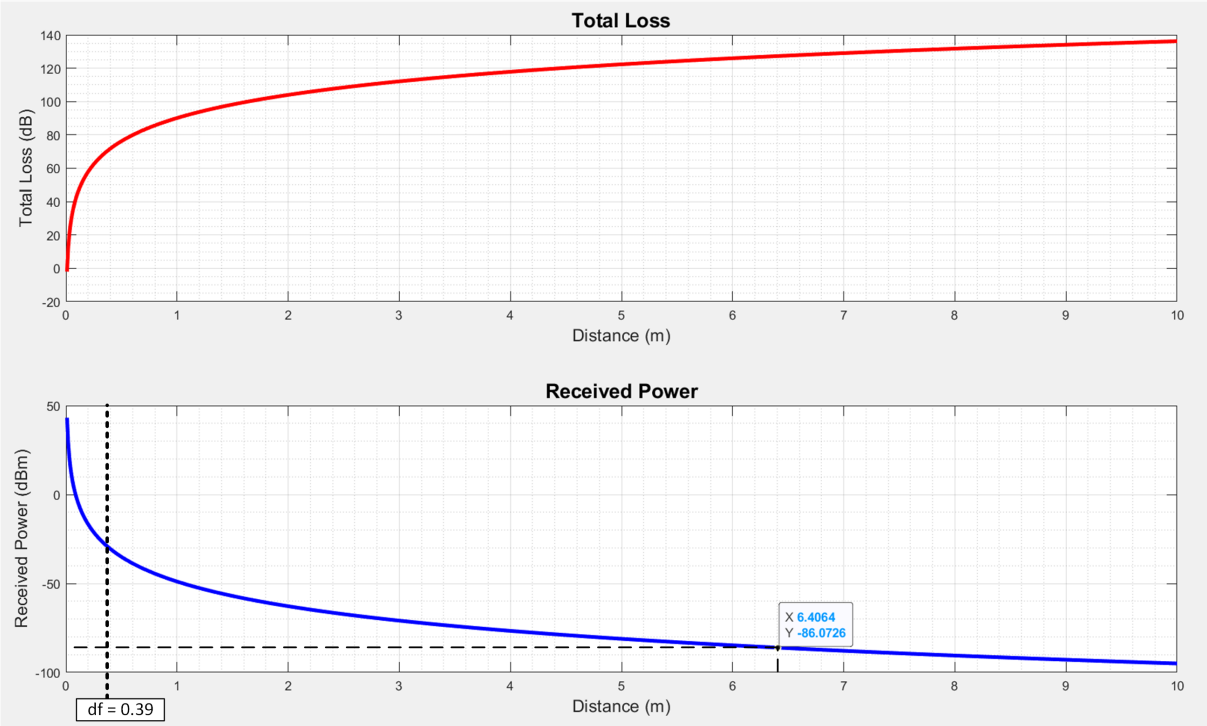


Figure 5.9: Total losses and received power by the reader

This graph shows two important values of the variable distance d. The first is the Fraunhofer distance df, which, as already mentioned, is the distance from which Friis' propagation model is valid. The second value is the distance at which the received power P_r is equal to the reader sensitivity P_{sens}, i.e., it represents the theoretical maximum range for reading tags in this system, in this case approximately 6.41 m. Table 5.1 shows the link budget data.

Table 5.1: System parameters and values

Parameters	**Value**	**Unit**
Reader TX power, P_{tx}	29.2	dBm
Reader TX antenna gain, G_{tx}	6	dBi
Reader RX antenna gain, G_{rx}	6	dBi
Tag antenna gain, G_{tag}	3	dBi
Modulation index, m	0.8	-
Power loss due to ASK modulation, k_{ASK}	7.394	dB
Power loss due to reflection, Γ	1.938	dB
Working frequency, f	865	MHz
Wavelength, λ	0.347	m
Largest physical linear dimension of the fixed antenna, D	259.1	mm
Fraunhofer distance, d_f	387.1	m
Coaxial cable length, L	20	m
Total coaxial cable attenuation, Att_{coax}	9.92	dB
Polarization loss factor, PLF	-3	dB
Reader sensitivity, P_{sens}	-86	dBm
Reading distance, d_{max}	6.41	m

5.2 Test Scenarios and Field Results

As mentioned earlier in section 4.1, the radiation pattern of the antennas is directional, so there is a detection zone and a 'blind' zone for each antenna. In this context, it is important to check which zone is the detection zone and which is the 'blind' zone covering the road at the gate, where the containers pass.

In order to determine the tag detection zone by the antennas, a test was carried out using the following method: starting from the antenna pole with a tag facing it, increase the distance between the two elements horizontally towards the road and record the distance at which the tag was detected. Tests were carried out every 50 cm, with a metal surface behind the tag, resulting in the points shown in Figure 5.10. The figure shows part of the entrance, namely the road and the antenna where sampling was carried out, from the front perspective of someone entering the premises. Five tests were carried out for each height interval, obtaining the detection point by averaging the values obtained in the tests at each height.

The figure shows part of the entrance, namely the road and the antenna where sampling was carried out, from the front perspective of someone entering the premises. Five tests were carried out for each height interval, obtaining the detection point by averaging the values obtained in the tests at each height.

Given that all antennas are of the same brand and model and have been configured to transmit at the same power, it is safe to assume that the radiation pattern is identical between

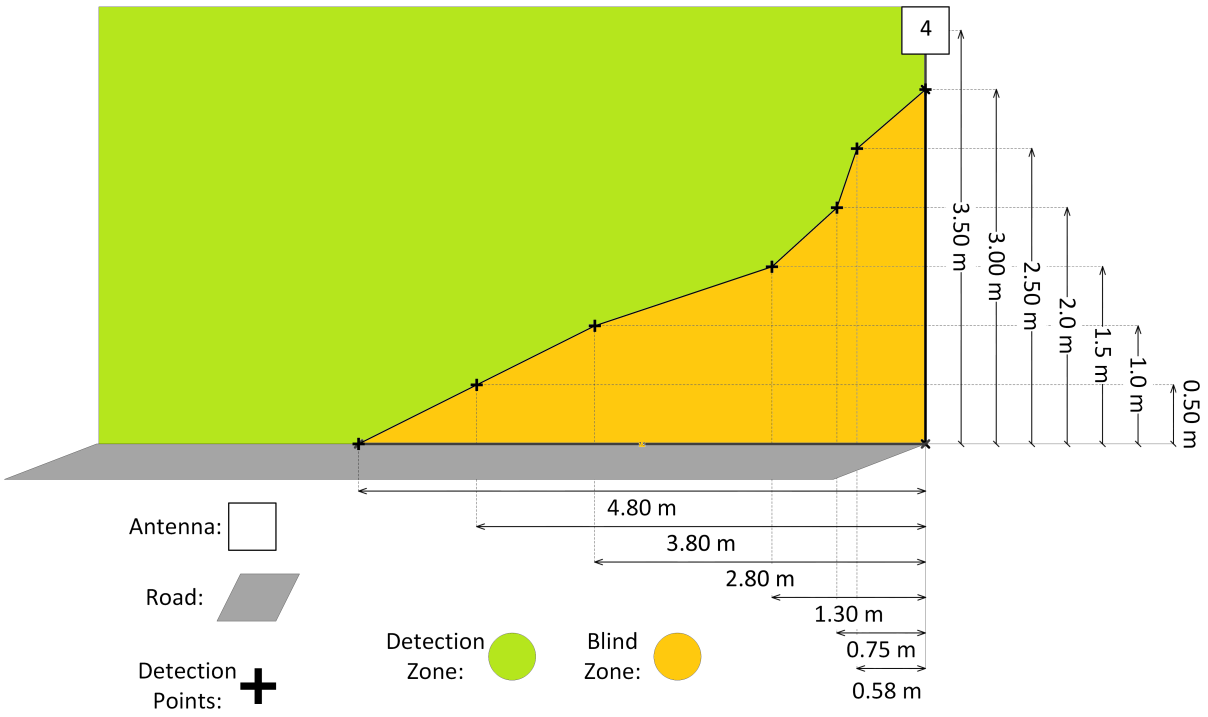


Figure 5.10: Tag detection points by the antenna

them. Knowing that the shape of the main lobe of the antenna radiation pattern is approximately symmetrical around the maximum propagation direction and based on the results in Figure 6.11, the detection zone of the tags by the antennas at the gate was estimated, obtaining the configuration shown in Figure 5.11.

To test the performance of tag detection, the gate was crossed with two rigid RFID passive tags of different models through the antenna detection zone to simulate the passage of industrial containers through the gate. One model was the HID EXO Keg RFID tag [61] and the other was the Tags HID EXO Pro RFID tag [24]. A total of 105 tests were carried out, including: five different passage scenarios, four different heights in relation to the ground and the antennas, two models of rigid tags, with and without a metal surface background.

In order to compare the performance of the two hard tag models, 32 crossings were made at a distance of 1 m horizontal from the antennas, with no metal behind the tags. The results showed that the models have identical behaviour in terms of detection capacity between them. This was expected because, according to their data-sheets, both have up to 10 m reading range. Relating to the middleware, passages at the antenna's heights (3.50 m in the inbound lane and 4.35 m in the outbound lane), all the passage scenarios were correctly received and interpreted .

After concluding that the two tag models behave identically in this context, the impact of unequal heights between the antennas was assessed. For this purpose, crossings were made

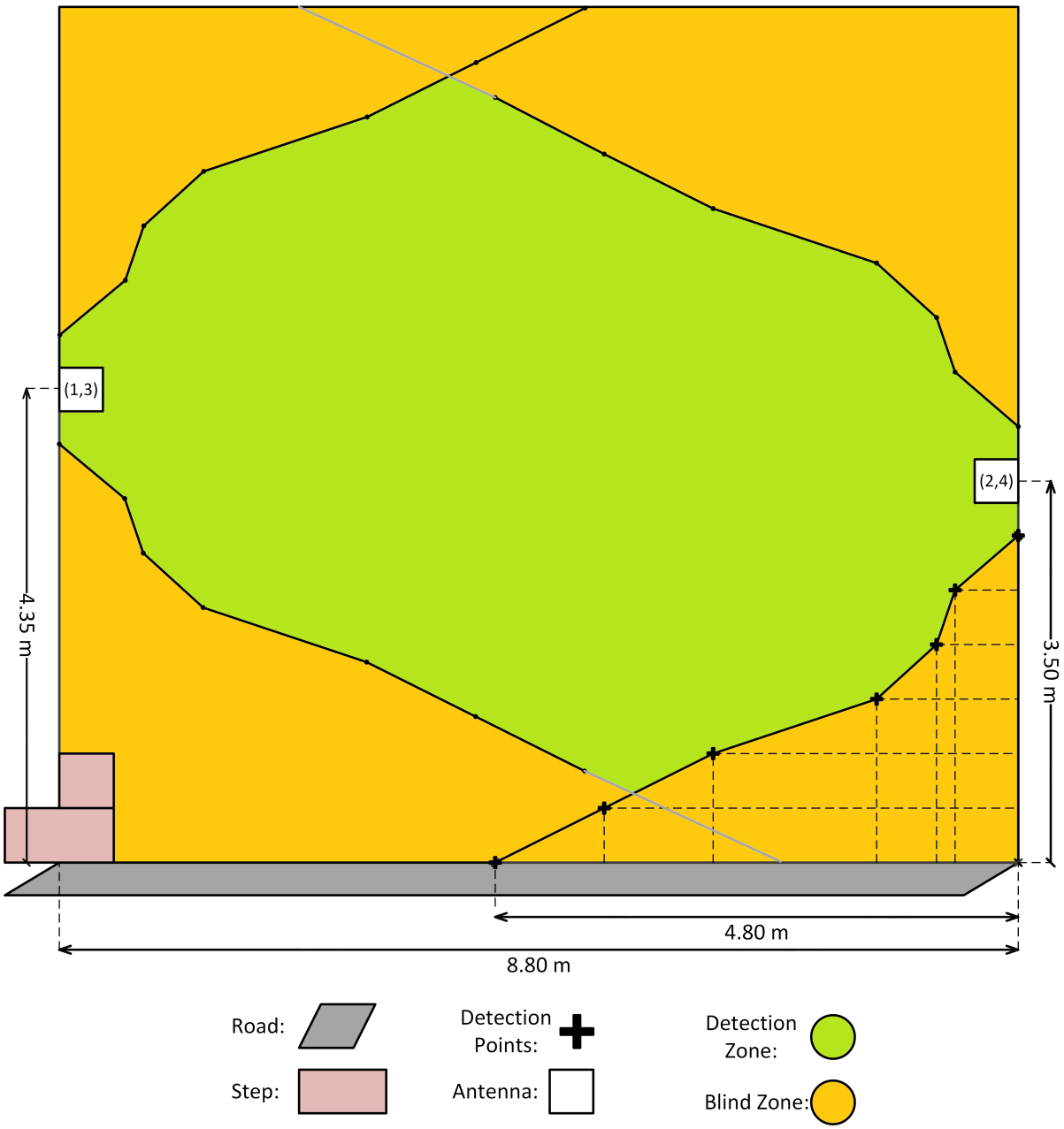


Figure 5.11: Tag detection zone by the antennas on both sides

on the road at a distance of 1 m horizontal from the antenna, with no metal behind the tag. At a height of 3 metres from the ground, the success rate was 64% (14/22), with the antennas on the inbound side achieving the best results (85% - 11/13) and the antennas on the outbound side achieving 6/11 (55%). Although these tests were carried out without metal behind the tag, they show that the unequal heights of the antennas can have a big impact, depending on the height of the tag's passage.

