Research Repository UCD

Title	An IEEE 802.11ax based Edge Computing System for Industrial IoT Applications
Authors(s)	Kelly, Mark A.
Publication date	2023
Publication information	Kelly, Mark A. “An IEEE 802.11ax Based Edge Computing System for Industrial IoT Applications.” University College Dublin. School of Computer Science, 2023.
Publisher	University College Dublin. School of Computer Science
Item record/more information	http://hdl.handle.net/10197/30025

Downloaded 2026-05-02 11:03:35

The UCD community has made this article openly available. Please share how this access benefits you. Your story matters! (@ucd_oa)

© Some rights reserved. For more information

An IEEE 802.11ax based edge computing system for Industrial IoT applications

Mark A Kelly

This thesis is submitted to University College Dublin (UCD)

in fulfilment of the requirements for the degree of

Doctor of Philosophy

School of Computer Science

Head of School: Prof. Neil Hurley

Under the supervision of: Prof. Joe Carthy

—

July 2023

Contents

Acknowledgements ix

Dedication x

Statement of Authoriship xi

List of Tables xii

List of Figures xiv

1 An Introduction **2**

1.1 An Overview of the Internet of Things (IoT) 2

1.2 Components of the IoT 3

1.3 IoT Application areas 4

1.3.1 Industry 4.0 5

1.4 Edge computing 10

1.5 Wireless comes of age 12

1.5.1 Wi-Fi and 5G advances 14

1.5.2 The case for Wi-Fi 17

1.6 Research Motivation 18

1.7 Research question 20

1.8 Contributions 21

1.9 Organisation 24

2 Industrial digital transformation 25

2.1 Industry 4.0 26

2.1.1 Characteristics of Industry 4.0 26

2.1.2 Industry 4.0 & IIoT applications 28

2.2 Industrial Automation & Control Systems 30

2.3 Prognostics and Health Management 37

2.3.1 Maintenance types 39

2.3.2 PHM Process 43

2.4 Digital Twins 47

2.4.1 Digital Twin operation 50

2.5 Conclusion 55

3 Wireless Industrial Networks 57

3.1 Wireless Industrial Networks 58

3.2 Performance considerations for industrial wireless networks 61

3.2.1 Harsh RF Environment 63

3.3 Leading industrial wireless technologies 64

3.3.1 IEEE 802.15.X based systems 64

3.3.2 Cellular based systems 75

3.3.3 The emergence of Private 5G networks 79

3.4 IEEE 802.11 & Wi-Fi 80

3.4.1 A chronology of Wi-Fi 84

3.5 802.11ax and Wi-fi 6E 90

3.5.1 OFDMA 93

3.5.2 1024 QAM 98
3.5.3 MU-MIMO 100
3.5.4 Enhanced PPDU formats 102
3.5.5 IoT Device support 107
3.5.6 BSS Colouring 108
3.5.7 Target Wake Up Time 109
3.6 Conclusion 111

4 Radio propagation testing for Industrial Wireless Networks 114
4.1 Introduction 116
4.2 Test site overview 117
4.2.1 Channel sounding testing 120
4.3 Channel sounding system design 124
4.4 Radio propagation testing process 127
4.4.1 Data Collection and Measurement Process 129
4.4.2 Channel Sounding Waveform Selection 130
4.4.3 Calculations 131
4.5 Radio Propagation Test Results 139
4.5.1 Channel impulse response 140
4.5.2 Channel Gain and Path Loss 142
4.5.3 Delay Spread and Power Delay Profile 149
4.5.4 Multipath fading and Rician K factor 155
4.6 Conclusion 160

5 Wi-Fi based industrial wireless network solution design 162
5.1 The evolution of Industrial computing 164

5.2 System Design and Architecture 166
5.2.1 Event driven Architecture technologies: MQTT and Sparkplug 167
5.2.2 Virtualisation Technology: Containers 171
5.2.3 System design details 174
5.2.4 Key system components 180
5.2.5 Key System Components 180
5.3 Edge Device 181
5.3.1 Edge of Network Node 185
5.3.2 Message Broker 186
5.3.3 Primary application -SCADA IIOT Host 187
5.3.4 Management and Applications 188
5.4 Data Historian 189
5.4.1 TimeSeries Databases 189
5.4.2 Database architecture 192
5.4.3 Entity descriptions 194
5.4.4 Data Definition Language 198
5.4.5 Protocol Mapping 200
5.4.6 Messaging structure 202
5.5 Conclusion 204

6 Industrial wireless network: System test and evaluation 207

6.1 Introduction 209
6.2 Test system and test criteria 211
6.2.1 Reliability 213
6.2.2 Latency and Round Trip Time 215

6.2.3 Payload Support 217
6.2.4 Update rate 219
6.2.5 Jitter 220
6.3 Experimental Approach and Configuration 221
6.3.1 Testing Duration 225
6.3.2 Data sampling approach 227
6.3.3 Frequency band selection 228
6.3.4 Timing and synchronisation 229
6.3.5 Network and application testing 230
6.3.6 Summary Statistics 230
6.3.7 5GHz Testing 231
6.4 Class 0 system testing 233
6.4.1 Experimental setup and Configuration 234
6.4.2 Results 237
6.5 Class 2 system testing 250
6.5.1 Experimental setup and configuration 251
6.5.2 Results 253
6.6 Class 4 system testing 266
6.6.1 Expermental setup and Configuration 267
6.6.2 Results 268
6.7 Conclusion 281
6.7.1 Performance Assessment and Network Dynamics 281
6.7.2 Key Observations and Optimisation Strategies 282
6.7.3 Future Optimisation Strategies 282

7 Conclusion **284**

7.1 Concluding thoughts 284

7.2 Contributions 288

7.3 Implications 289

7.4 Limitations 290

7.5 Future Work 291

7.5.1 Strategies to Improve Performance 293

8 Appendix A **294**

8.1 Wi-Fi data formats 294

Abstract

The integration of industrial processes into enterprises, known as Industry 4.0, represents a significant shift in product design and manufacturing. To meet strict performance criteria, wired networks are the norm in industrial settings. However, wireless technologies offer numerous advantages, including lower costs and greater factory flexibility. Thanks to recent advances in 5G technology and IEEE 802.11 standards, industrial wireless networks are becoming increasingly viable.

Our dissertation proposes a design for a Wireless Industrial system that leverages Wi-Fi technology and supports new and emerging industrial applications based on the IEEE 802.11ax standard. We conducted radio propagation testing of the technology at an industrial test bed and developed an open-source-based system that promotes interoperability between legacy industrial protocols and emerging IoT protocols.

To evaluate the system's performance, we established a physical test bed based on international standards and outlined a set of performance criteria. Our test results provide valuable insights into the system's effectiveness.

Acknowledgements

I want to express my deepest gratitude to two individuals who were instrumental in my research journey. Firstly, I am immensely grateful to Professor Joe Carthy for his invaluable guidance. His practical and helpful advice has shaped my research and helped me stop striving for perfection. Secondly, I want to thank Dr. Keith Nolan for his unwavering support. He has been a sounding board and a constant source of assistance. His simple but profound advice to 'just play the note' became a mantra, reminding me to focus, simplify, and submit. I am truly thankful for their wisdom, patience, and inspiration.

Dedication

To Rebecca, Alexia, Isaac and Roman, you are my everything.

To my dad, for your unwavering support

Statement of Authorship

I hereby certify that the submitted work is my own work, was completed while registered as a candidate for the degree stated on the Title Page, and I have not obtained a degree elsewhere on the basis of the research presented in this submitted work.

List of Tables

2.1 Manufacturing process types and examples 32

2.2 ISA-95 Levels description and examples 32

2.3 performance requirements for industrial application 37

2.4 Summary of maintenance types and examples 43

3.1 ISA categories, classes and application types 61

3.2 Cellular base station types 77

3.3 Cellular response time evolution 79

3.4 Comparison of IEEE802.11 standards 91

3.5 802.11ax Comparison to legacy versions 93

3.6 IEEE 802.11ax PPDU Frame structure 104

4.1 Inventory of test equipment used for sounding system 125

4.2 Test parameters, values, and units 140

4.3 Gain Data for a 6 GHz Wireless Industrial Network 143

4.4 Path Loss Data for IMR at 6 GHz 150

4.5 Measurement data for various distances 151

4.6 Summary Statistics for K-Factor results 156

5.1 Basic TEDS format 195
5.2 ISA-95 to IMR mapping 202

6.1 Reliability requirements for various industrial applications 213
6.2 Latency numbers for various industrial applications 216
6.3 Payload sizes for application class in Bytes 218
6.4 Jitter specifications for various industrial applications (illustrative) 221
6.5 Summary of performance requirements for Wireless Industrial Network 223
6.6 Test runs for industrial application classes 226
6.7 Class 0 5GHz Industrial System Test Data 232
6.8 Class 2 5GHz Industrial System Test Data 232
6.9 Class 4 5GHz Industrial System Test Data 233
6.10 Class 0 6GHz Industrial System Test Data 237
6.11 Class 2 6GHz Industrial System Test Data 253
6.12 Class 4 6GHz Industrial System Test Data 270

8.1 802.11 frame structure 294
8.2 802.11 Common information field subfield 295
8.3 802.11 Control frames description 295
8.4 802.11 management Subtypes 297
8.5 802.11 management frame structure 297
8.6 Sparkplug version B message types 298
8.7 Sparkplug version B message types for finishing machine 299

List of Figures

1.1 IoT Themes 3

1.2 Basic IoT Concept 4

1.3 IoT Growth 2015 -2025 5

1.4 A multilayered view of Industrial IoT 9

1.5 Edge computing logical architecture 11

1.6 Industrial Application Performance requirements 14

2.1 Industry 4.0 sits at the intersection of multiple technologies 27

2.2 Example of smart factory 29

2.3 Top 10 Industrial IoT applications 30

2.4 ISA Layered automation pyramid 33

2.5 SCADA system and main components 35

2.6 PhM process overview 44

2.7 Reliability Bath Tube Curve of equipment 46

2.8 Conceptual representation of 3d model beside a physical object, source; Nokia 48

2.9 Digital Twin system overview 51

3.1 802.15.4 network topologies 65
3.2 WirelessHart network topology 67
3.3 Typical ISA10001a network 69
3.4 Typical WIA-PA network 74
3.5 A Private 5G network 81
3.6 Electromagnetic spectrum; source OFCOM 87
3.7 difference between OFDM and OFDMA 94
3.8 802.11ax OFDMA operation 95
3.9 OFDMA subcarriers 97
3.10 OFDMA Resource Units allocation in frequency bands 98
3.11 QAM constellation plots showing the difference between Wi-Fi 5 and Wi-Fi 6[1]. 99
3.12 Multiuser MIMO operation 101
3.13 802.11ax Trigger Frame 104
3.14 802.11ax common information field 106
3.15 802.11ax User information field structure 106
3.16 BSS Frequency reuse, frequency reuse, and BSS Colouring 108
3.17 802.11ax Target Wake up Time 110

4.2 IMR Network test layout 119
4.3 Testing bay and manufacturing cells 121
4.4 Channel sounding operation 122
4.5 RF sounding sequence 123
4.6 High-level RF measurement setup 124
4.7 RF sounding system layout 126

4.8 RF measurement process flow diagram 128
4.9 RF sounding test route and waypoints 130
4.10 Mean Channel impulse response for 1-10m at IMR 141
4.11 Plot of gain versus distance 144
4.12 Path Loss diagram for IMR 149
4.13 Delay measured from the experimental set-up 152
4.14 Delay spread calculations for IMR 153
4.15 K-factor chart for IMR 157

5.1 MQTT operation overview 168
5.2 Container technology architecture 172
5.3 High-level System Architecture 178
5.4 System Architecture with numbered subsystems 179
5.5 Arduino-based sensor module 182
5.6 Zephyr-based Node system 183
5.7 Edge of Network Node Component Architecture 184
5.8 Edge Server Component Architecture 185
5.9 Edge Server Installed system and key components 186
5.10 Data storage in Timescale DB 192
5.11 Information model of system database 197
5.12 ISA-IMRHierarchy Mapping 201
5.13 ISA-95 and Sparkplug mapping 202

6.1 System Test flows 211
6.2 Example payload format including network and SparkPlug data . 219
6.3 Industrial Wireless System test configuration architecture 224

6.4 Test configuration for Class 0 Applications 234
6.5 Basic Alert Message (ISA-5.00.01 Class 0) 236
6.6 Class 0 Reliability time series 238
6.7 Class 0 Reliability Histogram 238
6.8 Class 0 Reliability density diagram 239
6.9 Class 0 Reliability histogram with KDE 239
6.10 Class 0 Violin plot 240
6.11 Class 0 Round Trip Time smoothed over samples collected 241
6.12 Class 0 round trip time histogram 242
6.13 Class 0 round trip time density 242
6.14 Class 0 Throughput 244
6.15 Class 0 Throughput density plot 244
6.16 Class 0 Throughput Violin plot 245
6.17 Class 0 Throughput Historgram with KDE 245
6.18 Class 0 Histogram Histogram 246
6.19 Class 0 Jitter smoothed over samples collected 247
6.20 Class 0 Jitter density 248
6.21 Class 0 Jitter Histogram 248
6.22 Class 0 Jitter Violin plot 249
6.23 Class 0 Hi 249
6.24 Test configuration for Class 2 Applicatons 252
6.25 Class 2 example machine data 253
6.26 Class 2 Reliability time series 254
6.27 Class 2 Reliability Histogram 255
6.28 Class 2 Reliability density diagram 255

6.29 Class 2 Reliability histogram with KDE 256
6.30 Class 2 Violin plot 256
6.31 Class 2 Round Trip Time smoothed over samples collected 258
6.32 Class 2 round trip time histogram 258
6.33 Class 2 round trip time density 259
6.34 Class 2 Throughput 260
6.35 Class 2 Throughput density plot 260
6.36 Class 2 Throughput Violin plot 261
6.37 Class 2 Throughput Historgram with KDE 261
6.38 Class 2 Histogram Histogram 262
6.39 Class 2 Jitter smoothed over samples collected 263
6.40 Class 2 Jitter density 263
6.41 Class 2 Jitter Histogram 264
6.42 Class 2 Jitter Violin plot 264
6.43 Class 2 Histogram with KDE 265
6.44 System Test Configuration for class 4 and 5 applications 267
6.45 Class 4 sample machine data (excerpt) 269
6.46 Class 4 Reliability time series 270
6.47 Class 4 Reliability Histogram 271
6.48 Class 4 Reliability density diagram 271
6.49 Class 4 Reliability histogram with KDE 272
6.50 Class 4 Violin plot 272
6.51 Class 4 Round Trip Time smoothed over samples collected 273
6.52 Class 4 round trip time histogram 274
6.53 Class 4 round trip time density 274

6.54 Class 4 Throughput 275
6.55 Class 4 Throughput density plot 276
6.56 Class 4 Throughput Violin plot 276
6.57 Class 4 Throughput Historgram with KDE 277
6.58 Class 4 Histogram Histogram 277
6.59 Class 4 Jitter smoothed over samples collected 278
6.60 Class 4 Jitter density 279
6.61 Class 4 Jitter Histogram 279
6.62 Class 4 Jitter Violin plot 280
6.63 Class 4 Hist-KDE 280

8.1 Database schema for Edge based Telemetry Database 296

Chapter 1

An Introduction

1.1 An Overview of the Internet of Things (IoT)

The Internet of Things (IoT) signifies the revolutionary expansion of the internet, enabling the interconnection of physical objects through internet technologies, predominantly the Internet Protocol (IP) [1]. It aims to foster seamless interactions among devices and objects over the internet, marking a paradigm shift focused on machine-to-machine interactions, enhancing cyber-physical experiences [2, 3].