The reading capability using metal behind the tags was also evaluated, repeating the previous procedures as test scenarios. In passages at the height of the antennas (3.50 metres in the inbound lane and 4.35 metres in the outbound lane), the success rate was 96% (25/26). The only scenario that was not correctly interpreted was the non-passage scenario, i.e., a

scenario in which no passage occurred was determined as a passage occurrence. The most plausible explanation is that the tag was detected by an antenna without being supposed to, which indicates that, by applying a metal background, the tag's range increases significantly to the point where the horizontal distance between the antennas is not enough to accurately distinguish the tag's location at the gate. One possible solution, apart from repositioning the fixed antennas, is to adjust their transmission power.

Still using metal as background for the tags, at a height of 3 metres from the ground, 15 passage scenario tests were carried out. The tests showed success in detecting the tag, determining the passage scenario and publishing it on Kafka in all the passage tests, achieving a 100% success rate (15/15).

At a height of 2 m from the ground and still 1 m horizontal from the antenna, on the road, 10 tests were carried out. The success rate for detecting and determining the passage scenario was 60% (6/10), of which it can be seen that the success rate for exits (80% - 4/5) was higher than for entrances (40% - 2/5). Although the exit scenarios showed a better detection success rate, it is important to mention that these same detections were carried out by antennas 2 and 4 (dedicated to determining entries), which reinforces the conclusion previously drawn that the detection and response range of the tags increases significantly when a metal surface is placed behind them, as expected. On the other hand, it is clear that the unequal height of the antennas can cause a mismatch in the success rate between inputs and outputs for certain tag passage heights, also reinforcing the previously drawn conclusion about the impact of the difference in antenna heights.

While the passage scenario tests were being carried out, a small fleet of containers was equipped with HID Exo Pro tags and RFID printed tags that produced results. These results were monitored on the company's Kafka server over six months. The container tests were carried out, with one rigid and one printed tags each, placed on top of the front of the containers (Figures 5.12, 5.13 and 5.14).

Although we knew in advance that printed tags are not suitable for these applications, the company requested verification of the impact and results of both types of tags. Regarding the rigid tags, the vast majority of the containers were detected, although in several passages the scenario was not correctly determined. The most plausible explanation is that the tags were not positioned correctly. Further on, in section (5.4), a recommendation for the installation of the RFID equipment is made, based on the results obtained in the pilot project's field tests. Furthermore, none of the printed tags was detected. Therefore, it was concluded that the rigid

tag's position needs to be optimized and confirmed that the printed tags are not suitable in this context.

Figure 5.12: Container with tags (rigid passive RFID tag)

Figure 5.13: Container with tags (printed passive RFID tag)

Figure 5.14: Container with installed RFID tags

5.3 Financial Analysis Model

Finally, relating to the company's pilot project, a relatively simple financial analysis model was developed to assess the impact of the project on the company's profits. The model is divided into four main financial impacts: CAPEX (Capital Expenditures), OPEX (Operational Expenditures), earnings and results, where the resulting profit is obtained by subtracting CAPEX and OPEX costs from earnings.

The following constants were used for the calculations: average salary in Portugal of €1,602 and 180 working hours per month, resulting in an average salary of €8.9/hour. It was also assumed that the system would be installed in the company's six facilities.

CAPEX costs are the ones associated with the acquisition or upgrading of fixed assets. Thus, these costs include the acquisition of RFID material and the labour costs for installing it. Table 5.2 shows the costs taken into account in the CAPEX calculation. It was assumed that the RFID system would be installed in six facilities (company's current number of facilities). Equipment prices are approximately those found on the market. Labour was calculated based

on the current national average wage, assuming that one worker per facility will be hired.

Table 5.2: CAPEX costs

Fixed Reader	
Quantity (un)	6
Unit price (€)	1000
Total equipment cost (€)	6000
Fixed Antennas	
Quantity (un)	24
Unit price (€)	200
Total equipment cost (€)	4800
Coaxial Cables	
Quantity (un)	24
Unit price (€)	50
Total equipment cost (€)	1200
Tags	
Number of containers with tags	200
Quantity (un)	400
Unit price (€)	5.5
Total equipment cost (€)	2200
Labour for tag placement (internal)	
Number of employees	6
Hourly labour cost (€)	8.90
Number of working hours	200
Total labour cost (€)	10680.00
Civil labour (external)	
Number of employees	6
Hourly labour cost (€)	8.90
Number of working hours	20
Total labour cost (€)	1068.00
Electrician labour (external)	
Number of employees	6
Hourly labour cost (€)	8.90
Number of working hours	20
Total labour cost (€)	1068.00
Total CAPEX cost (€) = 27016	

OPEX costs are associated with the maintenance of fixed assets. Thus, these costs include the replacement of damaged tags, VM usage, software updates, and labour costs. Table 5.3 shows the costs taken into account in the OPEX calculation. Once again, it was

assumed that the RFID system would be implemented in the company's six current facilities, labour was calculated based on the current national average salary, and it was assumed that one worker per facility would be hired.

Table 5.3: Annual OPEX costs

Replacement of damaged tags (annually)	
Number of tags initially purchased (un)	400
Tags to be replaced (%)	10
Number of tags to replace (un)	40
Unit cost (€)	5.5
Total cost of equipment (€)	220
VM cost (annual)	
Daily cost of VM (€)	0.1
Number of days of VM usage	365
Total annual cost of VM (€)	37
Labour for tag placement (internal) (annual)	
Number of employees	6
Hourly labour cost (€)	8.9
Number of working hours	20
Total labour cost (€)	1068
Software/firmware maintenance labour (internal) (annual)	
Number of employees	6
Hourly labour cost (€)	8.9
Number of working hours	12
Total labour cost (€)	641
Total OPEX cost (€) = 1965	

The financial gains from the project (Table 5.5) are mainly twofold: increased operational efficiency of containers and reduced losses due to fraud. In terms of operational efficiency, it is demonstrated how digital tracking of containers allows for better management of containers parked at the facilities. By knowing exactly which containers are parked at each facility, the company has more reliable and accessible information to manage them in order to profit from their use. On the other hand, as mentioned in the 5.2 section, manual recording of container movements is not entirely feasible, as some containers pass through the gate without being recorded (manually). Thus, digital recording of movements reduces losses due to container fraud, as more secure recording of container movements discourages attempts at fraud.

Table 5.4: Annual earnings

Operational efficiency (annually)	
Number of containers with tags (un)	200
Containers on standby (%)	10
Container rental cost (€)	1000
Rental cost of all stationary containers (€)	20000
Fraud Reduction (annually)	
Number of undetected container crossings	100
Undetected crossings involving fraud (%)	2
Number of undetected container shipments involving fraud	2
Average transport capacity of a container (tons)	7
Average value of the contents of a container (€/ton)	200
Average value transported per container (€)	1400
Average amount lost to fraud (€)	2800
Post-project fraud reduction (annually)	
Reduction in the number of unauthorized container transits (%)	70
Number of undetected container shipments involving fraud (post-project)	30
Average amount lost to fraud (post-project) (€)	840
Value gained from fraud reduction (€)	1960
Total Earnings (€) = 21960	

Finally, having calculated the CAPEX and OPEX costs and the project's gains, it is possible to assess the financial impact of the project over the years, as shown in Table K. It can be seen that the company recovers its investment in the year following the implementation of the project, as CAPEX costs are only applicable in the first year. Assuming relatively constant annual OPEX costs, the company's profit should be around €19,995 from the second year onwards.

Table 5.5: Annual profits

Annual profit results (€)	
Year 1	-7021
Year 2	19995
Year 3	19995
Year 4	19995

After analysing the pilot project's results, a recommendation was made regarding the installation of the equipment. The results obtained in the field were taken into account, as well as European standards for the size of containers and lorries and equipment safety.

5.4 Results Analysis and Recommendations

In order to optimise the placement of equipment, it is necessary to take into account the size of the containers and lorries that transport them. In this project, the focus is on skip-type waste containers, these being the most commonly used for transporting industrial waste. Thus, the European standards regulating the dimensions of industrial containers and the vehicles that transport them were consulted. Typical values for these dimensions were also collected, because although the standards and directives impose maximum limits, these dimensions can vary significantly in relation to these limits.

Directive 96/53/EC specifies the maximum dimensions for industrial transport vehicles, which are: a maximum length of 12 m, a maximum width of 2.55 m and a maximum height of 4 m. All these measurements include the container, i.e. the vehicle with the container attached must comply with these maximum measurements.

The DIN 30722 technical standard defines limits for the maximum size of industrial containers, which are: a length of 7 m and a width of 2.55 m. Although the maximum height and volume are not strictly standardised by this standard, the implementation of DIN 30722 and Directive 96/53/EC together often implies a maximum height of 2.4 m and a maximum volume of between 36 and 38 m^3.

The directives and standards specify maximum values for the dimensions of industrial containers and vehicles. However, they do not specify minimum or typical values for these dimensions. Therefore, AI (Artificial Intelligence) tools were used to gain an understanding of the typical and minimum values of industrial container and vehicle dimensions. According to [90], the typical height of container transport lorry chassis is 1 to 1.5 m, the typical height of industrial containers is 1 to 2.5 m, and the typical width of lorries together with containers is 2 to 2.5 m. These values give us two limits for the typical size of container lorries, with minimum limits of 2 m in height by 2 m in width and maximum limits of 4 m in height by 2.5 m in width.

Industrial container suppliers were consulted to confirm the values provided by the AI tools. [91], from UK (United Kingdom), supplies containers within the following minimum and maximum dimensions: 0.97 to 2.44 m in height; 1.02 to 6.17 m in length; 1.47 to 2.40 m in width; 3 to 30.6 m^3 in capacity. [92], from Turkey, supplies containers within the following minimum and maximum dimensions: 0.97 to 2.68 m in height; 1.83 to 6.10 m in length; 1.29 to 2.44 m in width; 3.05 to 30.6 m^3 in capacity. [93], from UK, supplies containers within the following minimum and maximum dimensions: 1.30 or 2.60 m in height; 6.10 m in length; 2.44 m in width; 15 or 30 m^3 in capacity. [94], from Germany, supplies containers within the following

minimum and maximum dimensions: 1.25 or 2.50 m in height; 3.20 to 4.40 m in length; 1.80 or 2.00 m in width; 5 to 10 m^3 in capacity.

”Based on the values found, it was possible to estimate the typical average and minimum values of industrial containers. In order to design the system for ‘extreme’ values of vehicles with mounted containers, the following limits were chosen for the maximum and minimum container sizes: 1 or 2.5 m in height and 2 or 2.6 m in width. As for the vehicles, it was decided to use 1 or 1.5 m for trailer height. Since the tags are placed on the containers, the dimensions of the vehicle cabins were not taken into account.

For security reasons, tags should be installed at the top of the container, at least 2.5 m high, to hinder and discourage vandalism. As the height of the top of containers mounted on lorries can vary between 2 and 4 m above the ground, the tag detection zone should be centered at 3 m above the ground. Therefore, it is recommended that the antennas be installed 3 m above the ground in order to center the main lobe of their radiation pattern within the height range of the containers being transported.

Considering that the height of lorry trailers can vary between 1.0 and 1.5 m high, the following installation methodology is recommended: In containers less than 1.80 m high install the tag as high as possible in relation to the base of the container; In containers 1.8 m high or more try to install the tag at a height of approximately 1.8 m from the base of the container, allowing the tag to be at a height of approximately 3 m (between 2.8 m and 3.2 m) when the container is mounted on the lorry.