The inception of IoT was marked by the International Telecommunication Union (ITU) in 2005, propelling an era where objects ubiquitously connect and communicate over networks [4]. IoT's transformative potential has been immense, with widespread implications across various industries, revolutionizing conventional operational methodologies [5].

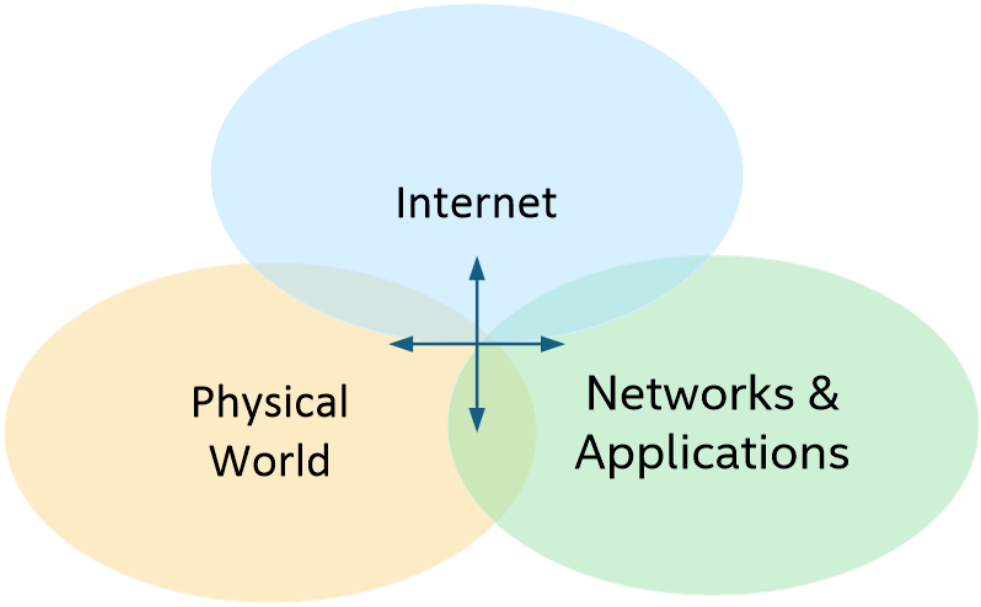


Figure **(1.1)** –IoT Themes

1.2 Components of the IoT

IoT is an amalgamation of numerous technological innovations, encompassing essential components like connectivity, cloud computing, and intelligent objects or "things" [6]. A quintessential IoT system embodies a network of sensors, gateway, and cloud infrastructure, facilitating data collection, processing, and management [7, 8].

The agile development in wireless connectivity has significantly bolstered the IoT framework, fostering the evolution of a plethora of connected devices and wireless networks [9]. IoT platforms play a pivotal role, enabling comprehensive data management, analytics, and remote device control, symbolizing a convergence of diverse technologies aimed at optimizing operational efficiencies [10].

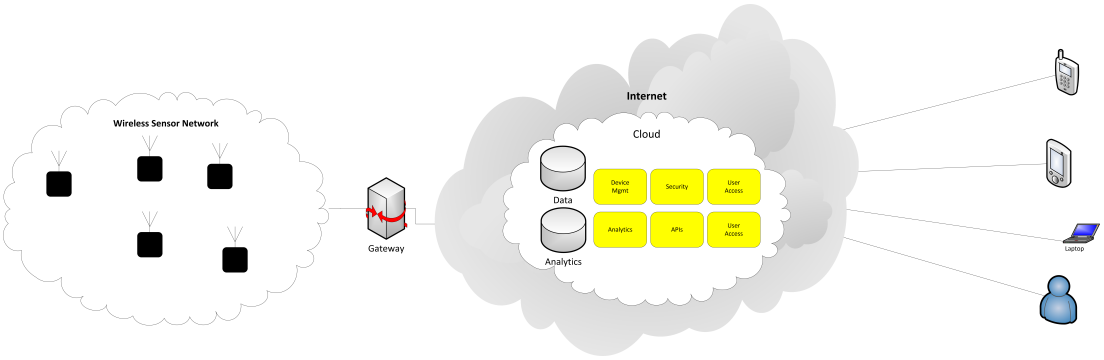


Figure **(1.2)** –Basic IoT Concept

1.3 IoT Application areas

According to a Forbes magazine article from 2018 [11], the growth and impact of IoT are finally living up to its initial hype. The authors highlighted how IoT has explosively evolved across different industries and discussed the top 10 IoT segments. The top three segments, intelligent cities, connected industry, and connected buildings, make up 52% of the total share of IoT projects. Other notable segments include energy, health, and agriculture. A recent report from Meticulous Research predicted that the smart agriculture market would be worth over $35 billion by 2027 [12]. Over the last decade, IoT has grown from approximately 15 billion devices in 2015 to a projected greater than $75 billion in 2025, as shown in Figure 1.3.

In this thesis, we will briefly examine the role of IoT in smart cities, agriculture, and Industry 4.0 to illustrate three areas where the application and use of IoT have a very significant impact.

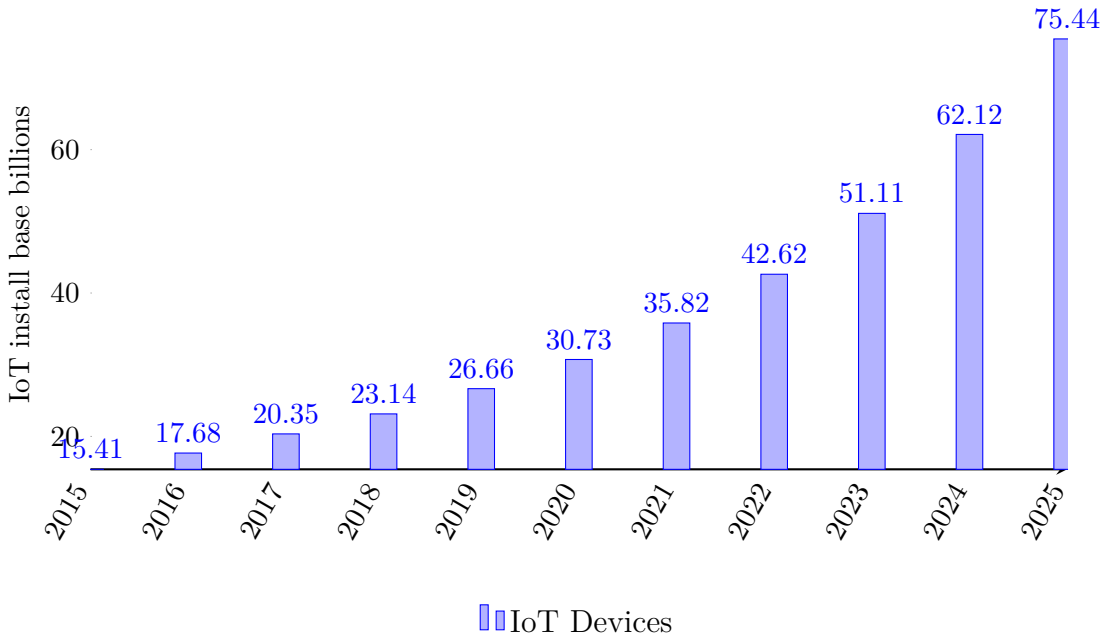


Figure **(1.3)** –IoT Growth 2015 -2025

1.3.1 Industry 4.0

The transformation and digitalisation of industries adopting and leveraging the IoT are commonly known as Industry 4.0. This transformation is enabled using IoT technologies across the industry, widely known as the Industrial IoT, *IIoT*. The industry is undergoing a radical transformation driven by the macro trend of digital transformation [13]. In Europe, this is as Industry 4.0 or *Smart Manufacturing* [14]. Increased sensorisation and advancing sensing techniques enable greater visibility into industrial environments and supply chains [15]. This enhanced data and insight provide a more effective means of managing and optimising every aspect of the production process [16].

The IIoT promises to provide far richer insights, which, in turn, enables faster decision-making across a range of industries. For example, process and production

environments leverage additional sensing connected to legacy machinery to reduce factory downtime and improve throughput [17]. Advanced sensing combined with advanced analytics enables pervasive monitoring of factories, leveraging many lower-cost technologies [18]. Beyond improving factory operations, tighter integration with the supply chain enables greater supply chain transparency, improving product logistics efficiency [19]. The IoT covers many segments, including continuous and discreet manufacturing and hybrid production systems. The promise of the IIoT is in realising intelligent products and production, capable of change in response to data collected from across the interconnected enterprise. They are more modular, flexible, and reconfigurable in such environments [20]. Data is collected and integrated into a much more dynamic fashion [21], fundamentally changing the industry and enabling the fourth industrial revolution.

Broadly the industry is undergoing a significant digital transformation shift, as indicated by the macro trend [13]. In Europe, this is called Industry 4.0 or Smart Manufacturing [14]. With the help of advanced sensor technology, there is increased visibility into industrial environments and supply chains [15]. This improved data collection and analysis allows for better management and optimisation of the production process [16].

The IIoT provides valuable insights that lead to quicker decision-making in various industries. For instance, factories can use additional sensors connected to older machines to decrease downtime and improve productivity [17]. By combining advanced sensors with analytics, factories can monitor operations more effectively and use inexpensive technologies [18]. Integrating the IIoT with the supply chain can also increase transparency and efficiency [19]. The IIoT applies to

various manufacturing types, including continuous, discreet, and hybrid systems. The potential of the IIoT lies in producing intelligent products and adaptable production methods that respond to data from the interconnected enterprise. These systems are modular, flexible, and easily reconfigured [20]. Real-time, reliable data collection and integration are integral to this strategy [21].

The IIoT also extends to merging traditional IT with control and automation systems, commonly known as *operational technology* (OT), which has numerous benefits. This convergence reduces reliance on expensive, custom equipment and improves interoperability between production and other enterprise systems [21]. As IT and OT systems merge, they become more uniform. The convergence of these technologies is desirable for several reasons, including cost savings from using a general-purpose computing infrastructure [22]. The telecommunications industry has already seen the benefits of moving from specialised hardware to software-based systems, transforming network operators' infrastructure management. This transformation is called Network Functions Virtualization [23].

The trend towards automation and modern technology is evident in industrial processes. Cruz et al. have successfully converted a programmable logic controller (PLC) into a software-based system that runs on general-purpose computing hardware [24]. This example illustrates how technology is improving industrial processes. Additionally, modern IT-based technologies such as microservices and orchestration are being explored and adopted in the industry [25]. The convergence of open standards and protocols also contributes to industry advancements. Merchan et al. have demonstrated how open standards and protocols, such as *Open Process Control Unified Architecture* (OPC-UA), enable open source ap-

plications, like *Supervisory Control and Data Acquistion* SCADA systems, for advanced monitoring of industrial processes [26].

IIoT and wireless technologies are becoming increasingly desirable in many industrial applications. Industrial applications rely heavily on IIoT and wireless technologies, but there is still much scope for more widespread use. While wireless technology in ultra-low latency environments is currently limited, there are areas where it is being deployed. One of these areas is advanced sensing, which is the main focus of this thesis. Wireless technologies will play a central role in this transformation as factories and their products evolve. Thanks to time-sensitive networking technologies based on the IEEE 802.1 protocols, the previous limitations of standard networking and communications in factory or process automation have been eliminated [27]. Furthermore, significant advancements in wireless technology have made wireless networks increasingly viable for various time-sensitive industrial applications [28].

These changes represent a significant shift in future industrial systems' design, development, and implementation. By utilising more standard infrastructure and open-source technologies, factories have more significant potential for interoperability, flexibility, and efficiency. This conversion will allow for more dynamic and easily reconfigurable manufacturing processes [29]

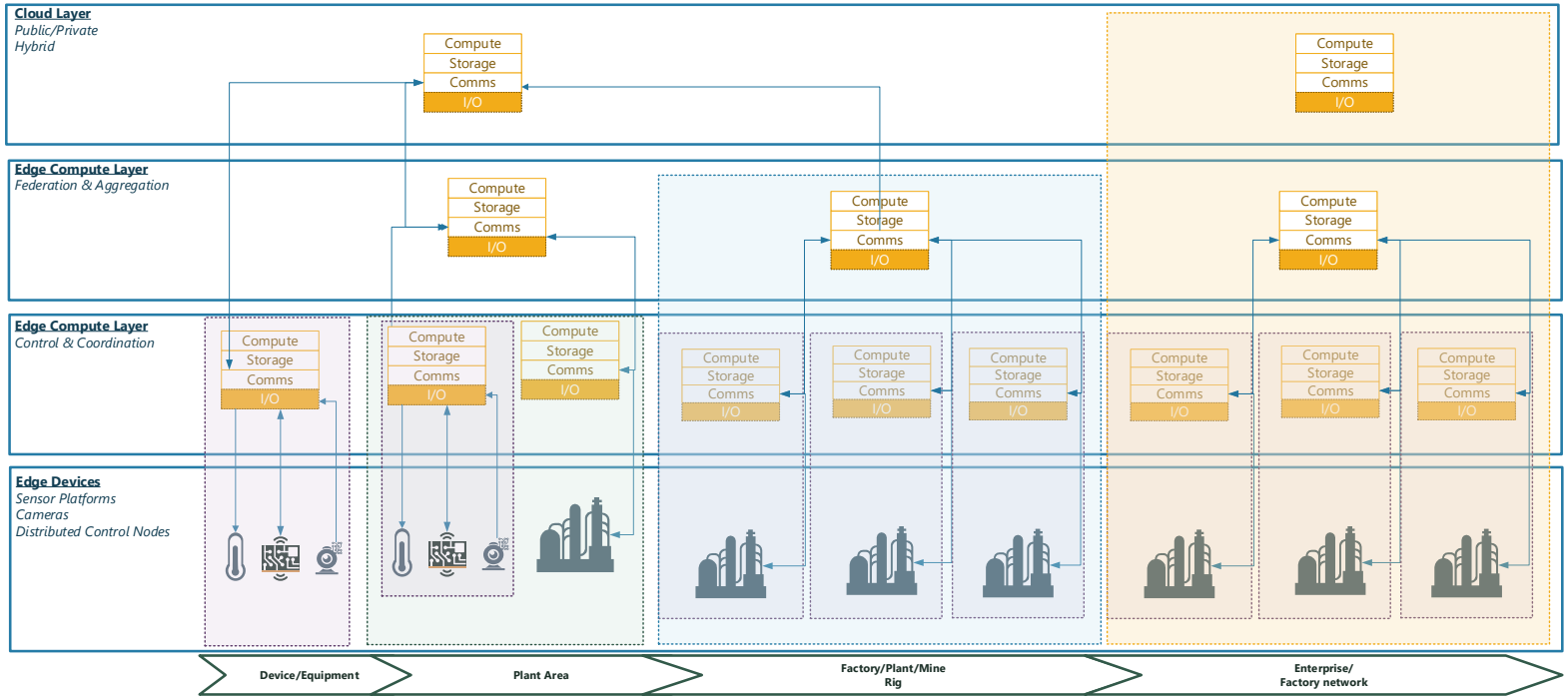


Figure **(1.4)** –A multilayered view of Industrial IoT

1.4 Edge computing

During the beginning stages of IoT, the most common structure was connecting a device to the cloud and sending data from the device to a public or private cloud through gateways. This architecture remains the primary pattern for IoT. However, due to the growth of IoT, the complexity of IoT devices and networks has evolved. IoT devices and architectures have become more advanced, capable of collecting more data from a broader range of sensors and networks [30].