Figure 5.15 illustrates the recommended installation of tags on containers, viewed from the rear of the truck with the container mounted. On the left is a representation of the minimum dimensions of the truck with container (with the respective tag installation areas) and on the right is the equivalent for the maximum dimensions.

Although there are standards and directives that regulate and classify vehicle access gates, they do not classify them according to size or associated infrastructure. Therefore, a classification system was developed for this project, identifying the architecture of the gateway in terms of its width and type of infrastructure. In terms of width, each gateway are be classified as small, medium, or large, based on tag detection range. In terms of infrastructure type, industrial access gates are generally classified into two types: simple and gantry. The classification criteria are explained below.

With regard to the object detection range within the scope of this project, the most limiting parameter is the reading range of the rigid tags themselves. On the other hand, the reading

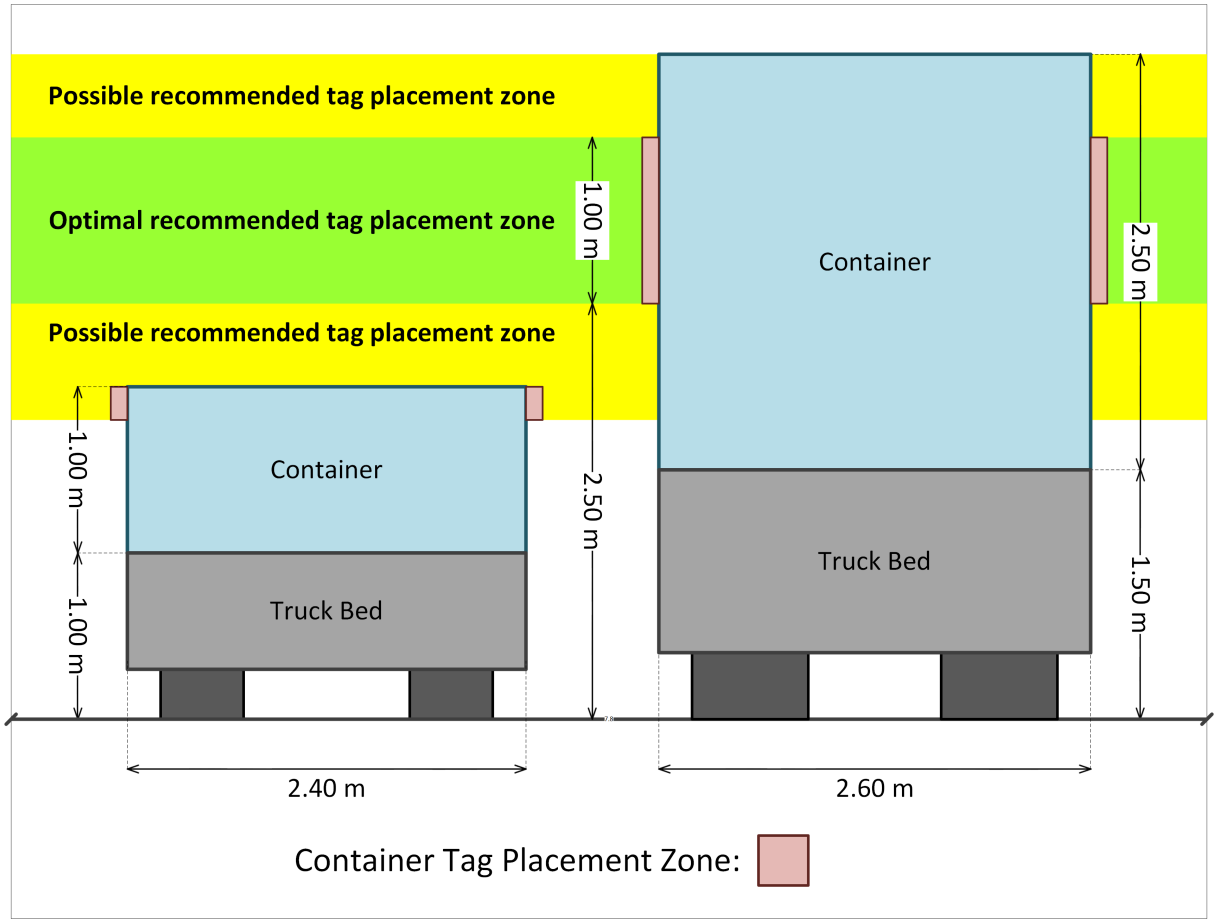


Figure 5.15: Tag placement areas

range of the antennas can be adjusted by setting the transmission power value on the reader. However, due to the backscatter technique used in passive RFID, it is not possible to directly adjust the tag's detection range. As mentioned in Chapter 4, Section 4.1, the range of HID EXO Pro rigid tags, as specified by the manufacturer, is 10 m.

In the case of a simple gate, there is no infrastructure in the area to be controlled. In these cases, the area of vehicle flow with containers consists essentially of a road, which may or may not be delimited by side-walks. It may even contain gates or barriers if it is a vehicle access point to facilities. In these scenarios, at least four antennas must be installed to enable the middleware algorithm to interpret container passage events.

Small simple gateway

If the distance between the antennas on opposite sides of the road is 10 m or less wide, the probability of the tags being read by antennas on opposite sides of the road is very high. Therefore, in these cases, the gateway belongs to the small gatehouse category. This is the case of the gate where the pilot project was implemented and tested, measuring 7.80 m in

width. Based on what was observed in the pilot project tests, one of the precautions to be taken with this type of gatehouse is the risk of unwanted cross-readings between antennas, i.e., overlapping of main lobes of radiation patterns. Thus, in the case of small gateways in particular, it may be necessary to adjust the transmission power of the antennas more carefully in order to fine-tune the coverage area of each one.

Figure 5.16 shows, to scale, an example of a small simple gate and two vehicles with containers, as well as the detection zone and the blind zone in relation to the antennas. In this figure, no mandatory directions of passage are distinguished, leaving it to the system to be capable of identifying them throughout the entire container detection area.

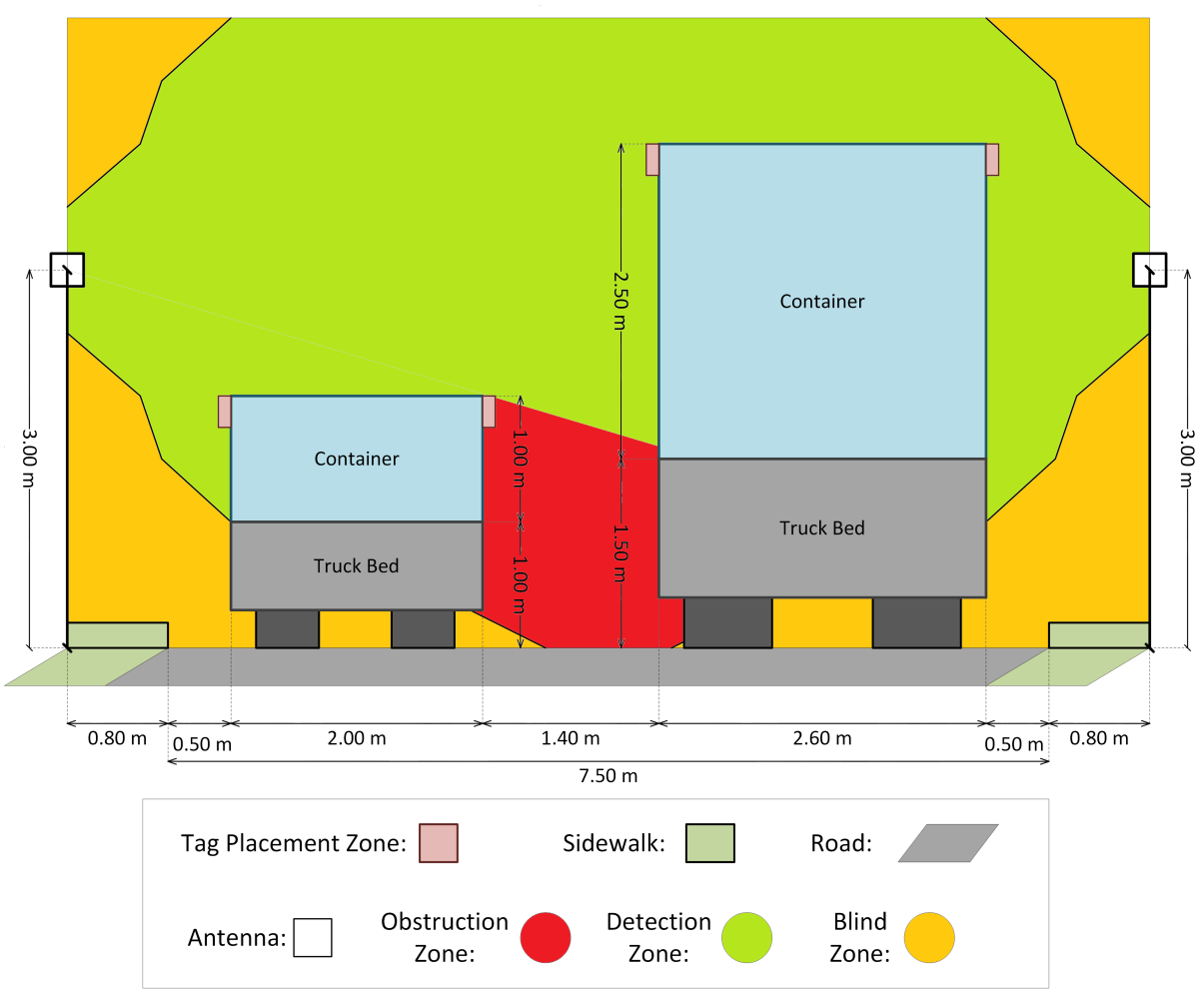


Figure 5.16: Small simple gateway equipment installation example

The vehicle with a container on the right represents the maximum dimensions of such vehicles according to the European standards and directives mentioned above, with the tap positioned outside the optimal zone in order to represent the limit case. The vehicle on the left represents the minimum dimensions according to typical European values. The representation of the detection zone and blind spot used are experimental results obtained from the pilot

project. Given the directional radiation pattern of the antennas, it is recommended to install them at some distance from the edge of the walkway in order to obtain a larger coverage area for tag detection.

It should also be noted that vehicles never pass too close to the side-walk, so this distance should also be taken into account. In the pilot project, it was recorded that vehicles generally pass between 60 and 120 cm from the side-walk. This is important because the tag detection area shrinks the closer the vehicle passes by the antennas, due to their directivity. In the image, this distance was represented as 50 cm, again in order to represent the limit case.

Medium simple gateway

In order to provide tag reading coverage on a road without the need to reinforce it with the installation of additional RFID equipment, the maximum distance between the antennas on opposite sides of the road is 20 m. Thus, if the distance between the antennas on opposite sides of the road is greater than 10 m and less or equal than 20 m, the gate is classified as medium. Figure 5.17 shows, to scale, an example of a medium simple gate and four vehicles with containers, as well as the detection zone and the blind zone in relation to the antennas. The distance between the antennas was set to 20 m in order to represent the tag detection limit case. In addition, it is assumed that the transmission power of each antenna has been adjusted to achieve a detection range of 10 m, so as to cover the entire road without overlap of coverage between its opposite sides. In this case, no mandatory directions of passage are distinguished, leaving it to the system to be capable of identifying them throughout the entire container detection area.

Although it is possible to provide coverage for the entire road, an undesirable obstruction may occur. As shown in red in Figure 5.17, if a vehicle with a larger container passes at the same time as a vehicle with a smaller container, the passage may not be detected, leading to the event not being recorded or being misinterpreted by the middleware. However unlikely this situation may be, the failure cannot be disregarded. Therefore, to obtain a more robust solution for this scenario, two options arise: reinforcing the passage area with additional RFID equipment or installing supplementary infrastructure, such as gantries. These solutions will be explored in greater detail below.

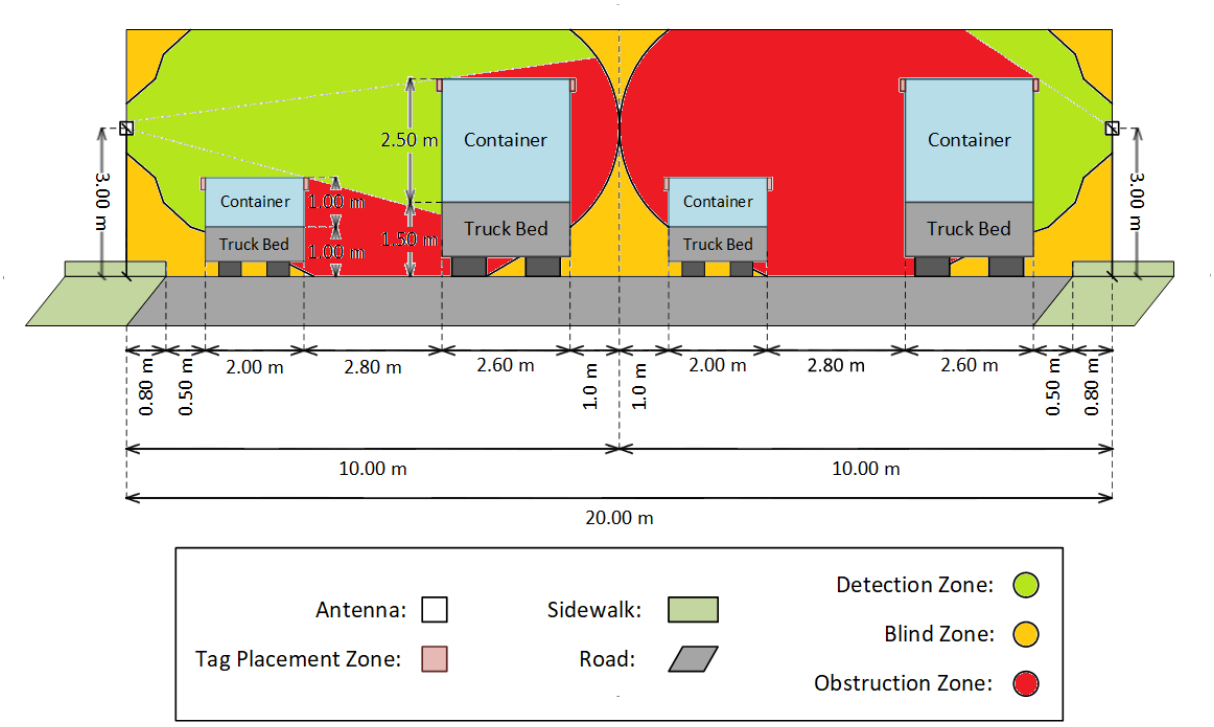


Figure 5.17: Medium simple gateway equipment installation example

Large simple gateway

If the gate is larger than in the previous case, the distance between the antennas on opposite sides of the road is greater than 20 m, jeopardising coverage of the tag reading zone. It will therefore be necessary to reinforce coverage of the reading zone with more RFID equipment, installing more antennas and fixed readers and longer coaxial cables. In this case, the gate is classified as the larger type.

Figure 5.18 shows an example of a Large Simple Gateway. In practice, the solution of installing additional RFID equipment makes it possible to convert an excessively wide gate into two or more smaller gates, providing tag detection coverage across the entire road. This greatly reduces the likelihood of containers obstructing each other's detection.

With regard to this type of solution, there is a disadvantage that may become significant: the length of the coaxial cables. In order to reach the antennas along the entire width of the road, it would be necessary to install coaxial cables that are considerably longer than those used in a small single gate. This factor has two direct impacts: the coaxial cable power losses and the cost and time of implementation.

With respect to the cable power losses, it was mentioned in Section 4.1 that the coaxial cables suffers losses of 24.8 dB/100 m, which means that, compared to a small single gate of 7.50 m, a wide gate of 24 m could, in the worst-case scenario, more than triple the level of power losses in the longer cables.

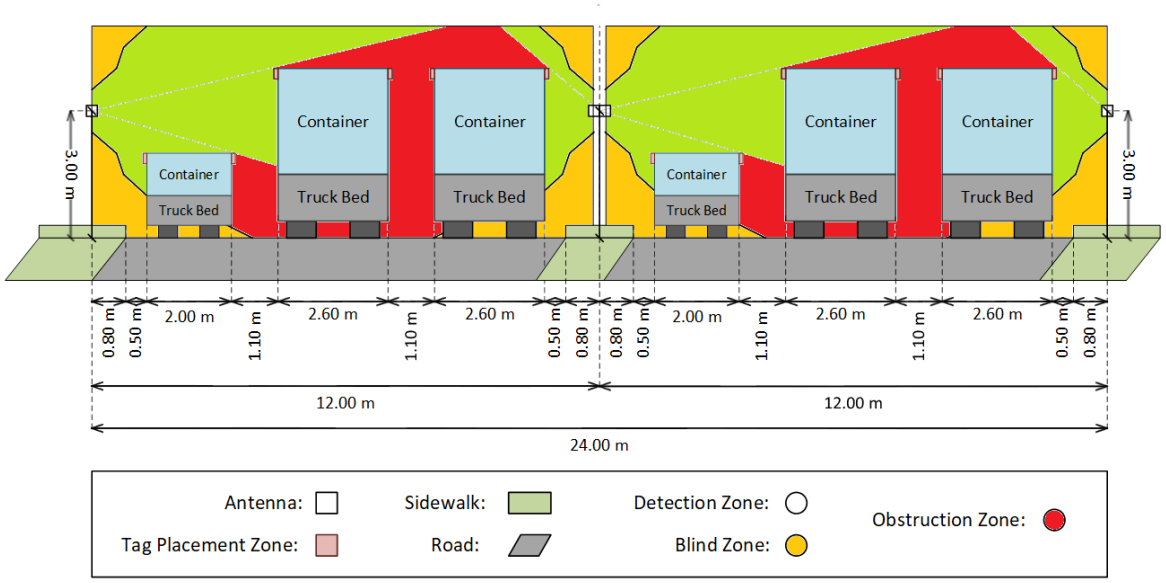


Figure 5.18: Large simple gateway equipment installation example

As for the implementation costs of a large simple gate, since the cables are installed underground, both the cost and duration of the installation works could also increase threefold, compared to a small single gate. One way of avoiding the installation of underground cables would be the construction of gantries, or the use of ones already pre-built on the premises.

Large gantry gateway

There may even be cases where a simple gateway is not adequate and it is necessary to reinforce its infrastructure, for example by installing gantries. In this case, the gatehouse would be classified as a gantry type, in terms of its infrastructure type. If the infrastructure already exists, it should be utilised. The main advantage of this type of access is that the directions of passage are pre-determined. As a result, the middleware does not require an algorithm to determine the direction of passage and can be adapted accordingly, requiring fewer threads to run simultaneously and asynchronously, thereby consuming fewer resources on the host machine. Furthermore, it is not necessary to install four antennas per road, but rather one for each traffic lane.

Let us take as a reference the access control system of MARL (Lisbon Region Supply Market). The vehicle access gantries at MARL are channelled and organised, particularly due to its size and the need to manage the constant flow of vehicles. With the aid of Google Earth, the following measurements were taken: the gantry structure measures approximately 43 m in length across all lanes and lane dividers; each lane measures approximately 3 m in width; and each lane divider measures 1 or 2 m depending on whether it contains a control booth or

not; the structure allows the passage of vehicles with a maximum height of 4.5 m. Figure 5.19 shows a section of a controlled vehicle access based on that of MARL.

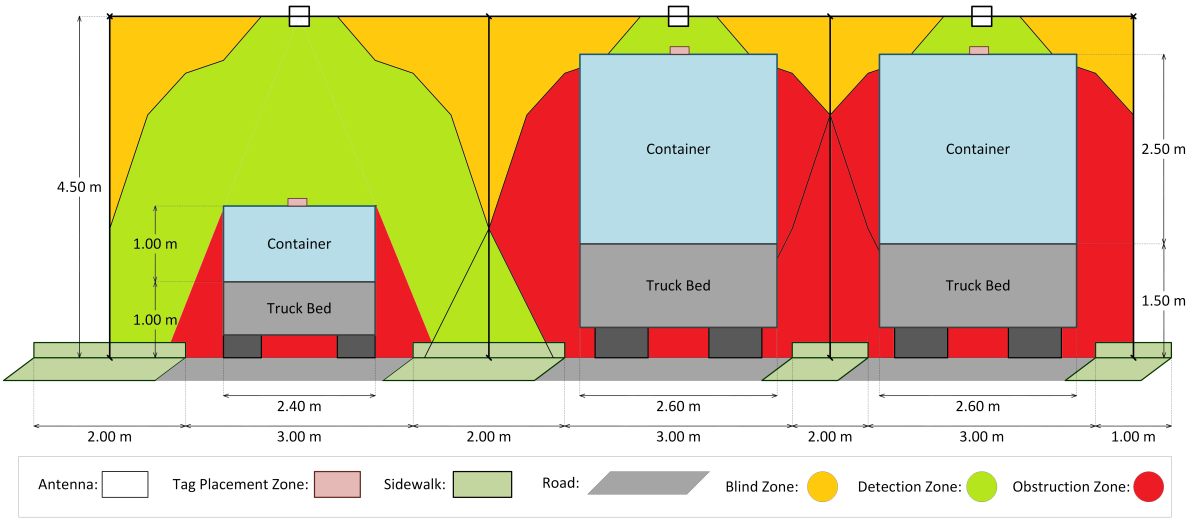


Figure 5.19: Large gantry gateway (classic implementation example)

This case represents the most common installation strategy on gantries, where the antennas are placed above the passage area, directed vertically downwards. This type of installation presents certain disadvantages. The first is that it requires the tag to be installed facing upwards, which becomes highly challenging in industrial containers as it is more exposed to physical impacts, for example when containers are stacked inside one another. The second disadvantage lies in the fact that the implementation is geometrically very different from the previous solutions, thereby disrupting the standardisation of large-scale deployment of this system. Thus, it was proposed to implement an alternative method of installing the equipment, as shown in Figure 5.20.

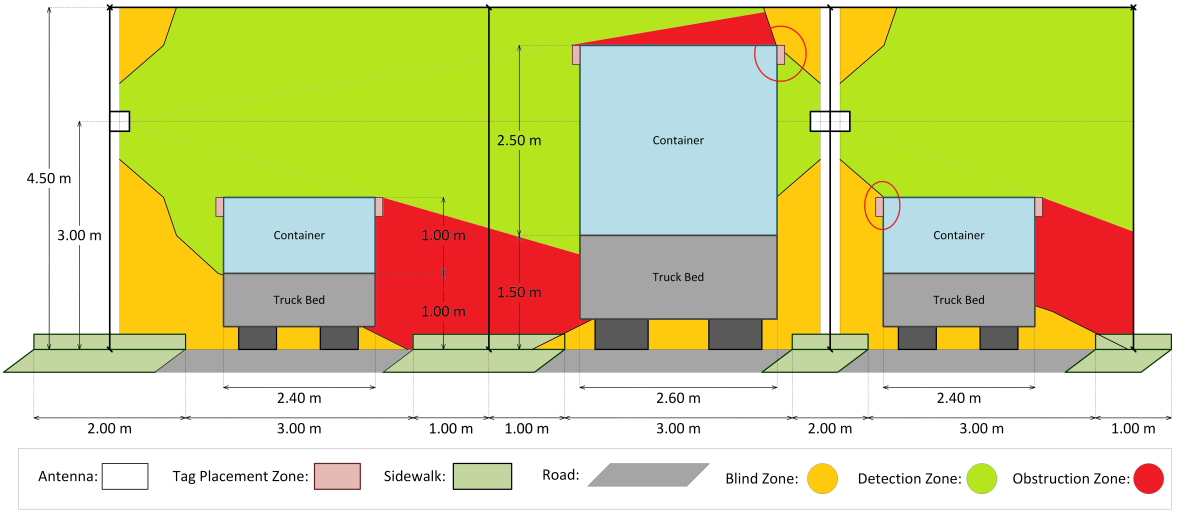


Figure 5.20: Large gantry gateway (normalized implementation example)

It can be seen that, at certain angles, there may be no coverage in the container tag passage area, as shown by the tags marked with a red circle. This happens when the lane divider pavement is too narrow, forcing the antennas to be installed too close to the road and therefore reducing the tag detection coverage. A possible solution is to install additional antennas on the narrower pavements at different heights, providing wider coverage. Installing them at 2 m and 3.5 m is suggested to ensure good detection. In this way, the standardisation of the recommendation for tag installation on containers is maintained, without compromising coverage in the container passage area.