The Internet of Things (IoT) is expanding and evolving, particularly in advanced fields such as self-driving cars and augmented reality. These types of IoT applications require complex data processing and strong network capabilities [31, 32]. In many IoT applications, low latency is critical due to high-bandwidth and multimodal data processing and the increasing number of connected devices.

Regarding industrial applications, meeting application performance requirements is crucial, such as network latency, bandwidth consumption, and security and privacy concerns. As discussed earlier, the round trip time required to transmit data is critical in meeting latency requirements for most applications [33].

Edge computing has become a solution to expand the capabilities of IoT to meet the growing demands of IoT applications. Unlike traditional IoT, Edge Computing goes beyond collecting and forwarding data to the cloud for processing [34].

Edge computing is crucial in applications where control and low latency are needed, such as power management [35]. Other examples are in smart cities and healthcare, demonstrating how the Internet of Things (IoT) is evolving [36]. In

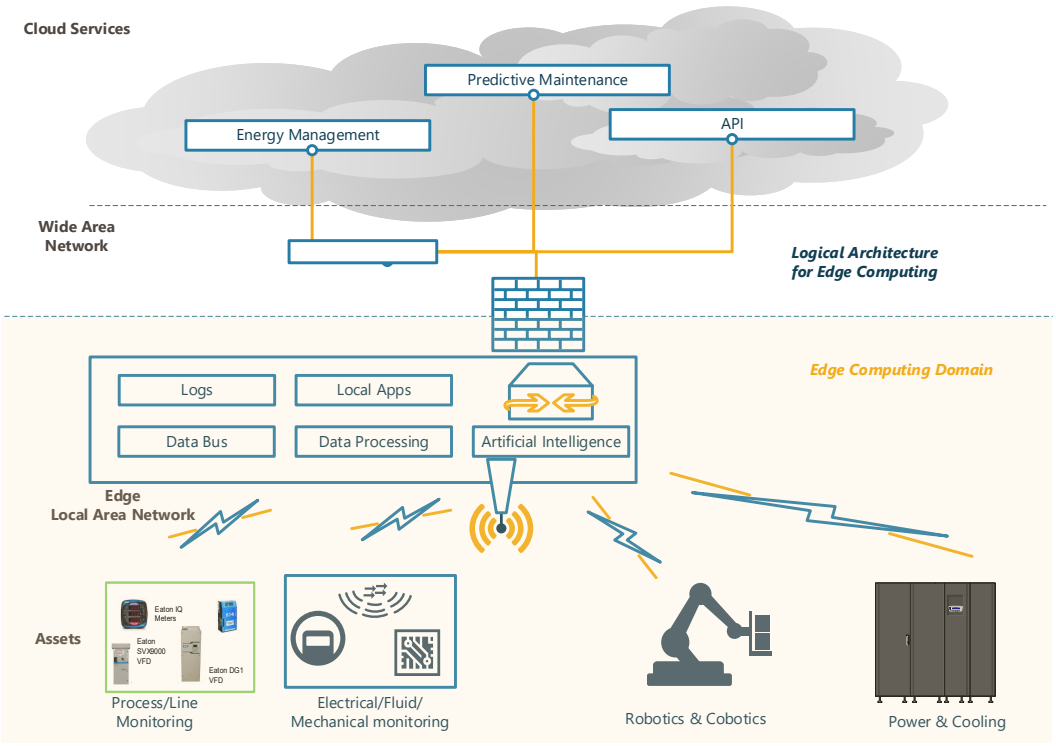


Figure **(1.5)** –Edge computing logical architecture

mission-critical areas with promising potential, edge computing is necessary to meet performance requirements [37]. As a result, edge computing is expanding and enhancing the IoT by bringing cloud and data centre capabilities to where data is created, enabling processing, storage, and action [38].

Edge computing can be viewed as an extension of cloud computing at the network's edge. However, it's more accurately a distributed computing paradigm where computing resources and applications are located closer to where data is created. This technology represents a significant milestone in the evolution of IoT.

Edge Computing involves placing algorithms, computing, storage, and networks between the devices generating data and the cloud or data centre.

Various edge computing architectures have recently gained popularity, including Fog computing, mobile edge computing, and cloudlets [39, 40, 41]. Dolui et al. provides a detailed explanation of the similarities and differences between these paradigms [42]. Despite some differences in radio networks, these computing paradigms offer the same functionality. Yousefpour et al. provide a comprehensive taxonomy of edge-related technologies and concepts [43]. While the technologies presented in this thesis align more with edge computing, we may use the terms interchangeably in subsequent chapters.

Edge Computing offers several benefits, such as improved performance by reducing the costs of moving data across networks. Processing data at the point of creation significantly reduces operating costs associated with managing data. Edge computing is beneficial in closed-loop control applications where the cost of moving data back and forth is too high to meet actuation needs. Satyanarayanan's research shows how high data rate sensing applications drive the demand for edge computing [44]. Cisco's study on the Internet and IoT outlines various use cases that require edge computing applications [45]. Additionally, edge computing addresses concerns about sending all data to the cloud, a topic of concern for many users, businesses, and applications [46, 47].

1.5 Wireless comes of age

. The Internet of Things (IoT) is advancing thanks to the ongoing development of wireless communications and networks [48] rapidly. Wireless technology has become increasingly popular in the industrial sector in recent years, providing numerous benefits such as enhanced mobility and flexibility when managing

machines, processes, and plants [49]. Wireless systems also enable the easy deployment of new equipment and monitoring systems while avoiding the high costs associated with cable installation and wired equivalents [50, 51]. As a result, wireless technologies are helping factory operators achieve greater flexibility and modularity in their factory configurations [52].

Wireless technology is widely used in various industries for many purposes. Wireless licensed solutions like *Mircowave Data Systems* (MDS) and cellular-based solutions ensure reduced interference and reliable communications for industrial process monitoring and control applications, as stated in [53]. License-exempt communications, such as the industrial, scientific, and medical (ISM) bands, have also become prevalent. Technologies like WirelessHART, Wi-Fi, and Zigbee are communication methods, as mentioned in [54, 55, 56]. Besides, low-power wide-area (LPWA) networks have gained popularity for collecting low bandwidth data from non-time-critical applications, as stated in [57]. Wireless technology has evolved and supports an increasingly diverse set of industrial applications.

However popular or desirable these technologies are, some perceive their implementation in industrial environments as problematic. Industrial environments are often harsh and challenging, containing obstructions such as large metallic objects and surfaces, creating the most demanding radio propagation environment [58]. Interference, congestion, and network planning and management are significant barriers to widespread adoption [59]. This is particularly true in large, dense environments [60]. Adopting and using wireless technologies has often been hampered by a perceived notion, i.e., the need for more reliability, integrity, and security in

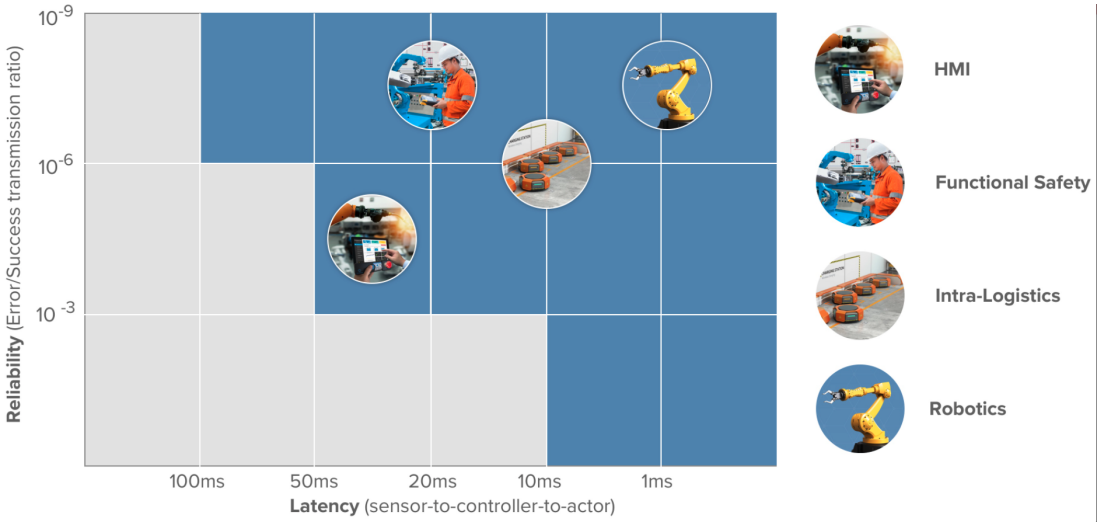


Figure **(1.6)** –Industrial Application Performance requirements

wireless links [61]. In addition, many existing technologies lack the performance requirements of low latency and high bandwidth applications [62].

There remains a degree of scepticism that wireless technologies can meet the needs of ultra-reliable and ultra-low latency communications, which typify IoT communications. Emerging industrial applications such as control systems, robotics systems, and emerging technologies such as immersive digital twins will depend on the flexibility of wireless industrial networks. Traditionally, the commonly deployed technologies in industrial applications struggle to meet the latency and reliability requirements of the applications described in Figure 1.6.

1.5.1 Wi-Fi and 5G advances

In recent years, wireless technology has made significant progress, resulting in two notable advancements in wireless communication. The fifth generation of mobile

network standards enhances performance and caters to emerging IoT requirements in various industries.

In addtion the IEEE 802.11 standard, which the Wi-Fi standard is based upon has also had many advances. Cavalcanti et al. explain how cellular and Wi-Fi-based technologies have evolved, enabling wireless capabilities suitable for industrial applications [63]. 5G offers three services that are essential for diverse industrial applications. They include:

- **URLLC (Ultra-reliable low latency communication)**: Enables service for latency-sensitive devices such as factory automation, autonomous vehicles and haptic internet applications. URLLC targets require sub-millisecond latency performance with error rates that are lower than one packet loss in $< 10^{-5}$ packets
- **mMTC (Massive machine type communication)**: Provides narrow-band Internet access for high-density devices typically used for sensing, metering, and monitoring devices and applications.
- **eMBB (Enhanced mobile broadband)**: High bandwidth internet access is suitable for video streaming and augmented and virtual reality applications. While primarily targeting phones, this service provides support for applications using video of vision based systems also.

The latest Wi-Fi technology, Wi-Fi 6, has significantly improved over its predecessors, Wi-Fi 5 or IEEE 802.11ac. Wi-Fi 6 offers enhanced efficiency, better performance, lower latency, and increased capacity, making it an exciting prospect

for industrial IoT. We will briefly overview these improvements in this section and delve into them in more detail in Chapter 3.

- **OFDMA (Orthogonal Frequency Division Multiple Access)** is a crucial feature of Wi-Fi 6. The use of OFDMA is a significant reason for the performance leap of Wi-Fi 6.OFDMA enables much more efficient use of the Wi-Fi channels, which improves the network's uplink and downlink efficiency.

- Wi-Fi 6 has introduced a groundbreaking innovation using the **6 GHz** spectrum. This spectrum offers four times more available frequency compared to previous versions. With the 6 GHz frequency band, Wi-Fi channels can now be doubled from 80 to 160 MHz, allowing faster speeds exceeding >1 Gbps and a $\leq$ ms latency. However, since the 6 GHz spectrum is already in use, Wi-Fi 6E devices must adhere to specific standards to limit interference and enable outdoor use. These standards include Low Power Indoor and automated frequency coordination. These features will be included in future Wi-Fi releases and are designed to make the 6 GHz spectrum future-proof and avoid the congestion issues experienced with the 2.4 GHz and 5 GHz bands.

- **MU-MIMO (Multi-User Multiple Input, Multiple Output)** allows more data to be transmitted simultaneously. It supports increased user access and capacity, allowing multiple simultaneous applications. With up to 8 spatial streams, more uplink and downlink data transmissions are possible on the same channel.

- **1024 QAM**In Wi-Fi 5, a Quadrature Amplitude Modulation (QAM) modulation scheme was utilised. In Chapter 3, we will delve deeper into QAM. Wi-Fi 6 introduced 1024 QAM, which can boost throughput by around 25%. This feature is essential in densely populated areas like industrial hubs where high-quality service is essential.

1.5.2 The case for Wi-Fi

There has been a lot of discussion and attention recently regarding the development of 5G technology and its ability to support Ultra-Reliable Low Latency Communications (URLCC) applications. This technology can potentially revolutionise many challenging industrial applications [64]. Companies such as Nokia and Ericsson have already begun deploying 5G networks, which are expected to become more prevalent in industrial wireless solutions. Private 5G networks are likely the preferred deployment model for industrial applications. Emerging architectures and designs are already tailored to industrial use cases [65].

Using 5G-based technologies in industrial applications has several advantages. Firstly, 5G technology has a solid and reliable foundation. Additionally, it can use a variety of frequency ranges, making it an ideal technology for various applications, particularly in logistics and asset tracking, where it can provide coverage over vast areas [66].

While 5G is a good choice for network connectivity, Wi-Fi 6E is also attractive. 5G technology and Wi-Fi 6/6E share standard features, including OFDMA, MU-MIMO, and QAM modulation, which help achieve Gigabits throughput for better spectrum efficiency. However, not all industries have fully embraced the latest

advancements in Wi-Fi or explored its potential impact. Nevertheless, Wi-Fi can be a viable option for industrial applications and compete with 5G technology.

In many cases, it is not a matter of choosing one option over the other but determining which specific technology meets the needs or requirements of the business or application.

While Wi-Fi is a popular and affordable option for many businesses due to its widespread availability, it can easily integrate with existing infrastructure, expertise, and applications. With advancements in Wi-Fi technology, it has become a feasible solution for most industrial uses. However, further research is needed to confirm the potential benefits of Wi-Fi.

We aim to explore the possibilities of using Wi-Fi in industrial wireless networks and address any unanswered or new questions related to this topic.

1.6 Research Motivation

The Industrial Internet of Things (IIoT) has seen significant growth in recent years. IIoT applications are using more advanced sensor technologies to improve data accuracy and effective networking and communication technologies to collect and transport data quickly. Edge computing is a viable solution that offers efficient data movement and closed-loop control with fast response times.

Wired networks in industrial settings can be inflexible and expensive, requiring more adaptable solutions to accommodate the growing need for mobility and flexibility. While industrial wireless networks have faced challenges with interference

due to harsh RF conditions, recent advancements have made supporting higher bandwidth and more demanding applications possible.