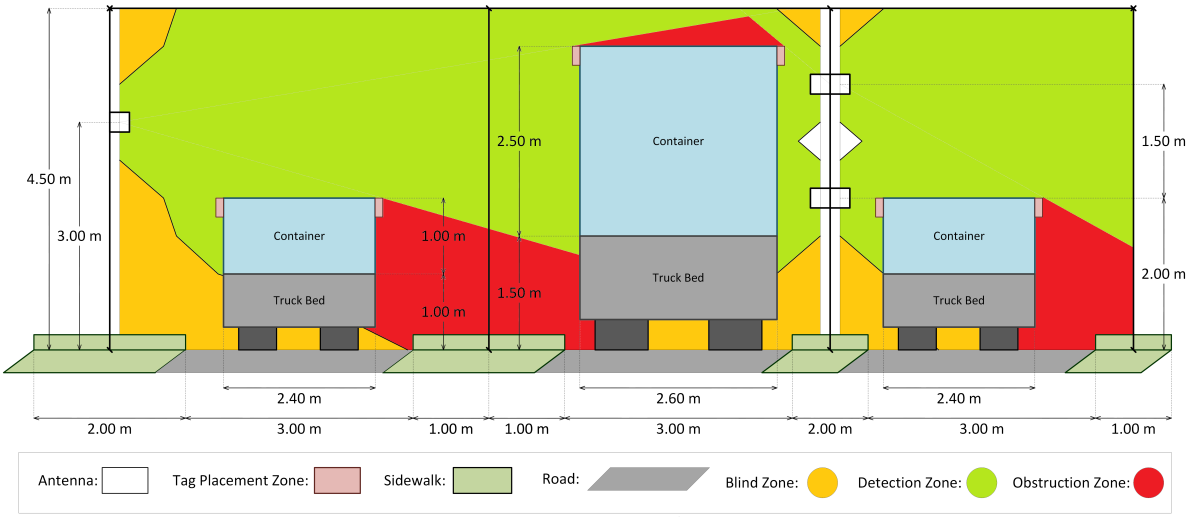


Figure 5.21: Large gantry gateway (Re-enforced normalized implementation example)

Having made the recommendations for the installation of RFID equipment in various scenarios, a further set of possible additional optimisations for this proposed system is recommended, representing suggestions for future work.

6
Conclusions

In conclusion, UHF passive RFID solutions demonstrated potential effectiveness when it comes to controlling access to industrial and urban containers. From all the passive tags crossing scenarios tested it was possible to conclude that: 1) The tag models acquired have identical performance in detection range; 2) The unequal heights of the antennas can have a large impact on the tag's detection statistics, depending on the crossing's height; 3) The tag's detection range increases significantly when using a metal background, due to constructive reflection effects that improved tag backscatter efficiency. The containers that already had tags attached produced results, revealing that the printed tags were not suitable for this application and the rigid tag's position on the container should be optimized.

One of the main contributions of this project was the development of installation guidelines for the implementation of passive UHF RFID systems at gateways. Based on experimental analysis and prototype tests, it was possible to identify installation solutions to different gateway scenarios. These recommendations serve improve traceability, provides higher reliability of access control processes, and support for efficient waste management.

6.1 Main Conclusions

The implementation of the system using the MQTT protocol proved to be an efficient choice for real-time data exchange between the reader, endpoints and the central server. Its lightweight nature and compatibility with IoT architectures allow seamless integration, ensuring low latency. Deploying the broker on a VM further enhanced flexibility and robustness, enabling centralised management and facilitating future scalability of the system.

The theoretical analysis of the link budget provided valuable insight into the expected performance of the RFID system. By accounting for free-space path loss, cable attenuation, and antenna and tag gains, the model was able to approximate detection range (6.41 m) values with good accuracy.

In the context of physical security in industrial environments, passive UHF RFID systems play a key role in deterring and preventing container theft, through access control, traceability, and real-time unauthorized detection. Full visibility of the logistics chain increases the perceived risk for offenders, acting as a psychological deterrent.

A financial analysis highlighted the economic viability of adopting passive UHF RFID solutions for container access control. While the initial investment is driven by infrastructure costs, namely readers and antennas, the negligible unit cost of passive tags ensures scalability and long-term sustainability. Compared to active RFID or alternative tracking systems, the passive approach offers a favourable cost-benefit balance, particularly when applied to large-scale deployments in industrial environments.

The prototype tests demonstrated that the system is robust to normal operating conditions, both in hardware and software terms. The use of a VM for server deployment proved resilient, offering rapid recovery in case of failure and supporting redundancy mechanisms. Nevertheless, operational reliability remains sensitive to antenna placement and tag positioning, factors that should be optimised during the hardware's installation phase. Overall, the system showed potential for stable and dependable performance in real-world scenarios.

6.2 Future Work

The development of the development system opens up opportunities for several future works that can increase its robustness, efficiency, and applicability in different industrial scenarios.

It is necessary to create a record of the inventory of tags belonging to the company in a database and the middleware's program must be adapted to access this database. In this way, it will be possible to more consistently automate the recording of the passage of vehicles that belong to the company and those that do not.

The implementation of an algorithm to calculate the speed of container passage would provide an additional operational metric regarding the movement of industrial containers. This implementation uses the time difference between consecutive antenna readings (tag event

timestamps) and the known distance between them on site.

Another aspect to be further explored is the system's Link Budget. A more detailed analysis of transmitted power, path losses, and reader sensitivity would allow optimisation of the effective range of RFID communication and reduce the likelihood of reading failures. This work could also guide decisions on antenna positioning, adapting the solution to different gate configurations.

With respect to infrastructure, the solution of using only two antennas could be explored, especially in scenarios with narrow gates. This study aims to validate whether reducing the number of antennas, when correctly positioned, ensures acceptable detection levels while reducing implementation and maintenance costs.

System interoperability with existing infrastructure is also relevant. A functionality could be developed for the automatic opening and closing of the barrier upon RFID validation, representing a natural step towards gate automation and enhanced security.

From a software perspective, one challenge to address will be the implementation of a synchronisation mechanism for reading and writing threads in the hash maps used to store passage records. This improvement will ensure greater consistency and reliability of data in high-concurrency scenarios.

In parallel, it is important to research and test other models of passive tags, including those that allow memory writing. The ability to update information directly on the tag could make passages more informative, adding value to the container traceability process.

Finally, reinforcement of the system with ANPR (Automatic Number Plate Recognition) technology is recommended as a redundancy mechanism in the event of RFID reading failure. This additional layer of security and reliability ensures that the system continues to operate even when tags are damaged.

Altogether, these future developments could transform the current prototype into a mature industrial solution, scalable and integrated with the logistical and operational ecosystem of companies.

References

[1] B. Leander, “Access control models to secure industry 4.0 industrial automation and control systems,” 2020.

[2] S. S. G. de Surveillance SA, “Tap into tapa to prevent theft, transportation crime and loss of goods in your supply chain — sgs portugal,” 7 2022.

[3] T. EMEA, “341 new cargo thefts and losses 6 mio across 30 countries in may – tapa emea,” 7 2025.

[4] L. LTD, “Unpacking the biggest cargo crime trends in the eu — loadsure,” 10 2024.

[5] T. Silva, A. Serrador, and P. Sandu, “Controlling industrial waste containers using rfid tags,” *Inforum*, 2024.

[6] J. M. dos Santos Pinheiro, “Identificação por radiofrequência: Aplicações e vulnerabilidades da tecnologia rfid,” *Cadernos UniFOA*, vol. 1, pp. 18–32, 3 2006.

[7] B. Penguin, “Rfid: Radio-frequency identification — applications pros,” 5 2025.

[8] X. Chen, M. A. Eder, A. S. Shihavuddin, and D. Zheng, “A human-cyber-physical system toward intelligent wind turbine operation and maintenance,” *Sustainability (Switzerland)*, vol. 13, pp. 1–10, 1 2021.

[9] J. M. dos Santos Pinheiro, “Identificação por radiofrequência: Aplicações e vulnerabilidades da tecnologia rfid,” *Cadernos UniFOA*, vol. 1, pp. 18–32, 3 2006.

[10] J. Tang, L. Wan, J. Schooling, P. Zhao, J. Chen, and S. Wei, “Automatic number plate recognition (anpr) in smart cities: A systematic review on technological advancements and application cases,” *Cities*, vol. 129, p. 103833, 10 2022.

[11] Z. Zhang, Y. Ding, R. Li, and K. Chen, “Enhancing ocr with line segmentation mask for container text recognition in container terminal,” *Engineering Applications of Artificial Intelligence*, vol. 133, p. 108667, 7 2024.

[12] K. E. Jeon, J. She, P. Soonsawad, and P. C. Ng, “Ble beacons for internet of things applications: Survey, challenges, and opportunities,” *IEEE Internet of Things Journal*, vol. 5, pp. 811–828, 4 2018.

[13] J. Peltokorpi, L. Isojärvi, K. Häkkinen, and E. Niemi, “Qr code-based material flow monitoring in a subcontractor manufacturer network,” *Procedia Manufacturing*, vol. 55, pp. 110–115, 1 2021.

[14] F. Reclus and K. Drouard, “Geofencing for fleet freight management,” *2009 9th International Conference on Intelligent Transport Systems Telecommunications, ITST 2009*, pp. 353–356, 2009.

[15] S. ALAmri, F. ALAbri, and T. Sharma, “Artificial intelligence deployment to secure iot in industrial environment,” *Quality Control - An Anthology of Cases*, 1 2023.

[16] ETSI, “Radio frequency identification (rfid); coordinated eso response to phase 1 of eu mandate m436,” 2011.

[17] W. Xunxun, “Master thesis design of passive uhf rfid tag antennas and industry application,” Master’s thesis, University of Gävle, 2010.

[18] D. d. S. Costa, “Rfid tag aided navigation system for lawnmowers,” Master’s thesis, Universidade de Aveiro, 2022.

[19] S. Hofmayr, “Diplomarbeit title: Analysis and comparison of the potential of rfid-technology in european and u.s. retail supply chains,” Master’s thesis, Vienna University of Economics and Business Administration, 2005.

[20] J. M. Sardroud, “Influence of rfid technology on automated management of construction materials and components,” *Scientia Iranica*, vol. 19, pp. 381–392, 6 2012.

[21] H. I. Inc., “Honeywell ih45 rfid handheld reader.”

[22] Z. Technologies, “Leitor de rfid fixo fx7500 — zebra.”

[23] Laird, “Laird lhcp 5x5 rugged ip67 rfid antenna s9025pxrtn.”

[24] H. G. C. G. Corporation, “Hid® exo pro tag™ rfid tags — hid global,” 2025.

[25] SRK, “Rfid active tags, size: Small at 633.00/piece in nagpur — id: 22989078591.”

[26] Z. Technologies, “Rfid labels and tags — zebra — zebra.”

[27] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Pearson Education India, 2 ed., 2010.

[28] H. Yoon and B.-J. Jang, “Link budget calculation for uhf rfid systems — microwave journal,” 12 2008.

[29] T. K. Adenekan, “(pdf) the evolution of rfid: Trends shaping the industry and challenges ahead,” 6 2022.

[30] D. Kim and J. Yeo, “A passive rfid tag antenna installed in a recessed cavity in a metallic platform,” *IEEE Transactions on Antennas and Propagation*, vol. 58, pp. 3814–3820, 12 2010.

[31] T. Björninen, K. E. Delzo, L. Ukkonen, A. Z. Elsherbeni, and L. Sydänheimo, “Long range metal mountable tag antenna for passive uhf rfid systems,” *2011 IEEE International Conference on RFID-Technologies and Applications, RFID-TA 2011*, pp. 202–206, 2011.

[32] Evizal, T. A. Rahman, and S. K. A. Rahim, “Rfid vehicle plate number (e-plate) for tracking and management system,” *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, pp. 611–616, 2013.

[33] W. Zhao, G. Wang, and X. Lai, “Active e-plate with slot antenna,” *2008 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2008*, 2008.

[34] A. Shukla and E. P. Limited, “10 global brands that use rfid technology,” 1 2025.

[35] H. G. Corporation, “Rfid for oil equipment and yard management,” 2025.

[36] H. G. Corporation, “Case study: Optimizing waste container logistics with rfid,” 2025.

[37] H. G. Corporation, “Transforming waste management with rfid,” 2025.

[38] J. M. dos Santos Pinheiro, “Identificação por radiofrequência: Aplicações e vulnerabilidades da tecnologia rfid,” *Cadernos UniFOA*, vol. 1, pp. 18–32, 3 2006.

[39] Nabto, “A comparison of iot protocols for developers [2023],” 2023.

[40] R. Doshi, S. Inamdar, T. Karmarkar, and M. Wakode, “Distributed mqtt broker: A load-balanced redis-based architecture,” *2024 International Conference on Emerging Smart Computing and Informatics, ESCI 2024*, 2024.

[41] ETSI, “En 302 208 - v3.4.1,” tech. rep., 12 2023.

[42] S. T. S. C. Co., “Rfid tag price - best deals & bulk discounts,” 2025.

[43] R. Tesoriero, J. A. Gallud, M. Lozano, and V. M. Penichet, “Using active and passive rfid technology to support indoor location-aware systems,” *IEEE Transactions on Consumer Electronics*, vol. 54, pp. 578–583, 5 2008.

[44] bcc Research, “The top 5 companies in radio-frequency identification industry,” 8 2023.

[45] R. Card, “The leading rfid solution providers of 2025,” 2025.

[46] Markets and M. Inc., “Rfid companies - top companies list of rfid industry,” 2025.

[47] Metoree, “28 rfid manufacturers in 2025 — metoree,” 8 2025.

[48] R. Jornal, “What are the leading rfid companies? - rfid journal,” 2025.

[49] R. Store, “Zebra fx9600 rfid reader - 4 ports - rfid4ustore,” 2025.

[50] LOGISCENTER, “Comprar zebra fx9600, leitor pelo melhor preço — logiscenter,” 2025.

[51] atlasRFIDstore, “Zebra fx9600 reader — zebra fx9600 rfid reader — 4-port — atlasrfid-store.”

[52] EnCstore, “Zebra fx9600 vs zebra fx7500 rfid reader: Key considerations,” 2025.

[53] A. Teknoloji, “Zebra fx9600 rfid reader 4 ports — altis teknoloji,” 2025.

[54] E. Electronics, “Zebra fx9600 rfid scanner review - energy electronics llc,” 2025.

[55] Z. Technologies, “Leitor de rfid uhf fixo fx9600,” tech. rep., Zebra Technologies, 2025.

[56] Z. Technologies, “Zebra uhf rfid antennas brochure a4,” *Zebra Technologies*, 2 2025.

[57] C. A. Balanis, *Antenna Theory: Analysis and Design*. John Wiley Sons Inc., 4th ed., 2016.

[58] M. Inc., “Rfid polarization explained - metalcraft, inc.,” 7 2022.

[59] C. Mendes, “Parâmetros fundamentais de antenas,” 3 2025.

[60] C. Swedberg, “Hid global takes wide view for rfid growth - rfid journal,” 5 2024.

[61] H. G. Corporation, “Hid® exo keg tag™ rfid tags — hid global,” 2025.

[62] T. M. Systems, “Lmr240 coax cable datasheet,” tech. rep., Times Microwave Systems, 2015.

[63] S. Telecom, “2025 ultimate guide to the coaxial cable assembly - sanny telecom,” 6 2025.

[64] atlasRFIDstore, “A guide to cables, connectors, and adapters,” 2025.

[65] I. Poland, “Additional elements of rfid system - rfid,” 2025.

[66] R. Card, “In-depth understanding of rfid cable connector - rfid card,” 2025.

[67] Wiringo, “Coaxial cable types: How to pick the right one for your application - wiringo,” 5 2025.

[68]

[69] atlasRFIDstore and S. Smiley, “6 things rfid middleware can do for you - atlasrfidstore,” 2 2016.

[70] XMINNOV, “What is rfid middleware software,” 4 2018.

[71] RFID4U, “Rfid middleware - software for rfid readers and printers,” 2025.

[72] C. University, “Java and the internet of things (iot),” 1 2024.

[73] A. Klimenko, “Java: For iot (internet of things) — by alex klimenko — medium,” 4 2024.

[74] A. Obregon, “Java for iot: A perfect match — medium,” 4 2023.

[75] Maasmind, “Why java is the good choice for iot development? - maasmind,” 3 2024. Why Java 5.

[76] SoftTeco, “Top three programming languages for iot projects,” 1 2024. Why Java 2.

[77] E. Foundation, “Maven repository: org.eclipse.paho ≫ org.eclipse.paho.client.mqttv3,” 2025.

[78] A. S. Foundation, “Maven repository: org.apache.kafka ≫ kafka-clients,” 2025.

[79] QOS.ch and C. Gülcü, “Maven repository: org.slf4j ≫ slf4j-simple,” 2025.

[80] QOS.ch and C. Gülcü, “Maven repository: org.slf4j ≫ slf4j-api,” 2025.

[81] JSON.org and D. Crockford, “Maven repository: org.json ≫ json,” 2025.

[82] E. Foundation, “Eclipse paho — projects.eclipse.org.”

[83] A. S. Foundation, “Apache kafka.”

[84] Q. S. (Switzerland), “Slf4j.”

[85] D. P. Baeldung, “Introduction to json-java — baeldung.”

[86] Baeldung, “Jackson json series — baeldung,” 9 2023.

[87] B. Tripathy, “Json serialization and deserialization in java — by bubu tripathy — medium,” 4 2023.

[88] IBM, “Callbacks and synchronization in mqtt client applications,” 1 2025.

[89] Baeldung, “Callback functions in java — baeldung,” 1 2024.

[90] OpenAI, “Industrial container standards eu,” 2025.

[91] W. Waste, “Skip & container sizes - westminster waste,” 9 2025.

[92] Downwaste, “Skip bins for large-scale waste disposal,” 9 2025.

[93] H. Ltd, “Roll on roll off (roro) skip hire essex - lunnon waste,” 9 2025.

[94] S. Gruppe, “Steil gruppe: Skip container,” 9 2025.

Appendix A: Hardware specifications

Physical Characteristics

Dimensions	10.75 in. L x 7.25 in. W x 2.0 in. D 27.3 cm L x 18.4 cm W x 5.0 cm D
Weight	Approx. 4.4 lbs/2.13 kg
Housing Material	Die-cast aluminum, meets IP53 standards
Visual Status Indicators	Multicolor LEDs: Power, Activity, Status and Applications

Figure 6: Zebra FX9600 physical characteristics (extracted from [55])

RFID Characteristics

Max Receive Sensitivity	-86 dBm monostatic
Air Protocols	ISO 18000-63 (EPC Class 1 Gen 2 V2)
Frequency (UHF Band)	Global Reader: 902 MHz - 928 MHz (Also supports countries that use a part of this band), 865 MHZ - 868 MHz US (only) Reader: 902 - 928 MHz
Transmit Power Output	0dBm to +33.0dBm: PoE+, 24V External DC, Universal 24 VDC Power Supply; 0dBm to +31.5dBm: PoE, 12V External DC (4-port-models only), 24V External DC, Universal 24 VDC Power Supply

Figure 7: Zebra FX9600 RFID characteristics (extracted from [55])

Connectivity

Communications	10/100 BaseT Ethernet (RJ45); USB Host and Client (Type A and B)*; Serial (DB9)
General Purpose I/O	4 inputs, 4 outputs, optically isolated (Terminal Block)
Power Supply	POE (802.3af) POE+ (802.3at) +24V DC (UL Approved)
Antenna Ports	FX9600-4: 4 monostatic ports; (Reverse Polarity TNC) FX9600-8: 8 monostatic ports; (Reverse Polarity TNC)

Figure 8: Zebra FX9600 connectivity (extracted from [55])

Environmental

Operating Temp.	-4° to +131° F/-20° to +55° C
Storage Temp.	-40° to +158° F/-40° to +70° C
Humidity	5-95% non-condensing
Sealing	IP53

Figure 9: Zebra FX9600 environmental (extracted from [55])

Hardware, OS and Firmware Management

Processor	Texas Instruments AM3505 (600 MHz)
Memory	Flash 512 MB; DRAM 256 MB
Operating System	Linux
Firmware Upgrade	Web-based and remote firmware upgrade capabilities
Management Protocols	RM 1.0.1 (with XML over HTTP/HTTPS and SNMP binding); RDMP
Network Services	DHCP, HTTPS, FTPS, SFPT, SSH, HTTP, FTP, SNMP and NTP
Network Stack	IPv4 and IPv6
Security	Transport Layer Security Ver 1.2, FIPS-140
API Support	Host Applications — .NET, C and Java EMDK Embedded Applications — C and Java SDK

Figure 10: Zebra FX9600 hardware, OS and firmware management (extracted from [55])

Regulatory Compliance

Safety	UL 60950-01, UL 2043, IEC 60950-1, EN 60950-1
RF/EMI/EMC	FCC Part 15, RSS 210, EN 302 208, ICES-003 Class B, EN 301 489-1/3 For Malaysia: 919-923 MHz
SAR/MPE	FCC 47CFR2:OET Bulletin 65; EN 50364
Other	ROHS, WEEE

Figure 11: Zebra FX9600 regulatory compliance (extracted from [55])

Environmental Compliance

Environment

- RoHS Directive 2011/65/EU; Amendment 2015/863
- REACH SVHC 1907/2006

For a complete list of product and materials compliance, please visit www.zebra.com/environment

Figure 12: Zebra FX9600 environmental compliance (extracted from [55])

AN480 Specifications

PHYSICAL CHARACTERISTICS	
Polarization	Left-hand circular or right-hand circular
Dimensions	259.1 mm x 259.1 mm x 33.5 mm/ 10.2 in. x 10.2 in. x 1.32 in.
Connector	N-Type Female
Connector Location	Rear
Mounting Options	Mounting studs provided
Weight	1.13 kg/2.5 lbs
Casing/Materials	Aluminum with white plastic cover
Frequency Ranges	865–956 MHz
VSWR (Return Loss)	1.3:1

Gain	6.0 dBiL
Front to Back Ratio	18 dB
3 dB Beam Width	65° in both planes
Maximum Power	2 Watts
Axial Ratio	1.5 dB typical
Operating Temperature	-25° to +70°C/-13° to +158°F
Storage Temperature	-40° to +70°C/-40° to +158°F
IP Sealing	IP54
Vibration	IEC-68 series
Humidity	IEC-68-2-30

Vertical Markets
- Retail
- Enterprise/Office
- Hospitality
- Healthcare

Applications
- Point of sale
- Control points
- Hallways

Figure 13: Zebra AN480 specifications (extracted from [56])

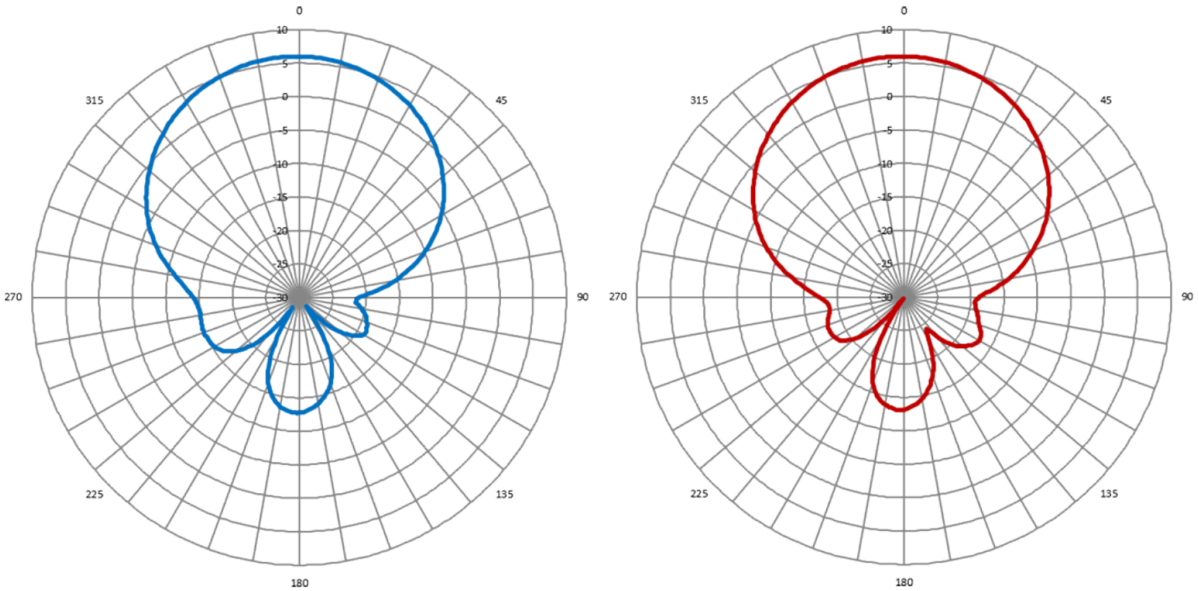


Figure 14: Zebra AN480 radiation diagram (FCC) (extracted from [56])