With the introduction of 5G and updated Wi-Fi 6, wireless industrial systems have been presented with new possibilities. These standards prioritize performance and reliability, with 5G focusing on ultra-reliable and low-latency networks (URLLC). The IEEE 802.11ax standard enables Wi-Fi 6E to be a significant improvement on previous versions. Both standards utilize technologies like OFDMA, advanced QAM, and MU-MIMO, which enable better frequency spectrum usage and higher throughput.

The enhanced performance of wireless and process control technologies offers greater flexibility in adding or configuring mobility applications, reducing wiring costs and complexity in factories and machines. The potential for wireless industrial systems to transform the industry is significant.

While some companies are taking advantage of these opportunities, there are still doubts about using Wi-Fi for industrial wireless networks. Despite the technological advancements introduced by Wi-Fi 6, it remains to be seen if it can meet the growing bandwidth demands of industrial applications. Additionally, the use of 6GHz is still in its early stages.

Industrial enterprises are increasingly interested in open-source technologies and interoperability to reduce infrastructure costs. However, a thorough evaluation is necessary to determine how these technologies can be integrated to create a cohesive solution.

This thesis examines the potential of Wi-Fi 6E technology in industrial environments and its ability to support various applications such as prognostics, health management, and emerging Digital twins applications.

1.7 Research question

This thesis addresses the question of ***Can IEEE 802.11ax technologies support high reliability wireless industrial networks, and more specifically*:**

- [**R1**] What are the current and emerging applications for wireless industrial networks?
- [**R2**] What is the current state of the art in industrial wireless networks?
- [**R3**] How is the radio propagation environment impacted in additive manufacturing industrial facilities?
- [**R4**] Can we design an IEE802.11ax Wi-Fi 6 industrial wireless system for modern industrial applications?
- [**R5**] Can we improve interoperability between legacy industrial standards by leveraging modern IoT protocols
- [**R6**] Can our candidate design meet the communication requirements of International standards for industrial wireless networks

1.8 Contributions

Our dissertation introduces advancements in industrial wireless systems by utilising Wi-Fi 6E technology. We have created a robust industrial wireless system that can support advanced applications such as predictive maintenance and monitoring of industrial processes and equipment. Our proposed system has undergone rigorous testing in a sophisticated industrial testbed, surpassing the performance standards set by both US and European authorities.

We have designed comprehensive system protocols that ensure seamless interoperability between legacy industrial systems and modern industrial IIoT protocols. Our contribution includes providing optimised implementation code for deployment in Linux-based computational environments.

We have also designed an innovative IEEE 802.11ax-based multimodal sensing system compatible with the prevalent Arduino hardware within the open-source ecosystem. Our contribution includes developing a meticulous test and validation paradigm that objectively evaluates the network's design proficiency and operational performance against established metrics.

The body of work presented in our dissertation encompasses a range of contributions, summarised as follows:

- **Industrial IoT Analysis:** A deep analysis delineating contemporary trends within the realms of Industrial 4.0 and IIoT, identifying strategic application domains poised for transformational impact through IIoT implementation.

- **Wireless Industrial Networks:** A critical evaluation emphasises wireless networks' escalating significance within industrial settings, featuring a nuanced analysis of prevalent wireless technologies, their applicability, strengths, and inherent limitations.
- **5G and Wi-Fi 6 Assessment:** A thorough review focused on applying emerging 5G and Wi-Fi 6 technologies, elucidating their transformative features and assessing their consequential impact on industrial wireless networks' operational reliability and performance.
- **Channel-Sounding Methodology:** The definition of a novel methodology to enable precise channel characterisations, fostering enhanced testing capabilities essential for the evolution of wireless industrial networks.
- **Industrial Interference Investigation:** A detailed exploration into industrial environments' multifaceted interference landscapes yields critical insights for enhancing network resilience and performance.
- **6 GHz Spectrum Evaluation:** A comprehensive exploration of the 6 GHz spectrum for industrial wireless communications, enriched by empirical assessments to optimise performance outcomes.
- **Edge Architecture:** The formulation of a novel edge architecture, capable of supporting wireless communications through open-source and standards-based technologies
- **Interoperability Framework:** Conception of an interoperability protocol architecturally designed to facilitate the integration of contemporary

IIoT applications with existing legacy infrastructures without necessitating extensive modifications.

- **Novel Database Design:** A new database design that augments the Industrial IoT and Edge computing landscape, significantly enhancing the applicability of the IEEE 1451.3 TEDS standard.
- **Wi-Fi-based Test Methodology:** Introduction of a novel Wi-Fi-based testing paradigm designed to enhance state of the art in wireless industrial network evaluations.
- **Analysis and Evaluation of Test Data:** A comprehensive analytic framework was established to facilitate rigorous assessments of Wi-Fi 6E-based network suitability across diverse industrial applications, delivering invaluable design and implementation insights.
- **Performance Evaluation of Wi-Fi 6E:** Execution of a meticulous performance evaluation regimen aimed at extrapolating the practical proficiencies of Wi-Fi 6E within real-world industrial settings, thereby contributing foundational insights pivotal for the strategic deployment of high-performance wireless industrial networks.

1.9 Organisation

- Chapter 1 provides a general introduction to the Internet of Things, Industrial IoT, and industrial wireless networks and provides a broad overview of the major themes of this work
- Chapter 2 evaluates the state-of-the-art in Industrial IoT and associated applications
- Chapter 3 analyses industrial wireless networks and the current state of the art across the primary technologies used in wireless industrial networks
- Chapter 4 outlines our radio propagation testing methodology conducted for IEEE802.11ax systems at the Irish Manufacturing Research test bed facility.
- Chapter 5 details the design and implementation of the system as well as the message protocol the system uses.
- Chapter 6 defines and examines the performance of our system against international standards for industrial wireless networks
- Chapter 7 concludes the work and reflects the questions these works seek to answer work addresses

Chapter 2

Industrial digital transformation

This chapter provides an evaluation and analysis of the state of the art in industrial IoT. The contributions of this chapter include the following:

- We extensively analysed trends in Industrial 4.0 and IIoT. We identified promising application areas where IIoT can impact industrial operations.
- Our analysis has explored three application areas: industrial and control systems, prognostics and health management, and digital twins for industrial systems. We have identified different approaches and emerging challenges and opportunities for each area.
- Furthermore, we have highlighted the increasing significance of wireless networks in industrial technology and outlined the pivotal role that open-source technologies play in transforming outdated industrial systems.

2.1 Industry 4.0

Industry 4.0 and the fourth industrial revolution refer to the advancement of manufacturing and production systems and related processes in various industries [67]. The idea was first introduced by the German government in 2006, and later, in 2011, it was more clearly defined concerning the Internet of Things (IoT) [68]. The US has also significantly contributed to this field with the "industrial internet" and intelligent manufacturing [69]. China has adopted its "Made in China2025" initiative, while Japan has the "Robot Revolution Initiative" and its broader Society 5.0 [70, 71]. Although their approaches may vary slightly, they share the same fundamental principles. Industry 4.0 and its equivalents worldwide rely on intelligent machines and increased connectivity to automate and optimise operations. This greater interconnectivity and interoperability allows a closer connection between the physical and digital worlds. Industry 4.0 is an umbrella term that describes the convergence of many technologies and broader trends in industrial applications. The intersection of Cyber-Physical systems and the IIoT, as illustrated in Figure 2.1. We will discuss both in more detail in this chapter.

2.1.1 Characteristics of Industry 4.0

The interaction of numerous technological advancements defines Industry 4.0. We have compiled a representative list of some key characteristics, which, while not exhaustive, provide an overview of Industry 4.0. These extensive characteristics cover a complete transformation and integration of the manufacturing value chain [72]. This transformation includes the adaptation of existing or new processes

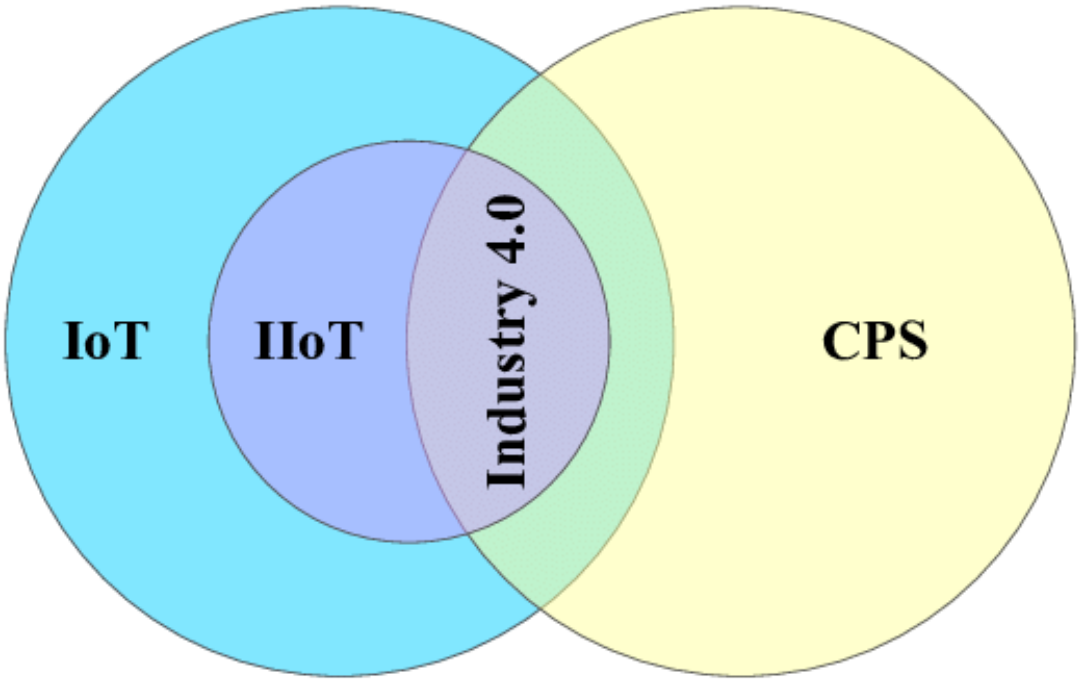


Figure **(2.1)** –Industry 4.0 sits at the intersection of multiple technologies

in factories or industrial processes [73]. The value chain integration extends beyond the factory and into a more unified and intelligent supply chain, as described by Rondero et al. [74]. This interconnected ecosystem changes mass production from mass customisation to mass personalisation, enabling manufacturing systems to produce highly customised parts for individual customer needs dynamically [75]. One such example of this technology can be seen in the medical device industry, where medical devices are manufactured specifically for individual patients [76, 77]. A broadly applicable set in industry 4.0 characteristics includes:

- Enhanced automation and autonomous machines and systems including robotics [78]
- Greater convergence of the physical and digital worlds through cyber-physical systems [79]

- Increased the use of modern computing paradigms such as virtualisation, cloud computing, and big data [80]
- Flexible, dynamic, decentralised systems usurping the traditional automation pyramid [81]
- Migration of flexible manufacturing, customisation or personalisation of products and services [82]
- Integration of systems into a *'systems of systems'* into an industrial internet [83]
- Greater convergence of the IT/OT worlds [84]

2.1.2 Industry 4.0 & IIoT applications

As previously stated, varied and diverse applications make up Industry 4.0. We focus on our analysis of three leading areas of Industry 4.0 where the IIoT arguably has the most impact across the industrial landscape [85, 86].

Previously, we discussed the evolution of Industry 4.0 and numerous incarnations of the global digital transformation of industry and manufacturing. We consider Industry 4.0 to be the overarching theme to describe the broad transformation of manufacturing and industry, incorporating technologies, services, and processes in a single term [87].

IIoT applications are a sub-grouping of Industry 4.0, an enabling capability. Frank et al. outline four key elements: Internet of things, cloud services, big data, and analytics [88]. The integration of these technologies has enabled a broad range of industrial applications to take root across the industrial landscape. More

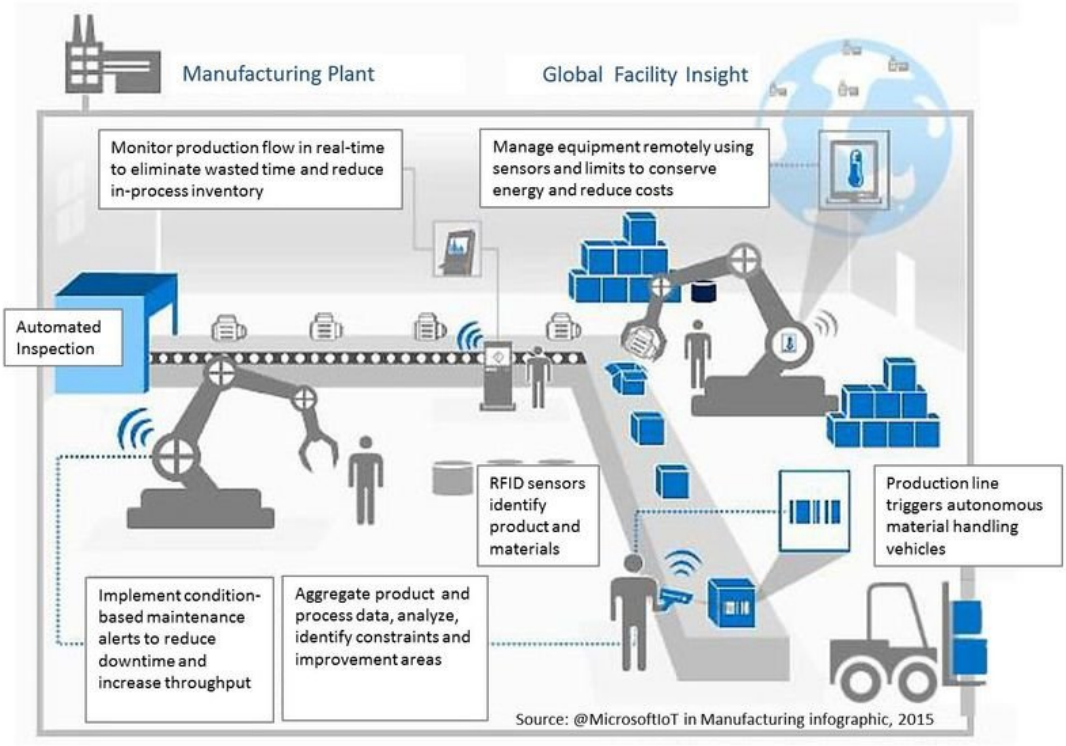


Figure **(2.2)** –Example of smart factory
[source: Microsoft]

specifically, the IIoT allows objects to be sensed and controlled remotely across the existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in improved efficiency, accuracy, and economic benefits.

As of 2020, the most popular and fastest-growing application of the IIoT was in manufacturing and industrial applications [89], with a 22% share of enterprise IoT projects. According to a white paper published by PTC, a world-leading IIoT platform provider, the top ten use cases in the Industrial IoT account for 70% of the total applications used in the Industrial IoT [90].

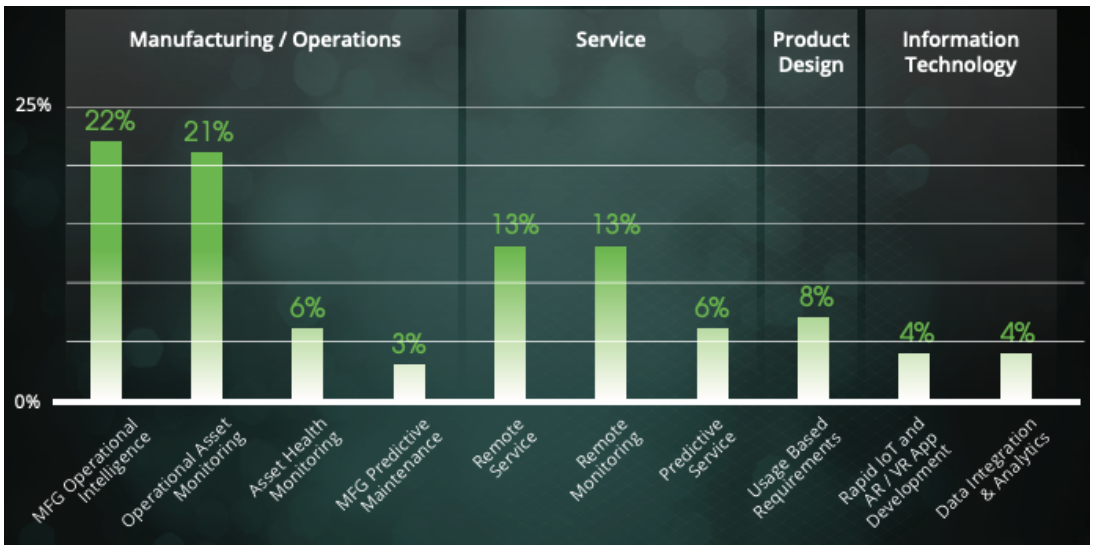


Figure **(2.3)** –Top 10 Industrial IoT applications [source: PTC [91]]

According to various reports, the top applications of industrial IoT include manufacturing, operational intelligence, and service and support applications, like remote monitoring and service [91]. These applications are highly desirable and impactful, especially in manufacturing operations and remote monitoring [92]. Industry 4.0 use cases will continue to grow in the future. The reports distinguish between remote service and predictive maintenance and highlight the critical areas of interest and their relative importance in IIoT. In the following sections, we will discuss each area in detail.

2.2 Industrial Automation & Control Systems

Industrial automation and control systems, (ICS), describe integrating control systems, machinery, devices, and equipment to operate various manufacturing processes and operations [93]. ICS, or IACS, describes multiple control and

automation systems that enable various manufacturing operations. Manufacturing operations comprise manufacturing, monitoring, management, and improving production processes [94].

Automating machines, processes, and tools allows efficient industrial operations using advanced software tools to monitor, operate, and continuously improve industrial processes. Manufacturing operations often use established methodologies such as Six Sigma, lean manufacturing and Overall Equipment Effectiveness(OEE) to achieve their productivity goals [95, 96, 97].

Almost all industrial methodologies monitor the parameters collected by sensors from plants and equipment. Sensors can be embedded into the machine or retrofitted . Data collected from these sensors can provide feedback to control actuators or adapt the equipment in real-time based on the sensor readings [98]. Industrial Automation systems tend to differ according to the manufacturing process or operations in question [99]. Manufacturing processes are broadly defined as follows:

- **Continuous process**
- **Discrete process**
- **Hybrid process**

Example process types are outlined in Table 2.1.

Manufacturing operations rely on reliable systems with low latency. These systems must perform at a high level and often consist of multiple interconnected systems that manage complex manufacturing processes.

Discreet	Process	Hybrid
Additive manufacturing & 3D printing	Cement kilning	Beverage mixing
Automated assembly	Chemical manufacturing	Brewing
Canning and bottling	Glass making	Dough mixing
Injection moulding	Paper manufacturing	Food processing
Metal forming	Power generation	Paint mixing
Packaging	Water treatment	Pharmaceutical processing

Table **(2.1)** –Manufacturing process types and examples

The unique requirements for each manufacturing operation will determine the necessary level of latency and reliability. The automation and control systems used will also play a significant role in determining the performance criteria.

The requirements for latency and reliability will vary based on the specific needs of the automation system and optimisation applications. Some common examples of process- or flow-based systems include oil refineries, chemical or water treatment plants, and recycling refineries, which all involve continuous processing of raw materials.

Level	Description	Examples
0	Defines the actual physical processes	
1	Defines the activities involved in sensing and manipulating the physical processes.	Intelligent Sensors
2	Defines the activities of monitoring and controlling the physical processes.	PLCs, DCS, SCADA
3	Defines workflow activities to produce the desired end products.	MES
4	Defines the business-related activities needed to manage a manufacturing operation.	ERP systems, Eg2

Table **(2.2)** –ISA-95 Levels description and examples

The ISA-95 international standard is widely used for integrating control and automation systems into business [100]. It is represented in a hierarchical structure,

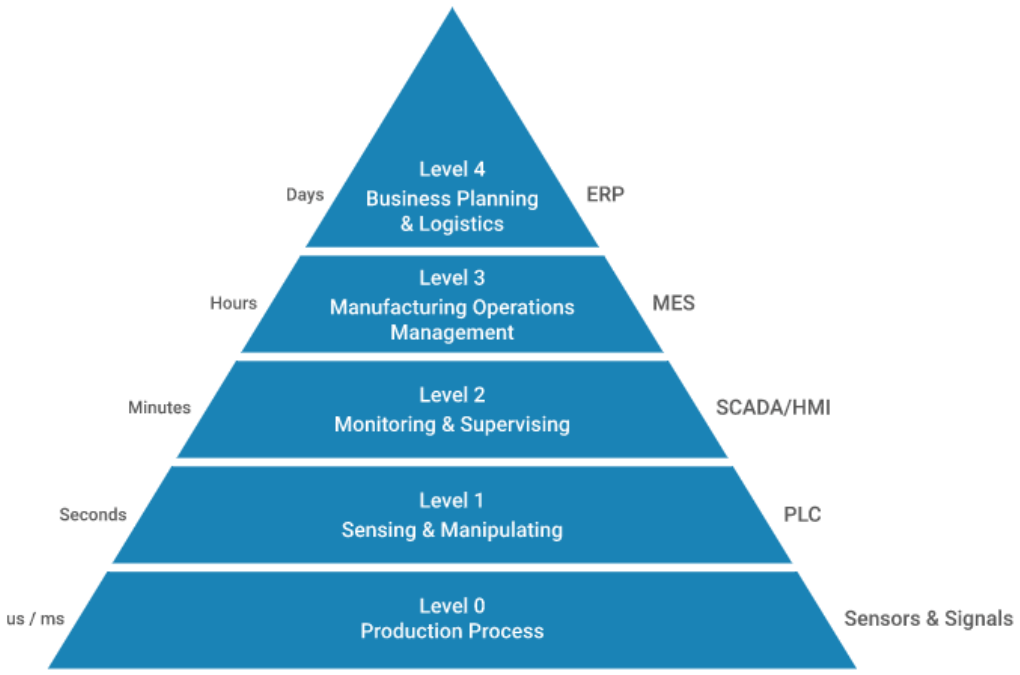


Figure **(2.4)** –ISA Layered automation pyramid

the automation pyramid, consisting of layers [101]. The operational technologies (OT) that comprise the pyramid were traditionally isolated from IT systems and comprised proprietary automation and control protocols [102]. Interoperability and interconnectivity were limited, with little connectivity to external systems [103, 104].

Bespoke and proprietary systems are often costly to purchase, manage and operate. Even with ICS, there is a migration towards adopting more open protocols such as Internet Protocol (IP) and general-purpose computing hardware to manage the cost and vendor lock-in, which has been a challenge in the ICS area [105]. The increasing risk and challenges around cybersecurity are also a solid motivation to embrace more open ecosystems where systems are up to date with the latest security technologies [106].

Consequently, many products used across ICS are increasingly adopting general-purpose into existing technologies such as embedded systems, networking equipment, and commercial software to run their operations [107]. The architectural conversion of ICS systems to general-purpose technologies enables the continued convergence of OT and IT systems. This convergence leverages cloud computing virtualisation, allowing manufacturers and industrial system operators to redesign the systems that run their operations. The most common type of system uses supervisory control and data acquisition (SCADA) systems [22].

SCADA systems consist of hardware and software components that monitor and control various processes and systems. These systems allow for remote control and monitoring of continuous and discrete processing methods, including activating alarms and valves, motors, and pumps. Additionally, SCADA systems enable the centralised management and reporting of alarms through visualisation software and human-machine interfaces (HMI) [106]

SCADA systems typically consist of Programmable Logic Controllers (PLC) or Remote Terminal Units (RTU). These gather input data from sensors that are connected to machines. PLCs and RTUs control devices through actuators directly impacting the monitored machines or processes. Communications networks connect sensors and actuators to PLCs and RTUs, which can be wired or wireless, although wired connections are more common historically. HMI displays the collected data in various visualisations, allowing humans to operate, manage, and control the system based on the information presented. SCADA systems are the most widely used form of ICS in the manufacturing industry today.

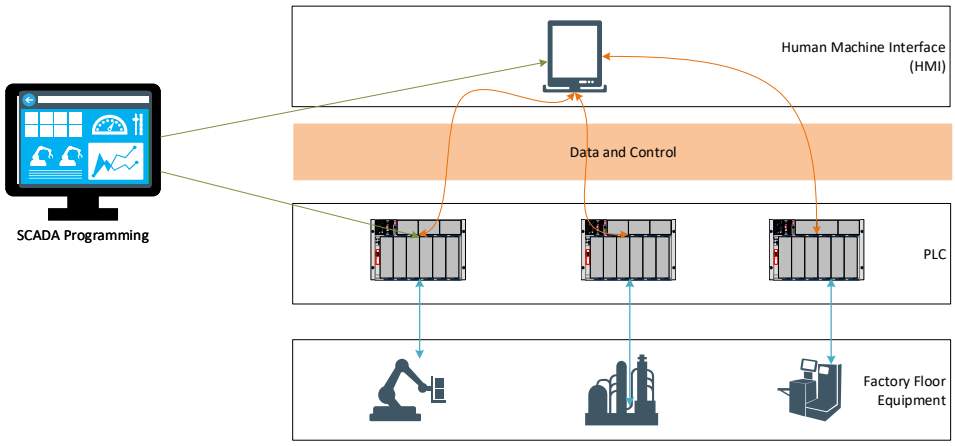


Figure **(2.5)** –SCADA system and main components

A type of control system frequently used is the Distributed Control System (DCS). This system employs automated local controllers connected to a central controller through a computer network, like Modbus [108]. The local controllers are responsible for controlling the devices in industrial settings. DCS is commonly used in large-scale manufacturing environments that involve continuous process manufacturing. Although DCS and SCADA can control and monitor manufacturing operations, some differences exist. DCS may have slower data processing, which can be crucial in specific applications. SCADA systems are typically utilised in larger, remote, and dispersed locations. At the same time, DCS manages sub-controllers and monitors their set points in factories or plants across the industrial setting.

Manufacturers have relied on traditional ICS systems for a long time due to their reliability and functionality.These systems were not designed with flexility and reconfiguration in mind. Automation systems have been slow to embrace new technologies, partly due to the mission-critical nature of existing systems. Despite this, virtualisation and cloud computing technologies are helping to create a more dynamic, open, interoperable control architecture for the future. One example is the Open Process Automation framework from the Open Group, which is gaining popularity among manufacturing companies [109]. Microsoft also has a vision for the future of industrial control, using container technologies and artificial intelligence in project Bonsai [110]. Furthermore, the virtualisation of ICS technologies, such as virtual PLC, is gaining interest within the industry [111]

With the rise of Industry 4.0, industrial control systems in the IIoT will need to adapt to meet the changing landscape. As these systems continue to grow and utilise new technologies, they must support a more flexible and dynamic environment.

There is some debate about whether SCADA is a part of the IIoT ecosystem. Some people argue that SCADA system is a part of the IIoT, while others see SCADA as simply a predecessor to the IIoT. Although SCADA systems have evolved to connect to the Internet, they offer a different level of analytics and connectivity than the IIoT.

The Industrial Internet is the integration of the physical and digital worlds. Companies can use sensors, software, machine learning, and other technologies to

gather and analyse data from physical objects or large data streams. This enables them to manage operations effectively and make informed decisions.

Application Class	Latency	Pr. Loss	Devices
Monitoring	$l < 1s$ 0	$r < 10^{-}5$	$s < 10000$
Supervisory control			
Flow-based	$l < 100ms$	$r < 10^{-}6$	$s < 30$
Job-based	$l < 100ms$	$r < 10^{-}7$	$s < 10$
Feedback control			
Flow-based	$l < 10s$	$r < 10^{-}6$	$s < 1000$
Job-based	$l < 10ms$	$r < 10^{-}7$	$s < 10$
Safety alarming	$1 < 1s$	$r < 10^{-}7$	$s < 10$

Table **(2.3)** –performance requirements for industrial application

The industries that involve the continuous movement of raw materials include paper mills, oil refineries, water treatment plants, and chemical reactors. These systems aim to minimise equipment downtime and enhance process efficiency. In case of any machine breakdowns, they strive to fix them promptly to avoid production delays. They continuously seek ways to enhance performance and productivity by incorporating more sensors and optimising operations. While collecting and analysing data from these systems is challenging, it also presents an opportunity for improvement. Early IoT installations have proven beneficial, leading to further development in this field.

2.3 Prognostics and Health Management

Maintenance is a crucial activity in almost all industries as it ensures the proper functioning of machines and prevents unexpected downtime or outages that can negatively impact production or customers. According to a report by Vanson Bourne, unplanned downtime and its consequences can be very costly for busi-

nesses, regardless of their industry in [112]. Therefore, industries need to have a maintenance strategy in place. A U.S. National Institute of Standards and Technology (NIST) study revealed that maintenance activities cost approximately $74 billion in the U.S. alone [113]. This number will continue to rise in the coming years. The same report highlights the benefits of adopting advanced maintenance techniques, including 44% reduction, lower defects 54%, and 35% fewer lost sales. Implementing advanced maintenance is crucial for any manufacturing organisation.

Prognostics and Health Management (PHM) refers to developing and applying advanced monitoring, diagnostics, and prognostics in various industries and industrial processes [114]. It is a significant area of interest in IIoT and Industry 4.0. PHM tools detect and identify when a component or process is not operating as expected. This helps determine the likely mode of failure and potential remediation. PHM systems aim to reduce major failure events and improve the performance and operation of industrial systems and processes. PHM systems seek to predict or determine the cause and manner of failure, which can lead to cost savings and avoidance of scheduled maintenance activities [115]. Additionally, PHM is essential in ensuring high availability and reducing downtime.

Automation in PHM is on the rise, as it involves advanced computational capabilities to examine a system's health or its components. The latest PHM systems use a combination of physics-based and data-driven models to detect faults, also known as anomaly detection. These systems aim to identify the type of potential fault, called diagnostic, and categorise it accordingly. Additionally, the system can predict how long the machine will operate with a particular fault after determining its failure mode, known as prognostics. With the increased connectivity of

equipment and the availability of data for advanced analytics based on Machine Learning (ML) techniques, there are more significant opportunities to identify and diagnose potential failures in monitored equipment. This trend is known as data-driven PHM and is gaining attention across many industrial operations.