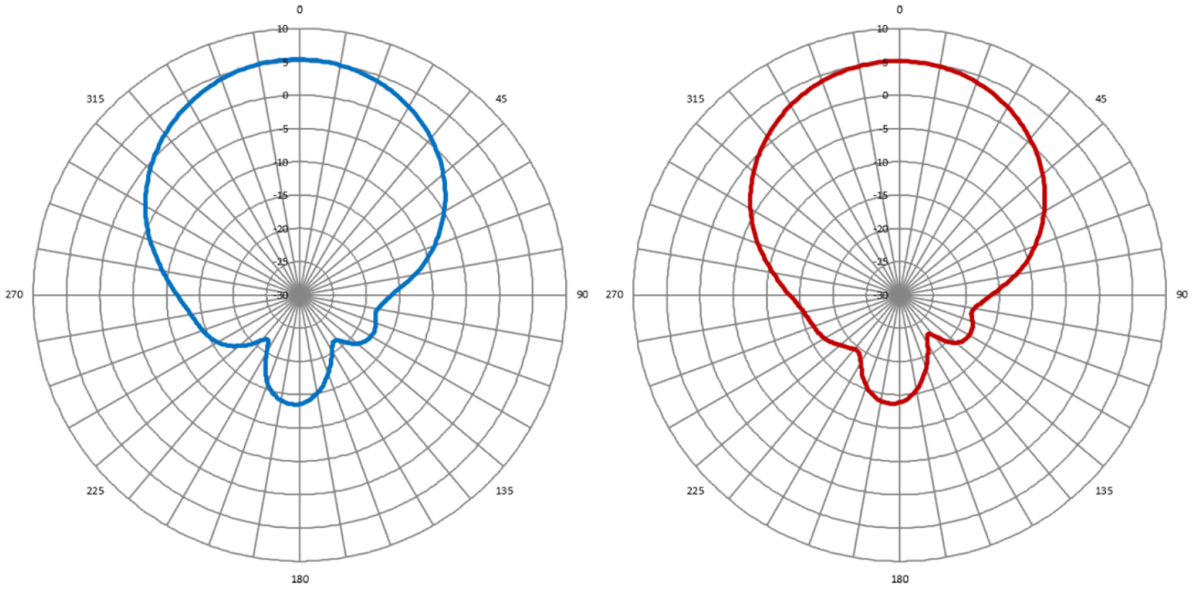


Figure 15: Zebra AN480 radiation diagram (ETSI) (extracted from [56])

	EXO Pro						
	400 HT	Midrange	InLine	600	750	800	InLine Combo
							
Base Model Number	CP16451 (EU) CP16453 (US)	AST1-174-3310 (EU) AST1-174-3300 (US)	6M6980-402 6M6981-402 (pro weld)	CP08785 CP16007 (M730)	CP08726 CP16100 (M730)	CP08725 CP16130 (M730)	6PC980-502
	ELECTRONIC						
Operating Frequency	(EU) - 865-868 MHz (ETSI) (US) - 902-928 MHz (FCC)		865-928 MHz (Global)				865-928 MHz (Global) / NFC
Chip Type	Monza R6-P	M750	M730	Monza 4QT M730			M730 + ICODE SLIX2
Memory	128/96 bit EPC 32/64 bit UM	96 bit EPC 32 bits UM	128 bit EPC	128 bit EPC + 96 bit TID + 512 bit user memory (M730 : 128 bit EPC)			128 bit EPC | 48 bit TID + 2560 bit ICODE SLIX2
Anti-Collision	Yes						
Reading Distance (2W reader ERP, free space)	Up to 13.1 ft (4 m)	Up to 32.8 ft (10 m)		Up to 42.65 ft (13 m)	Up to 47.24 ft (14.4 m)	Up to 49.21 ft (15 m)	Up to 32.8 ft (10 m)

Figure 16: HID Exo Pro InLine electronic characteristics (extracted from [24])

	PHYSICAL						
Dimensions	1.45 × 1.6 × 0.3 in (37.0 × 14.0 × 7.5 mm)	2.5 × 0.69 × 0.25 in (63.5 × 17.5 × 6.4 mm)	3.8 × 1.1 × 0.6 in (97 × 27 × 15 mm); Weld : 4.1 × 1.4 × 0.6 in (105 × 35 × 15 mm)	3.15 x 0.59 x 0.48 in (80 x 15 x 12.5 mm)	2.01 x 1.9 x 0.50 in (51 x 48 x 12.6 mm)	4.33 x 0.98 x 0.51 in (110 x 25 x 12.85 mm)	3.8 × 1.1 × 0.6 in (97 × 27 × 15 mm)
Mounting Method	Screw, weld (special models to glue on metal available on request)						
Screw Mounting Hole	Ø 0.12 in (3 mm)	Ø 0.075 in (2 mm)	Ø 0.2 in (5.2 mm)	Ø 0.2 in (4.9 mm)	Ø 0.2 in (5.5 mm)	Ø 0.2 in (4.9 mm)	Ø 0.2 in (5.2 mm)
Affixes To	All surfaces, including metal, plastic, wood						
Housing Material	Thermoplastic	Ryton PPS	High-impact plastic, Weld : stainless steel ring	ABS Rigid Plastic			High-impact plastic
Color	Black		Gray				
Weight	0.2 oz (5.7 g)	0.35 oz (10 g)	0.8 oz (23 g) Weld : 0.9 oz (26 g)	0.4 oz (12.5 g)	0.9 oz (25.6 g)	0.9 oz (26 g)	0.8 oz (23 g)

Figure 17: HID Exo Pro InLine physical characteristics (extracted from [24])

	CHEMICAL AND MECHANICAL						
Water	IP68, 68° F (20° C), 1 m × 24 h	IP69K (100 bar at 80°C, 30 sek., 16 l/min)	IP68, 68° F (20° C), 1 m × 24 h				
Withstands Exposure To	5% caustic soda, 10% salt water, vegetable oil, Motor oil, 68° F (20° C), 168hr	Dilute mineral acids, dilute alkali solutions (<20%), alcohols, petroleum, salt mist, vegetable oil, hydraulic fluid and most industrial cleaning agents	Mineral oil, petroleum, salt mist, vegetable oil; up to 80% humidity at 158° F (70° C); Caustic Soda (5%)	5% caustic soda, 10% salt water, vegetable oil, Motor oil, 68° F (20° C), 168hr			Mineral oil, petroleum, salt mist, vegetable oil; up to 80% humidity at 158° F (70° C); Caustic Soda (5%)
Vibration & Shock	MIL STD 810-G	IEC 68.2.6 / IEC 60068-2-27:2008		MIL STD 810-G			IEC 68.2.6 / IEC 60068-2-27:2008
Impact	2kg Steel, 1m	1.75kg Steel, 0.76m	IEC 62262-IK08	10kg steel, 1m	4Kg steel, 1m	10kg steel, 1m	IEC 62262-IK08
Axial/Radial Force			1000 N, 10 sec				

Figure 18: HID Exo Pro InLine chemical and mechanical characteristics (extracted from [24])

	THERMAL THERMAL						
Storage	-40° to +185° F (-40° to +85° C), 1x1000 h-40° to +185° F (-40° to +85° C), 1x1000 h						
Operating Temperature	-40° to +185° F (-40° to +85° C)						
Peak Temperature	437° F (225° C), 100 h	392° F (200° C), 100 h					
Shock/Fatigue	-40° to +185° F (-40° to +85° C), 100 x 5 min with 20 sec transition						
	OTHER						
Standards	UHF EPC Class 1 Gen 2, ISO 18000-6C, ISO 17364, DIN 40050-9						+NFC Tag Type 5
Options	Custom label or embossed logo, no logo or custom tag color. Laser engraving of custom logo, barcode or text on gray tag versions. By default, grey tags are supplied without logo or laser engraving. ATEX/IECEx, C1D1						
Box Size	450 pcs.	150 pcs.	240 pcs.	720 pcs.	450 pcs.	432 pcs.	240 pcs.
Warranty	2 Years						

Figure 19: HID Exo Pro InLine thermal characteristics and other information (extracted from [24])

	EXO Keg (UHF)		EXO Keg Inline Combo (UHF + HF)
			
Base Model Number	6M6982-102	6F1988-102	6PC982-102
	ELECTRONIC		
Operating Frequency	865-928 MHz		13.56 MHz + 865-928 MHz (Global)
Chip Type	M730	Monza R6	M730 + ICODE SLIX2
Memory	128 bit EPC + 96 bit TID	96 bit EPC + 96 bit TID	128 bit EPC + 96 bit TID (UHF) + 2560 bits user memory (HF)
Anti-Collision	Yes		
UHF Reading Distance (2 W reader ERP, free space)	Up to 32.8 ft (10 m)		

Figure 20: HID EXO Keg electronic characteristics (extracted from [61])

	PHYSICAL		
Dimensions	3.5 x 1.4 x 0.6 in (88 x 37 x 15 mm)	2.04 x 1.02 x 0.83 in (52 x 26.5 x 21.4 mm)	3.5 x 1.4 x 0.6 in (88 x 37 x 15 mm)
Curve Radius	450 mm (larger kegs)	126 / 163 mm (smaller kegs)	450 mm (larger kegs)
Mounting Method	Weld		
Affixes To	Steel Kegs		
Housing Material	PA (Polyamide)		
Weight	0.70 oz (20 g)		
Color	Gray		Warm Gray or Blue
	CHEMICAL AND MECHANICAL RESISTANCE		
Water	IP68, 6.6 ft (2 m) x 24 h		
Withstands Exposure To	Mineral oil, petroleum, salt mist, vegetable oil, caustic soda 5%; up to 80% humidity at 158° F (70° C)		
Environmental Test Conditions	68° F (20° C), 100 h		
Vibration	IEC 68.2.6 [10 g, 10 to 2000 Hz, 3 axis, 2.5 h]		
Shock	IEC 60068-2-27:2008 [40 g, 18 ms, 6 axis, 2000 times]		
Impact	IEC 62262-IK08	IEC 62262-IK07	IEC 62262-IK08
Axial/Radial Force	1000 N, 10 sec		

Figure 21: HID EXO Keg physical, chemical and mechanical characteristics (extracted from [61])

	THERMAL		
Storage	-40° to +185° F (-40° to +85° C)		-40° to +176° F (- 40 ° to + 80 °C)
Operating Temperature	-40° to +185° F (-40° to +85° C)		-40° to +176° F (- 40 ° to + 80 °C)
Shock/Fatigue	-40° to +185° F (-40° to +85° C), 100 x 5 min with 30 sec transition		
	OTHER		
Standards	UHF EPC Class 1 Gen 2		
Options	Laser engraving		
Box Size	240 pcs.	400 pcs.	240 pcs.
Warranty	2 Years		

Figure 22: HID EXO Keg thermal characteristics and other information (extracted from [61])

Part Description

Part Number	Application	Jacket	Color	Stock Code
LMR-240	Outdoor	PE	Black	54021
LMR-240-DB	Outdoor/Watertight	PE	Black	54090
LMR-240-FR	Indoor/Outdoor Riser CMR FRPE		Black	54029
LMR-240-FR-PVC	Indoor/Outdoor Riser CMR FRPVC		Black	54214
LMR-240-PVC	General Purpose	PVC	Black	54140
LMR-240-PVC-W	General Purpose	PVC	White	54202
LMR-240-MA	Indoor & Mobile Antenna	PVC	Black	54046

Environmental Specifications

Performance Property	°F	°C
Installation Temperature Range	-40/+185	-40/+85
Storage Temperature Range	-94/+185	-70/+85
Operating Temperature Range	-40/+185	-40/+85

Mechanical Specifications

Performance Property	Units	US	(metric)
Bend Radius: installation	in. (mm)	0.75	(19.1)
Bend Radius: repeated	in. (mm)	2.5	(63.5)
Bending Moment	ft-lb (N-m)	0.25	(0.34)
Weight	lb/ft (kg/m)	0.034	(0.05)
Tensile Strength	lb (kg)	80	(36.3)
Flat Plate Crush	lb/in. (kg/mm)	20	(0.36)

Construction Specifications

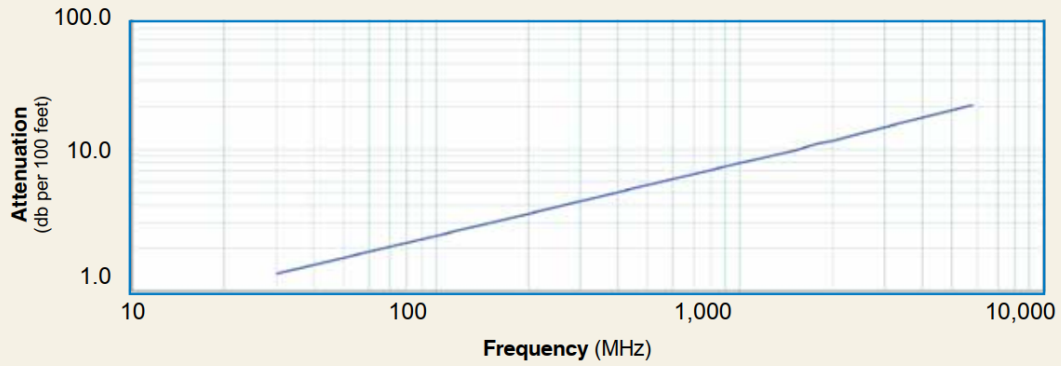
Description	Material	In.	(mm)
Inner Conductor	Solid BC	0.056	(1.42)
Dielectric	Foam PE	0.150	(3.81)
Outer Conductor	Aluminum Tape	0.155	(3.94)
Overall Braid	Tinned Copper	0.178	(4.52)
Jacket	(see table)	0.240	(6.10)