2.3.1 Maintenance types

- **Reactive Maintenance** (RM) repairs a machine or component when the component fails and will no longer function or operate. A reactive maintenance approach means that an element will run to failure, which means the amount of maintenance and resource costs can be kept low. This also means the equipment will not experience planned downtime. A machine effectivel runs until it fails. This wil incur downtime breaks in production and cost. Reactive maintenance, related to run-to-failure, corrective, failure-based, and breakdown maintenance, is generally done after the equipment has failed or stopped [116].

  However, there are risks associated with the RM approach. First and foremost, if a machine is allowed to fail, the potential health and safety implications could be significant, with a possible catastrophic failure resulting in unforeseen consequences. Such unanticipated outcomes could also result in extra costs and increase the time to repair significantly. RM approaches introduce significant risk and uncertainty by allowing components or equipment to fail in such a fashion. This uncertainty is far from ideal in many manufacturing environments.

- **Scheduled maintenance** (SM) and Preventative Maintenance (PM) are time-based maintenance based on performing against specific schedules or defined times. This type of maintenance activity is arguably the most common form of maintenance. PM activity is performed on a predefined schedule with preventive maintenance, time-based or based on the usage of a component [117]. The goal of PMs is to avoid downtime and have defined times for work and inspections to be carried out on the machinery. While an improvement to reactive maintenance, preventive maintenance involves downtime and cost, especially when the maintenance cycle takes time and is frequently required. Determining when components are nearing failure and scheduling downtime for maintenance rather than waiting for a potentially catastrophic failure is of great interest to industrial firms due to the cascading consequences that system outages can have across business segments.

  Proactive maintenance, PaM primarily focuses on preventing failure in an asset and focuses on the actual condition, understanding and addressing the underlying root cause of issues. PaM requires a deeper understanding of the equipment in questions and often involves more complex analytical approaches and tools. Given the costs associated with downtime, even unplanned downtime, there is a strong desire to perform maintenance when required, a *"right-on-time approach"*, ensuring the machines can operate with higher availability and avoid unplanned downtime.

  PaM primarily focuses on preventing failure in an asset by making design or operational changes to equipment to address the route cause of issues [118].

Proactive maintenance is an emerging strategy with tremendous potential for further minimising equipment and process downtime.

- **Predictive maintenance** (PdM) is a *reliability-based* or Condition-based *CBM* maintenance strategy that involves monitoring assets and process performance and their underlying condition based on the probability of failure or actual physical condition of the equipment in question [119]. The goal of PdM is to prevent unplanned, unscheduled downtime or machine failure but to predict failures before they happen [120]. This can be achieved by visually inspecting the machine for damage or signs of imminent failure. Today, the most common approach to PdM is the deployment of sensors to collect and monitor the data collected during the operation of the machine. PdM is sometimes referred to as condition-based monitoring. Data is collected from machines via a wired or wireless network. This data collected from sensors is stored and trended over time to establish the performance characteristics of the machine. The data is used to create models to determine the remaining useful life of an asset. A key advantage to PdM is that maintenance is performed when required and not scheduled. The data and trends inform maintenance teams when to take action when a high probability of failure is likely. [121]. Leaving an asset operational without scheduled maintenance is a significant advantage, enabling greater uptime and utilisation. Reacting to failure in a just-in-time fashion also has significant commercial advantages. This is true for process or discreet manufacturing environments. PdM has often focused on higher-value assets, as installing such solutions can be

expensive. The expense can include cabling, sensors, and integration with existing systems. PdM's value and usefulness are well established [118].

- **Prescriptive Maintenance** *(RxM)* builds on the PdM by using sensors to understand an asset's state instead of just predicting when a failure will occur. It provides or *prescribes* a recommended course of action to take, which can delay or prevent the failure from occurring [122]. Prescriptive systems often leverage machine learning and AI to evaluate historical data, patterns, behaviours or anomalies [123]. Multiple scenarios are often tested computationally, and recommendations are based on the most desirable probabilistic outcome [124]. Often, PdM models use a combination of edge and cloud computing resources. The value of PdM or RxM to ensure asset performance is even more pronounced in remote locations where access might be hazardous or costly. The ability to monitor and maintain such assets has both an economic and human safety benefit [125].

Strategy	Reactive (RM)	Proactive (PM)	Predictive (PdM)	Prescriptive (PaM)
Schedule	Fail/Fix	Time/Usage	Reliability/Condition	Continuous Monitoring
Object	Comp, Sub, Sys	Comp, Sub, Sys	Comp, Sys, Proc, Func	Comp, Sys, Proc, Func
Planning	On the Fly	Ideal Interval	Planned	Planned
Human Intervention	High	Intermediate	Low	Low
Tech Dependency	Low	Medium	High	High
Cost Effectiveness	Labour Intensive	Costly, Often Over	High, Reduced Costs	High, Mitigates Failures

Table (2.4) –Summary of maintenance types and examples

2.3.2 PHM Process

Prognostics and Health Management (PHM) is an advanced discipline that builds upon traditional maintenance strategies like Predictive Maintenance (PdM), Preventative Maintenance (PaM), Condition-Based Maintenance (CBM), and Reactive Maintenance (RM). By harnessing data-driven and model-based techniques, PHM provides real-time assessments of system health and estimates the remaining useful life of equipment. This holistic approach integrates the best aspects of previous methodologies to reduce unplanned downtimes, enhance system availability, and

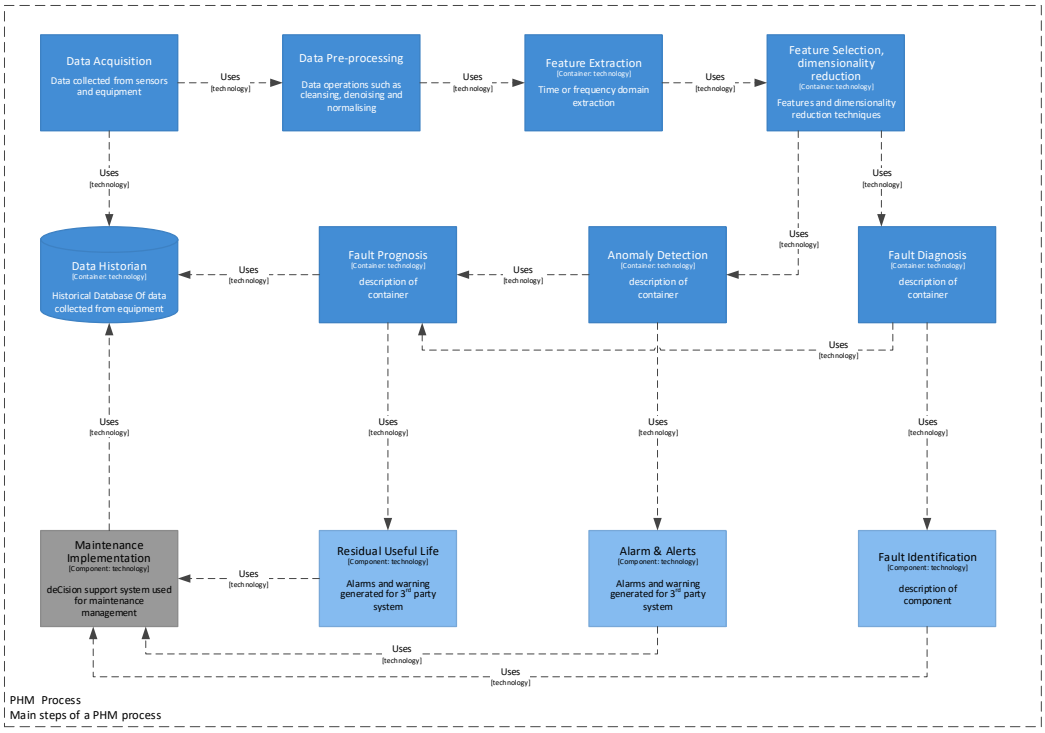


Figure **(2.6)** –PhM process overview

optimize overall maintenance strategies.. A PhM process is presented in Fig. 2.6, which includes many subprocesses

PHM monitors data collected from machines or processes to determine the *state of health* and typically assesses the health in a continuous or 'online' fashion

- **Anomaly detection** monitors key operating variables or metrics to identify deviations from their expected behaviour. An *anomaly* refers to a metric that deviates significantly from its usual pattern, such as an unexpected temperature surge or voltage spike. In this context, the term *signal* represents these significant deviations or anomalies that warrant attention. In contrast, *noise* refers to the usual fluctuations or variations that are considered normal

and don't indicate any problem. By distinguishing between signal and noise, anomaly detection serves as the first line of defence, promptly alerting operators to unexpected changes in normal operating conditions.

Modern anomaly detection systems will identify such anomalies, associate metadata or parameters related to the occurrence, and classify anomalies based on their potential to cause harm. Often, a representation or model or expected or standard behaviour is used to determine a machine's normal operating process and expected healthy state. Often, anomalies can be caused by intermittent events of faults, which do not imply impending failure. Therefore, the categorisation and classification of anomalies are vital. The category enables system users to act on events causal to failure modes.

- **Fault diagnosis** builds on anomaly detection advances and builds upon anomaly detection as it identifies the underlying cause of the underlying anomaly. The fault diagnosis process often includes important operating parameters or features to classify the anomaly as a fault with associated severity.

  Traditional fault diagnosis models use historical data models representing the fault conditions. These fault conditions and historical data provide an apriori representation of historical information, used to create models that can characterise new data with a set of historical data.

- **PHM** algorithms predict the *Remaining Useful Life* ***(RUL)*** of machinery or components or industrial equipment before a failure results in machine or production downtime. PM-based approaches rely on the RUL value as the parameter to plan maintenance activities not every day in CBM-type

activities. Therefore, the critical enablers of PM strategies are algorithms capable of efficiently forecasting the future state of a machine, i.e., providing prognostic information about its RUL, illustrated in Figure 2.7.

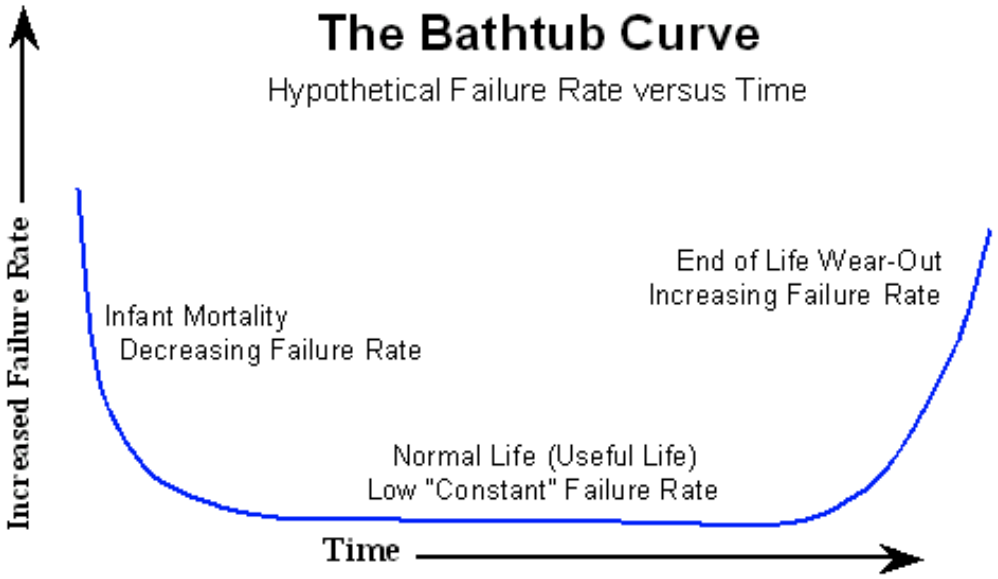


Figure **(2.7)** –Reliability Bath Tube Curve of equipment

- **Prognostics** or fault prognosis are techniques used to determine a prediction of RUL as accurately as possible. The RUL process will first select a timestamp for identifying a fault [126]. The objective of the prognostics is to determine how long a machine can operate and the rate of degradation with the fault being present [127].

  Diagnosis is not necessarily time-bound in delivering results; however, the prognosis is very time-dependent. The fault identification and timestamp of the anticipated failure are crucial determinants of how long a component or machine can operate. The models used for RUL are typically stochastic,

meaning they are always approximate. Based on age or state-dependent models [128]. Most data collected from equipment and devices, by their environments and locations, is susceptible to various noise sources. This noise can significantly alter the RUL predictions and is particularly problematic [129]. We can see the evolution of PHM from manual, human-led diagnosis to self-adaptive health management, which is evident in manufacturing environments that are becoming increasingly complex and autonomous [130].

2.4 Digital Twins

A Digital Twin is a digital or virtual representation of a real-world entity continuously updated to provide a digital, virtual replica of the entity in question. A Digital Twin offers insight into the entity's state throughout its lifecycle. An entity can be a physical object or a virtual entity, such as a process. A vital aspect of the digital twin is that the state of the physical and digital objects are synchronised by automatic data exchange. A Digital Twin can be discrete, representing a physical or abstract object or a composite comprising an assembly of multiple twins into a group [131, 132].

Digital Twins reside in a virtual computing environment. They are often rendered to consumers by visually representing the entity, sometimes as a 3D model of the entity, but this is not always the case [133]. It is essential to distinguish a digital twin from a 3D model of an entity. A digital twin integrates data about the entity into a unified digital representation of its physical form. Digital Twins can be combined to represent various business and manufacturing processes. They can

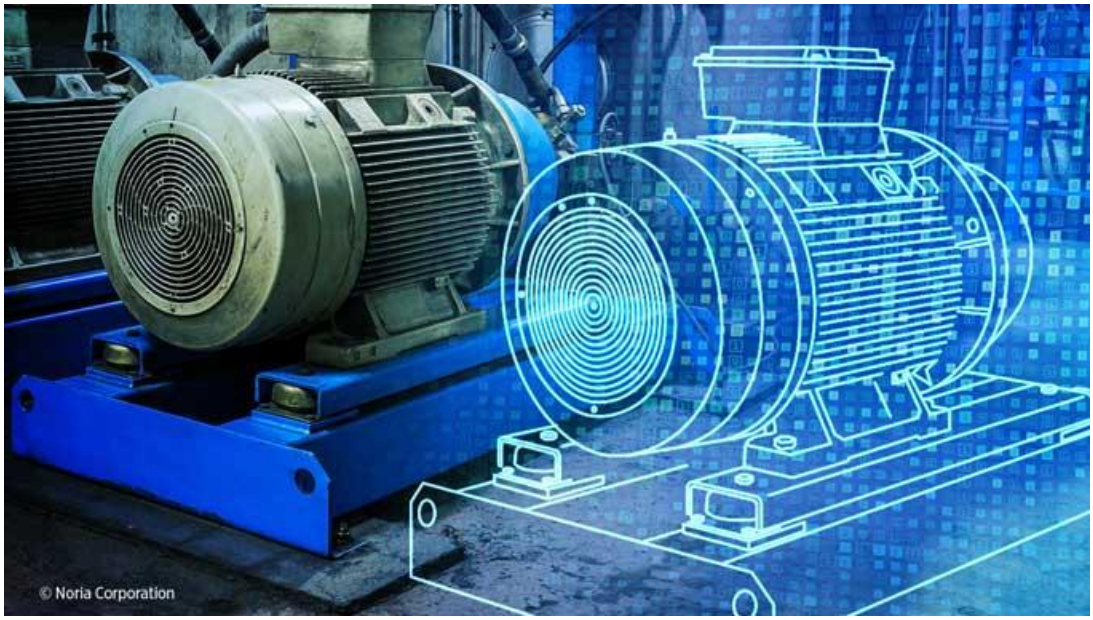


Figure **(2.8)** –Conceptual representation of 3d model beside a physical object, source; Nokia

mean anything we perceive in the world, physical or abstract, as outlined by the authors in [134].

The origins of Digital Twins can be traced back to NASA as a means to monitor, assess, and simulate conditions on space missions. Michael Grieves is also credited with the more modern definition of the term, commonly understood today [135].

Early proponents and adopters of Digital Twin technology were primarily manufacturers of high-value assets such as aerospace, automotive, wind-turbine, and other expensive capital assets [136, 137, 138].

The interest and application of digital twins have grown significantly in recent years. The American Society of Mechanical Engineers has outlined that Digital Twin technologies and applications are expected to grow significantly over the coming years, with DT technology being commonplace across the industry by

2028 [135]. Digital Twin technologies represent the convergence of multiple technologies, none more so than the IoT [139, 140]. Enabling technologies such as machine learning, simulation, and visualisation have grown the potential uses and applications beyond traditional high-value assets. Many companies want to leverage DT technology to provide a real-time view of their operations [141].

Digital Twin technology applications reach beyond manufacturing. For example, in the smart city domain, they are being used to provide insight and modelling for city planners and managers [142, 143]. There has been increased interest in applying Digital Twins in Healthcare [144, 145]. Applications of digital twins in health care include cardiovascular monitoring, elder care and cancer. However, digital twins significantly impact manufacturing and industry [146].

As previously discussed, industry 4.0 is the horizontal integration of multiple systems across the manufacturing ecosystem. It also encompasses the vertical integration of systems inside the enterprise leveraging general-purpose computing. Integrating and flowing data from various systems into one is crucial to future smart manufacturing. Qi discusses how Big Data enables digital twins[147]. Kitzinger et al. emphasises that the Digital Twin goes beyond data collection and can be used to control or change the state of a physical object [148].

Digital Twins use big data for analysis and dynamic control of physical and digital entities [149]. Digital Twin technology combines data collected from real-world entities into a data-driven model [150]. Integrating physics-based systems design and engineering with data-driven models opens up many new opportunities for performance, operation, and optimisation improvements from products to processes [151]. Digital Twin provides a means to integrate heterogeneous systems

horizontally across the product lifecycle. Combining data from multiple digital twins and linking them is known as the Digital Thread [152]. This digitalisation of products and processes points to a fundamental transformation of how products are made and managed [153].

2.4.1 Digital Twin operation

In figure 2.9, we provide an outline design of a typical digital twin system. A physical asset *depicted in grey* and digital asset *depicted in blue* are connected via a communications medium. In our illustration, data from sensors and data feeds from connected machines are sent from the physical asset to the digital asset, allowing the digital asset to mirror the physical system. In almost all instances of a Digital Twin, data flows from the physical asset to the digital asset. In some instances, data can also flow from the digital asset to the physical asset, often in the form of control data, instructing the physical asset to take some action. This bi-directionality of data flow is not mandatory and would depend on high reliability and low latency connectivity between physical and digital assets.

The digital asset will typically visualise the physical model, giving context to the system. There are multiple approaches to visualise the data, including the aforementioned 3D models. A Digital Twin uses analytics to monitor and take action on data collected from physical devices.

For example, complex event processing engines and predictive analytics enable alerts and steps to take on digital spatial data [154]. In cases where the remote control is possible, control can be closed-loop. As stated, in cases where this is impossible, alerts or actions can be sent to a human in the loop. Another key

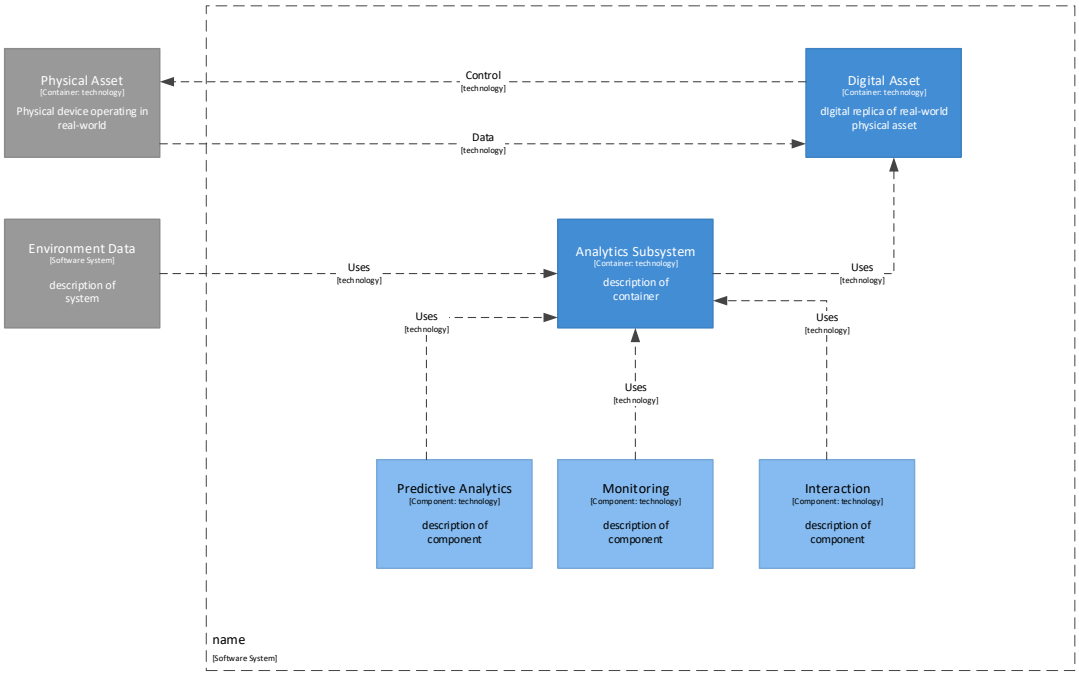


Figure **(2.9)** –Digital Twin system overview

feature of the Digital Twin is the ability to model the behaviour of the physical asset under a range of different scenarios [155]. Simulating a physical asset in the digital space enables operators to evaluate different modes of operation and predict failure or optimise the physical entity [156].

A Digital Twin continuously gathers information from its environment and updates itself to provide a real-time digital replica of its physical twin. Continuous monitoring involves collecting and networking vast volumes of data that must be acquired, analysed, and acted upon in real-time [157]. Digital Twin synthesises diverse data into single, coherent, high-fidelity dynamic models, updated in real-time. Digital Twin can be used for many applications to achieve various business objectives. A digital twin can simulate changes or events of the object in the virtual realm, enabling testing and evaluations to occur without interacting directly with

the thing [158]. Being in the digital sphere means having multiple types of digital twins of the same object [159]. One could be foe PHM based activities [160]. Another could be to try out potential configuration settings. These computer models of the physical objects could run thousands of tests simultaneously, enabling billions of scenarios to be tested at once. For example, it can be used in digital design to optimise the creation of a product [161].

Digital Twin technologies are critical in future manufacturing environments [162]. In manufacturing environments, physical and digital processes are deeply entwined through OT networks, leveraging sensors and actuators to gather from and control the production environment, which can continually adapt to its environment by leveraging data collected from the environment and its associated machines [163, 147].

2.4.1.1 Digital Twin Types and Applications

According to the UK Catapult Centre for Advanced Manufacturing, there are three main types of Digital Twin [164]. Trauer et al. also present a similar approach and provide a convenient method of describing the different types of digital twin and their uses [133]. Siemens also represents three main types of digital twins; although their description varies, they are broadly aligned [165]. IBM takes a different approach and describes the digital twin as a series of aggregations from the asset to process level [166]. However, it is generally agreed there are different types and uses of digital twins, which we will discuss presently.

- **Type 1 Supervisory**: In this type the DT model is fed data from the physical entity. It is used to monitor the state of the entity in question. This

type of twin is used to record observations and feed alerts or alarms. It can also be used as an engineering or planning tool for future states of the entity. A supervisory twin does not act on or control the twin it monitors. It is used as a tool to capture data and provide actionable insights to users. Chen demonstrates using such a digital twin for Wind Turbine operation [167]. Digital Twins are also used for condition-based monitoring and predictive maintenance support tools [168, 169]. Digital Twins also enable new forms of digital product design, integrating disparate data sources into a single unified model of an entity.. [161]. Type 1 DTs are used to provide actionable insights and enable humans to make informed decisions making. [170, 171]

- **Type 2 Interactive**: Type 2 Digital Twin provides the features of type 1 and has a degree of control over the physical twin. This type of twin can control actuators, settings, and set points of parts of the system, which are remote-control enabled. For example, this could include equipment such as motor controllers or valves. A type 2 Digital Twin shares similarities with SCADA Systems we discussed earlier. For example, Herlyn outlines using digital control twins to control an entire manufacturing process [172]. However, the breadth and scope of Digital Twin applications are more significant and extensible. SCADA systems are hierarchical, and their functionality is typically relatively fixed, whereas Digital Twin supports extensibility and enables multiple systems to be integrated to provide new functionality. Digital Twin technologies are being explored to provide robotic control of manufacturing systems [173]. Type 2 Digital Twins also model and control dynamic interactions between the physical and digital worlds [174]. Malik

outlines how interactive digital twins support human-robot collaboration [175]. Cimino illustrates the use of type 2 Digital Twin technology to integrate factory automation systems and automation infrastructure [163].

- **Type 3 Predictive** : Another influential application of Digital Twin technology is to verify and validate the performance of existing and future entities or products. Digital twins can validate the performance of products, processes, and complex systems. The digital and physical interplay allows powerful integration of physics-based models with data-driven models and simulations, enabling advanced new approaches to model and simulation complex systems [176]. Predictive Digital Twins can be used for PhM activities to improve the accuracy of complex equipment repair strategies [177]. This enables excellent productivity saving through responding to demand signals rather than waiting for failure-triggered signals or being driven by scheduled maintenance [178]. The notion of a *"product digital twin"* or *digital thread* also is concerned with understanding how products are used in the physical world. A Digital Twin provides a virtual-physical connection that lets users analyse a product's performance under various conditions. Product adjustments can be evaluated in the virtual world to test and validate the product, thereby reducing the cost and risk associated with product upgrades. Such tools also improve the quality of products as extensive testing takes place in the virtual or digital realm [179]. Aivaliotis demonstrates the use of Digital Twin technology to predict the residual useful life of a robotic system in advanced manufacturing [180] *Computational Design* describes the use of computational technologies in

the design and development process for a range of products [181]. Digital Twin technology is playing an increasingly important role in creation and production engineering. Doka et al. l illustrate how Digital Twin technology is used to design electrical drivetrains for electric vehicles [182]. Digital Twin technology is used to create and optimise industrial processes and production systems [183, 184, 185]. Digital TwinTechnology also enables the increasing product customisation and personalisation trend [186, 187]. Digital Twin technologies enable rapid prototyping and shortening of the product development lifecycle [188]. The ability to model design and prototype evolutionary evaluations of a product through simulation is outlined by Lin [189]. Li presents the use of Digital Twin technology for complex product design manufacturing and demonstrates its efficacy in improving the design lifecycle. Digital Twin can enable evolutionary evaluations of a product through simulation, enabling multiple designs to be evaluated significantly faster than conventional methods. [189].

2.5 Conclusion

In this chapter, we investigate the digital transformation of industry and its profound impact on manufacturing. While this transformation has been a research focal point for years, many technologies are only now gaining significant traction. As William Gibson aptly said, "the future is already here; it's just not evenly distributed."

Central to this digital shift is the IIoT, which emphasises machine connectivity and novel ways of linking devices, equipment, and systems. This evolution is reshaping numerous industrial sectors.

Historically, available technologies and frameworks like ISA-95 dictated industrial control and automation. Yet, emerging paradigms like edge computing are introducing innovative machine interactions and supporting modern manufacturing methods.

Enhanced connectivity, advanced analytics, machine learning, and AI revolutionise industrial maintenance. Prognostics and Health Management (PHM) techniques are improving, optimising asset utility and manufacturing uptime.

The surge in telemetry from connected equipment is fast-tracking the adoption of digital twins, marking a monumental shift in product design and manufacturing. This convergence of Industry 4.0, machine learning, and advanced connectivity allows for intricate simultaneous simulations of physical entities, redefining the interaction between physical and cyber systems.

However, the potential of these technologies hinges on reliable, efficient, high-bandwidth connectivity. The demands of these applications necessitate robust network support. Subsequent chapters will explore the current state of industrial wireless networks and the innovations required to drive the industry's digital transformation.

Chapter 3

Wireless Industrial Networks

This chapter discusses wireless industrial networks and state-of-the-art communication technologies commonly used. The chapter contains the main contributions:

- We assess wireless communication technologies in the industry, including IEEE-based standards, and cellular systems. We conduct a detailed evaluation of these technologies .
- Our review assesses the potential of 5G and private networks for industrial applications. We highlight ultra-reliable low-latency communication (URLLC) and massive machine-type communication (mMTC). our analysis explores the intricacies of Wi-Fi 6 technology and its relevance in industrial applications.
- Our analysis delves into the intricacies of IEEE 802.11ax/Wi-Fi 6E technology and the critical technologies most relevant for industrial applications.

We present a compelling argument for the relevance of Wi-Fi 6E in industrial applications.

3.1 Wireless Industrial Networks

Wireless industrial networks, WINs, are a class of communications networks designed for use in industrial environments [190]. WINs support machine-to-machine (M2M) communications, enabling industrial equipment to share data [191]. According to the UK's OFCOM, M2M data requires a high quality of service and narrowband, frequent data, supporting multiple connections and data [192].

In industrial settings, wired technologies like Fieldbus and Ethernet-based systems are widely used [193]. Fieldbus technology has been around for a while and is commonly used to connect field devices like sensors, actuators, switches, motors, and drives to controllers such as PLCs [194, 195]. Fieldbus technology transmits data serially and is still popular today, with technologies like PROFIBUS, Control Area Network (CAN), Modbus, and DeviceNet widely used. [196, 197, 198, 199]

Ethernet-based technologies like PROFINET, EtherCAT, Modbus TCP, EtherNet/IP, SERCOS, and POWERLINK have become more popular than Fieldbus technology [200, 201, 202, 203, 204, 205]. Ethernet-based systems have several advantages over Fieldbus technology [206], including low latency, flexible network management, and configuration [207]. Ethernet also supports high data rates of up to 1Gbps, with 100Mbps being the most popular [208], while Fieldbus technologies typically have lower data rates between 125kbps and 500Kbps [209].

Furthermore, it is easier to integrate Ethernet-based technologies into corporate networks, making them easier to manage and operate [62]. Both wired technologies are still widely used across industries and are known for their reliability and performance [210].

Why is the industry interested in wireless networks despite the advantages of wired networks in terms of performance, reliability, and stability? One reason is that wireless networks are much more cost-effective to install and maintain than their wired counterparts, allowing for greater flexibility in adapting or reconfiguring cyber-physical processes. Wireless communications have become necessary with the increasing use of Automated Guided Vehicles (AGV) and robotics. Wireless technologies also make it easier to connect and integrate new sensing systems, such as worker safety and mobile inspection systems. Finally, wireless technology is a critical enabler of transforming industrial spaces to support dynamic, adaptive, and reconfigurable manufacturing, a fundamental principle of Industry 4.0. Therefore, the value of wireless technology is far-reaching and essential for the future transformation of the industry.