Electrical Specifications

Performance Property	Units	US	(metric)
Velocity of Propagation	%	83	
Dielectric Constant	NA	1.42	
Time Delay	nS/ft (nS/m)	1.21	(3.97)
Impedance	ohms	50	
Capacitance	pF/ft (pF/m)	24.2	(79.4)
Inductance	uH/ft (uH/m)	0.060	(0.20)
Shielding Effectiveness	dB	>90	
DC Resistance			
Inner Conductor	ohms/1000ft (/km)	3.2	(10.5)
Outer Conductor	ohms/1000ft (/km)	3.89	(12.8)
Voltage Withstand	Volts DC	1500	
Jacket Spark	Volts RMS	5000	
Peak Power	kW	5.6	

Figure 23: LMR240 coaxial cable specifications (extracted from [62])

Attenuation vs. Frequency (typical)



Frequency (MHz)	30	50	150	220	450	900	1500	1800	2000	2500	5800	8000
Attenuation dB/100 ft	1.3	1.7	3.0	3.7	5.3	7.6	9.9	10.9	11.5	12.9	20.4	24.3
Attenuation dB/100 m	4.4	5.7	9.9	12.0	17.3	24.8	32.4	35.6	37.7	42.4	66.8	79.7
Avg. Power kW	1.49	1.15	0.66	0.54	0.38	0.26	0.20	0.18	0.17	0.15	0.10	0.08

Figure 24: LMR240 coaxial cable attenuation (extracted from [62])

Connectors

Interface	Description	Part Number	Stock Code	VSWR** Freq.	(GHz)	Coupling Nut	Inner Contact Attach	Outer Contact Attach	Finish* Body /Pin	Length in	(mm)	Width in	(mm)	Weight lb	(g)
1. F Male	Straight Plug	TC-240-FM-X	3190-2891	<1.25:1	(2.5)	Knurl	Solder	Crimp	N/G	1.1	(28)	0.45	(11.4)	0.014	(6.4)
2. N Male	Straight Plug	EZ-240-NMH-X	3190-2893	<1.25:1	(2.5)	Hex/Knurl	Spring Finger	Crimp	A/G	1.5	(38.1)	0.78	(19.8)	0.086	(39.0)
3. N Male	Right Angle	EZ-240-NMH-RA-X	3190-6143	<1.35:1	(6)	Hex	Spring Finger	Crimp	A/G	1	(25.1)	1.04	(26.4)	0.115	(52.0)

Figure 25: LMR240 connectors (1/2) (extracted from [62])

Connectors

Interface	Description	Part Number	Stock Code	VSWR** Freq.	(GHz)	Coupling Nut	Inner Contact Attach	Outer Contact Attach	Finish* Body /Pin	Length in	(mm)	Width in	(mm)	Weight lb	(g)
4. N Male	Right Angle	TC-240-NMH-RA-D	3190-2426	<1.35:1	(6)	Hex/Knurl	Solder	Crimp	A/G	1.2	(32.4)	1.22	(31.0)	0.091	(41.7)
5. N Male	Straight Plug	TC-240-NMH-X	3190-2887*	<1.25:1	(2.5)	Hex/Knurl	Solder	Crimp	N/S	1.5	(38)	0.75	(19.1)	0.086	(39.0)
6. N Male	Straight Plug	TC-240-NMC	3190-244	<1.25:1	(2.5)	Knurl	Solder	Clamp	S/G	1.5	(38)	0.75	(19.1)	0.082	(37.2)
7. 1.0/2.3 DIN	Straight Plug	EZ-240-1023M	3190-6283	<1.35:1	(2.5)	knurl	Spring Finger	Crimp	N/G	1.1	(228.5)	0.33	(8.5)	0.014	(6.63)
8. N Female	Bulkhead Jack	TC-240-NF-BH-X	3190-2888	<1.25:1	(2.5)	NA	Solder	Crimp	A/G	1.7	(44)	0.88	(22.2)	0.115	(52.2)
9. N Female	Panel Mount	TC-240-NF-PM-X	3190-2889*	<1.25:1	(6)	NA	Solder	Crimp	A/G	1.7	(44)	0.88	(22.2)	0.115	(52.2)
10. N Female	Straight Jack	EZ-240-NF-X	3190-2795	<1.25:1	(6)	NA	Spring Finger	Crimp	A/G	1.4	(35.4)	0.62	(15.8)	0.040	(18.0)
11. BNC Male	Straight Plug	TC-240-BMC	3190-242	<1.25:1	(2.5)	Knurl	Solder	Clamp	S/G	1.7	(43)	0.56	(14.2)	0.040	(18.1)
12. BNC Male	Straight Plug	EZ-240-BM-X	3190-6120	<1.25:1	2.5	Knurl	Spring Finger	Crimp	A/G	1.3	(34)	0.58	(14.7)	0.043	(19.5)
13. BNC Male	Straight Plug	TC-240-BM-X	3190-2890	<1.25:1	(2.5)	Knurl	Solder	Crimp	A/G	1.3	(34)	0.58	(14.7)	0.043	(19.5)
14. BNC Male	Right Angle	TC-240-BM-RA-D	3190-2869	<1.25:1	(2)	Knurl	Solder	Crimp	A/G	1.0	(25.1)	0.57	(14.5)	0.115	(52.0)
15. BNC Male	Right Angle	EZ-240-BM-RA-X	3190-2868	<1.30:1	(4)	KNURL	Spring Finger	Crimp	A/G	1.3	(33.6)	1.19	(30.1)	0.091	(41.7)
16. TNC Male	Straight Plug	EZ-240-TM-X	3190-2725	<1.25:1	(2.5)	Knurl	Spring Finger	Crimp	N/G	1.4	(34.3)	0.59	(15.0)	0.043	(19.5)
17. TNC Male	Straight Plug	TC-240-TM-X	3190-2797	<1.25:1	(2.5)	Knurl	Solder	Crimp	N/G	1.7	(43)	0.59	(15.0)	0.043	(19.5)
18. TNC Male	Reverse Polarity	EZ-240-TM-RP-X	3190-2892	<1.25:1	(6)	Knurl	Spring Finger	Crimp	A/G	1.4	(36)	0.59	(15.0)	0.043	(19.5)
19. TNC Male	Right Angle	TC-240-TM-RA-D	3190-2798	<1.25:1	(6)	Hex	Solder	Crimp	A/G	1.0	(25.1)	0.62	(15.7)	0.115	(52.0)
20. TNC Female	Straight Jack	EZ-240-TF-X	3190-6204	<1.25:1	(6)	NA	Spring Finger	Crimp	A/G	1.1	(27.2)	0.87	(22.0)	0.033	(15.0)
21. TNC Female	Reverse Polarity	EZ-240-TF-RP-X	3190-6167	<1.35:1	(6)	NA	Spring Finger	Crimp	A/G	1.1	(27.2)	0.87	(22.0)	0.033	(15.0)
22. QMA Male	Straight Plug	EZ-240-QM-X	3190-2894	<1.25:	(6)	Knurl	Spring Finger	Crimp	N/G	1.2	(30.0)	0.41	(10.5)	0.014	(6.35)
23. QMA Male	Right Angle	EZ-240-QM-RA-X	3190-2895	<1.25:	(<6)	Knurl	Spring Finger	Crimp	N/G	0.8	(20.3)	0.65	(16.5)	0.019	(8.62)
24. SMA Male	Straight Plug	EZ-240-SM-X	3190-2897	<1:25:	(6)	Hex	Spring Finger	Crimp	N/G	1.0	(25.4)	0.32	(8.1)	0.016	(7.26)
25. SMA Male	Straight Plug	TC-240-SM-SS-X	3190-2898*	<1.25:1	(10)	Hex	Solder	Crimp	SS/G	1.0	(25)	0.32	(8.1)	0.016	(7.3)
26. SMA Male	Right Angle	TC-240-SM-RA-SS-X	3190-2900*	<1.35:1	(6)	Hex	Solder	Crimp	SS/G	0.8	(20)	0.65	(16.5)	0.019	(8.6)
27. SMA Male	Right Angle	EZ-240-SM-RA-X	3190-2899	<1.25:1	(6)	Hex	Spring Finger	Crimp	A/G	0.9	(22.8)	0.31	(7.9)	0.019	(8.6)
28. SMA Male	Reverse Polarity	TC-240-SM-RP	3190-326	<1.25:1	(2.5)	Hex	Solder	Crimp	SS/G	1.0	(25)	0.32	(8.1)	0.016	(7.3)
29. SMA Female	Bulkhead Jack	TC-240-SF-SS-BH-X	3190-2896*	<1.25:1	(2.5)	NA	Solder	Crimp	SS/G	1.1	(29)	0.31	(7.9)	0.019	(8.6)
30. Mini-UHF	Straight Plug	TC-240-MUHF	3190-445	<1.25:1	(2.5)	Knurl	Solder	Crimp	N/G	1.1	(28)	0.45	(11.4)	0.014	(6.4)
31. 7/16 Din Male	Straight Plug	TC-240-716M	3190-2982	<1.35:1	(3)	Hex	Spring Finger	Crimp	A/S	2.0	(50.5)	1.26	(32.0)	0.186	(84.4)
32. 7/16 Din Male	Right Angle	TC-240-716M-RA-D	3190-2983	<1.35:1	(3)	Hex	Solder	Crimp	A/S	1.4	(34.3)	1.60	(40.6)	0.239	(108.5)

*Finish metals: N=Nickel, S=Silver, G=Gold, SS=Stainless Steel, A=Alballoy **VSWR spec based on 3 foot cable with a connector pair *Available in bulk pack

Figure 26: LMR240 connectors (2/2) (extracted from [62])

Appendix B: Link Budget Matlab Code

```
[ Matlab script used to calculate the link budget ]

clc;
clear all;
close all;

% Gains
Ptx = 29.2; % dBm
Gtx = 6; % dBi
Grx = Gtx; % Monostatic Reader
Gtag = 3; % dBi

% Modulation Index
m = 0.8;
% ASK modulation losses
kASK = -10*log10( (1-m^4) / ((1+m)^2) );
% Reflection power losses (RFID journal article)
T = 10*log10(m^2);


% Total distance of propagation in free space (uplink and downlink)
d = linspace(0, 10, 1000); % 5 m distance between reader and tag


% Free space propagation losses
f = 865*10^6; % Hz
c = 3*10^8; % m/s
lambda = c/f; % m
```

```
D = 259.1*10^-3; % m
df = (2*D^2)/lambda;
% L = 1; % if there are no hardware losses
PLtotal = -10*log( lambda^2 ./ (4*pi*2*d).^2 );

% Losses in coaxial cables
Att_LMR240 = 24.8/100; % dB/100m
length = 15; % m
Att_coax = (Att_LMR240 * length); % dB

% Loss factor due to polarization incompatibility
% Circular polarization in reader antennas
% Linear polarization in tag antennas
% PLF = 0.5 (linear)
PLF = -3; % (logarithmic scale) (dimensionless)

% Total Losses
Ltotal = PLtotal + 2*Att_coax - T - kASK;

% Total Link Budget
Pr = Ptx + Gtx + Grx + 2*Gtag - Ltotal + 2*PLF;

% Psens = -86; % dBm (Zebra FX9600 Datasheet)


% Plot

figure;
subplot(2,1,1);
plot(d, Ltotal, 'r', 'LineWidth', 3);   % Losses uplink/downlink
xlabel('Distance (m)', 'FontSize', 14);
ylabel('Total Loss', 'FontSize', 14);
title('Total Loss (dB)', 'FontSize', 16);
grid on;
grid minor;
xlim([0 10]);

```

```
66 subplot(2,1,2);
67 plot(d, Pr, 'b', 'LineWidth', 3);   % Received power uplink/downlink
68 xlabel('Distance␣(m)', 'FontSize', 14);
69 ylabel('Received␣Power␣(dB)', 'FontSize', 14);
70 title('Received␣Power', 'FontSize', 16);
71 grid on;
72 grid minor;
73 xlim([0 10]);
```