To enable pervasive wireless communications in industrial environments, networks need to provide capabilities like wired systems. However, wireless technology adoption is not as widespread because of the perception as less reliable, robust, and performant than wired systems [211].

In particular, wireless systems must address the stringent timing challenges expected in manufacturing environments. Wireless technologies must be able to meet cycle-time performance in the region of $<25\,\mu s$ to meet control applications such as robotics systems. The manufacturing and process environment can be

dynamic, especially in assembly or production environments with metalworking activities, such as car assembly plants [212]. Ultra-high reliability is also critical, with error rates expected to be less than 10^{-8} packet error rates. Achieving such low latency and high reliability in challenging environments is problematic [213]. The performance requirements of the above systems can vary given the type of manufacturing process and the domain or application in which it is operated [214]. As previously discussed, new applications such as digital twin technologies demand increasing data rates and low latency, high-reliability networks. [215, 216]

Today, a range of wireless technologies are already in use across many industrial applications. Technologies in the industrial, scientific, and medical (ISM) bands and those based on IEEE standards are popular. They include IEEE 802.11 and IEEE 802.15.X based wireless systems [217, 218]. Licenced technologies have been used for many years across multiple application areas [219, 220]. Low-power Wide Area (LPWA) technologies have also become popular, providing wide-area coverage for low-power devices; however, they are suitable for low-data (<250kb/s) and higher latency applications(1sec). LPWA technologies include LoRaWan, NB-IoT, and Sigfox [221]. Other fringe systems have evolved to meet more extreme applications, including leaky feeders, backscatter, and optical communications [222, 223, 224].

Several methods have been investigated to enhance the performance of WINs. Customised physical layer technologies have been proposed to tackle the challenges of low latency and higher data rates. For instance, Luvisotto et al. designed a custom-made IEEE802.11 PHY layer that achieves 1μs performance for low data rates. However, the authors acknowledged that it did not meet the reliability

requirements needed for critical applications [225]. Innovations in the MAC layer include using 6TiSCH, which leverages the IEEE802.15.4 standard [226, 227]. Additionally, the network layer approaches has improved performance. For example, ABB presented a network based on a time synchronisation protocol that provides less than 10μs performance of a multihop network [228]. The advent of 5G-based technologies, specifically 5G URLLC, has been designed to meet the demands of manufacturing and industrial operators, particularly for critical use cases [229].

3.2 Performance considerations for industrial wireless networks

We leverage three authoritative sources that comprehensively cover performance requirements for industrial wireless networks. These sources serve as foundational references for our work.

Category	Class	Application Type
Safety	0	Emergency Action
Control	1	Closed Loop Regulatory Control
Control	2	Closed Loop Supervisory Control
Control	3	Open Loop Control
Monitoring	4	Alerting
Monitoring	5	Logging and downloading/uploading

Table **(3.1)** –ISA categories, classes and application types

One of these sources is the ISA standard, specifically the *ISA TR100.00.03-2011 (Wireless Use Requirements For Factory Automation).* It outlines the requirements for using wireless systems in various industries and application domains [230]. The ISA standard categorises the usage of six classes, ranging from 0 to 6, with 0 being the most critical and 6 being the least stringent. This classification system applies to most industrial applications and is detailed in Table 3.1. The more stringent requirements apply to class 0 applications, while classes 4 and 5 have less strict requirements. Although maintenance activities typically fall under class 4 or 5, emerging PHM applications are better suited for class 3 or even class 2.

the National Institute of Standards and Technology (NIST) has improved the ISA's application classification system by providing additional context and perspective to the safety and condition monitoring categories ranging from class 0 to class 4. Additionally, NIST has analysed the wireless needs for each usage class, and highlighting the importance of a well-configured factory cell. [231].

The European Telecommunications Standards Institute (ETSI) thoroughly investigated the wireless needs of industrial applications. The paper highlights industrial applications like monitoring and diagnostics, discreet manufacturing, and functional safety. While ETSI does mention specific applications such as discreet manufacturing, logistics, and monitoring, it provides examples like motion control, AGV usage, and condition monitoring. The performance criteria of these applications are mostly similar to the aforementioned application performance criteria outlined by NIST. [232].

When implementing industrial wireless systems, Candell has researched the challenges involved [58]. In a previous discussion, we explored helpful performance

metrics for critical control applications presented by Luvisotto et al. [225]. Thornhill has also highlighted the difficulties of using wireless technology in harsh industrial environments and emphasised the importance of such systems supporting diverse network traffic [233]. Despite opposing views on using wireless technology for mission-critical industrial applications, the advancements in wireless technologies have improved their performance, thereby overcoming traditional barriers [234, 235]. The progress rate in wireless technology performance is promising for wireless industrial networks.

3.2.1 Harsh RF Environment

Industrial environments are often harsh and hazardous, resulting in electromagnetic interference (EMI) and radio frequency interference (RFI). These interferences can generate unwanted signals that interfere with the wireless indutrial network, causing issues [236]. Additionally, noise from other communication systems and local deployments can significantly impact wireless communications, leading to increased interference in the area [237, 238]. Wireless devices are susceptible to interference and contention from nearby devices. Compared to wired counterparts, wireless communication networks have limitations, particularly regarding reliability and latency, which can be negatively affected by the harsh radio propagation environment commonly found in factory environments. Manufacturing facilities typically consist of metallic and absorbing entities that reflect or absorb electromagnetic waves [239]. While shielding, grounding, and other techniques can help mitigate these issues, they are only practical in some cases.

Manufacturing locations can be challenging due to their complexity and constant change. These highly dynamic environments have continuously evolving electromagnetic settings [240]. Mobile equipment such as forklifts and cranes are also standard in these locations [241, 242]. As the use of AGVS and robotics grows, the complexity of industrial environments will likely increase over time [19, 243]. Unlike offices or other settings, industrial environments are prone to shadowing, attenuation, multipath, and scattering impairments [244]. These impairments can reduce the data rate and reliability, leading to network performance degradation [245].

In industrial environments, a variety of equipment is necessary for manufacturing operations. Some examples of this equipment include compressors, investors, variable-frequency motor drive units, and more [246]. This equipment is housed in enclosures, conduits, busbars, or racks, and it may generate noise due to electrostatic discharge, voltage spikes, or high-frequency electrical switching [247]. Additionally, this equipment is often installed near or on metallic objects, and improper grounding can cause interference with wireless communication [248].

3.3 Leading industrial wireless technologies

3.3.1 IEEE 802.15.X based systems

The Institute of Electrical and Electronics Engineers (IEEE) 802.15 family of standards covers wireless personal area networks (WPANs.) [249]. The standard covers Bluetooth technology *(IEEE 802.15.1)* as well as ultra-wideband (UWB)

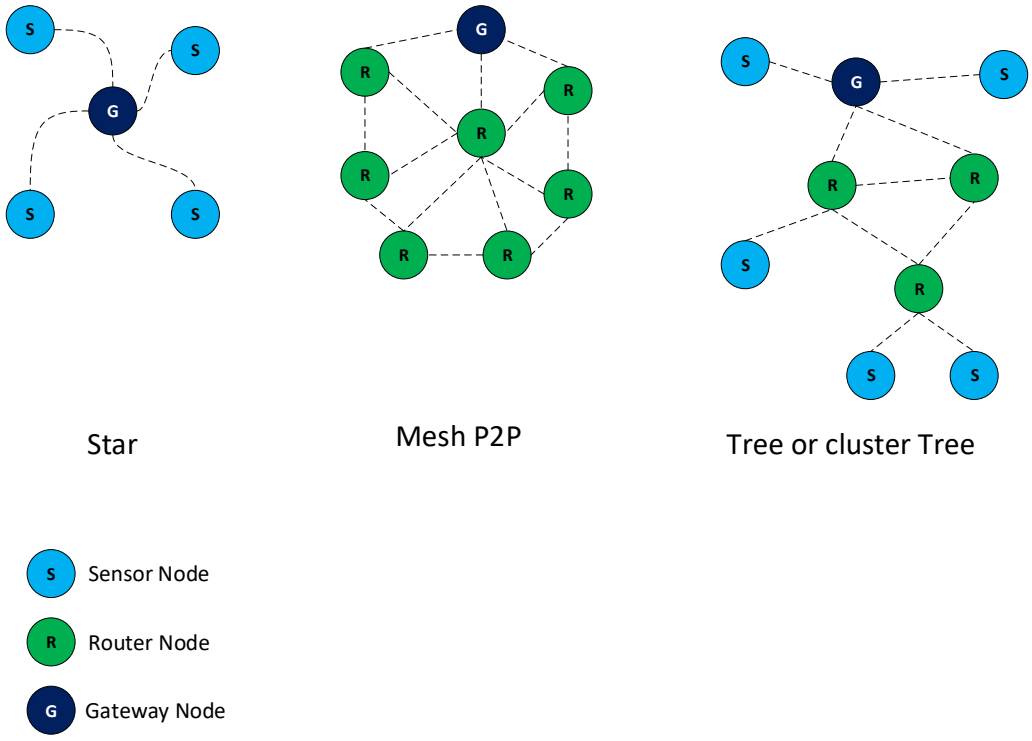


Figure **(3.1)** –802.15.4 network topologies

technologies *(IEEE 802.15.3)*. The standard also includes *802.15.6*, which covers body area networks (BAN).

IEEE 802.15.4 incorporates wireless personal area networks and covers short-distance networks to connect an individual to multiple personal devices. The name WPAN needs to be more accurate, as many of the applications of the standard extend way beyond the WPAN definition. The standard targets low data rate devices, typically operating on a battery for extended life and low-power applications. This standard has become very popular, with various variants supporting different application types. For example, *802.15.4g* supports utility networks and smart-grid applications [250].

The IEEE 802.15 family based networks are the amoung the most deployed industrial-based wireless technologies deployed. [251]. The standard can support different network topologies, such as those illustrated in Figure 3.1.

- **High-rate (HR-WPAN)** is defined in the IEEE 802.15.3 standard. Data rate is $>$ 20 Mbps [252].
- **Medium-rate (MR-WPAN)**: Defined in the IEEE 802.15.1 standard. Data rate is 1 Mbps [253].
- **Low-rate (LR-WPAN)**: It is defined in the IEEE 802.15.4 standard. Data rate is $<$ 0.25 Mbps [254].

The 802.15.4 standard establishes the physical *(PHY)* and medium access control *(MAC)* layers as a base standard and format for other protocols and applications. One such technology is Zigbee, managed by the Connectivity Standards Alliance and widely used in industries like buildings and home applications. Although used in industrial applications, it is less popular than other IEEE technologies [255].

3.3.1.1 WirelessHART

Wireless Hart is an industry-specific wireless communications standard that is interoperable and open. First released by the HART Foundation in 2007 and has since been widely adopted in process automation applications, proving to be successful [256]. WirelessHART operates using the IEEE 802.15.4 standard and operates on the 2.4GHz frequency band. It uses a mesh networking topology, with each device on the network containing routing information that allows for data transmission.

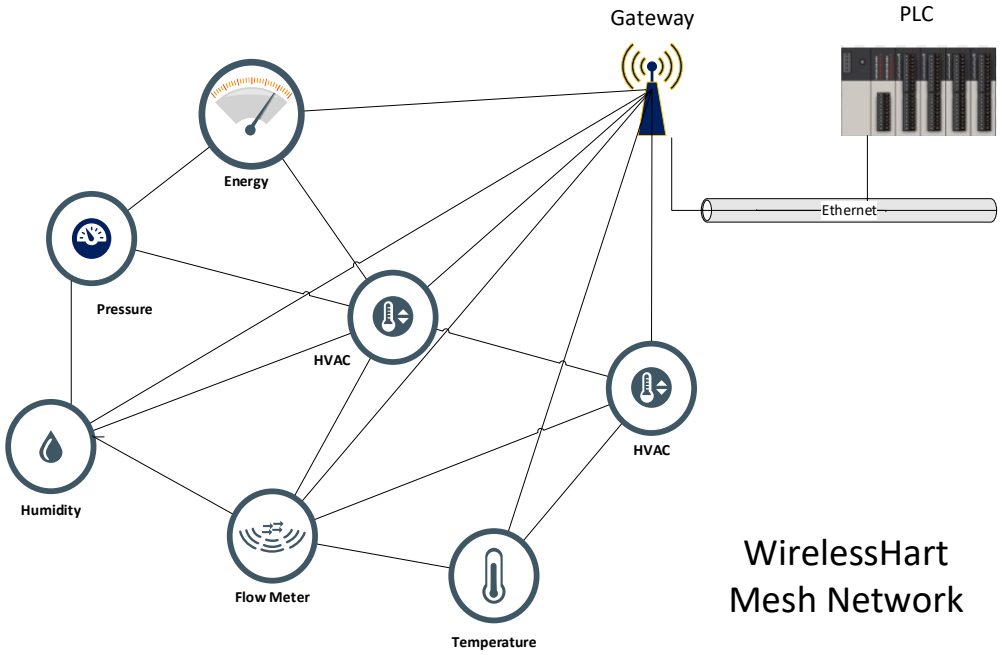


Figure **(3.2)** –WirelessHart network topology

WirelessHART utilises modulation schemes such as Direct Sequence Spread Spectrum (DSSS) and Offset-Quadrature Phase Shift Keying (OQPSK). It supports data rates of 250Kbits/s and communicates over 15 channels (11 to 25). To avoid non-overlapping transmissions, it leverages 3MHz channels, separated by a 5Mhz gap between channels. WirelessHART uses the packet format of the IEEE802.15.4 standard at the PHY layer, which contains the data structures from the higher protocol layers. WirelessHART networks can achieve reliability between 99.73% and up to 99.999%.

The Network Manager is a crucial component of a WirelessHART network, overseeing its operations and ensuring seamless communication between devices. This

functionality includes managing timeslots and frequency hopping schedules, authenticating devices, and regulating transmit power to conserve battery life. The Network Manager also assigns time slots for device communication, updates the mesh to establish alternative communication routes, and continuously adjusts transmit power to meet performance goals. The Network Manager guarantees reliable and low-latency communication with its adaptive network management techniques in dynamic industrial environments. WirelessHART supports a range of up to 100 metres and various update rates to suit diverse application needs.

WirelessHART uses a communication method called Time Division Multiple Access (TDMA), which involves fixed timeslots for device communication. These timeslots make up a superframe and persist throughout the network's lifetime. The system supports 100 timeslots per second (10ms). To manage contention, each timeslot is assigned a specific source and destination. WirelessHART also utilises channel hopping by alternating between 15 channels to avoid collisions and ensure deterministic communications. Additionally, it uses direct sequence spread spectrum (DSSS) and reliable channel frequency hopping, time division multiple access (TDMA) synchronisations, and delay-controlled communication to provide a high level of reliability, low power consumption, and affordability for industrial wireless communication [239].

WirelessHART is backward compatible with Wired HART field devices under the IEC 62591 standard. WirelessHART supports integration with legacy equipment and machines using dongles or adapters.

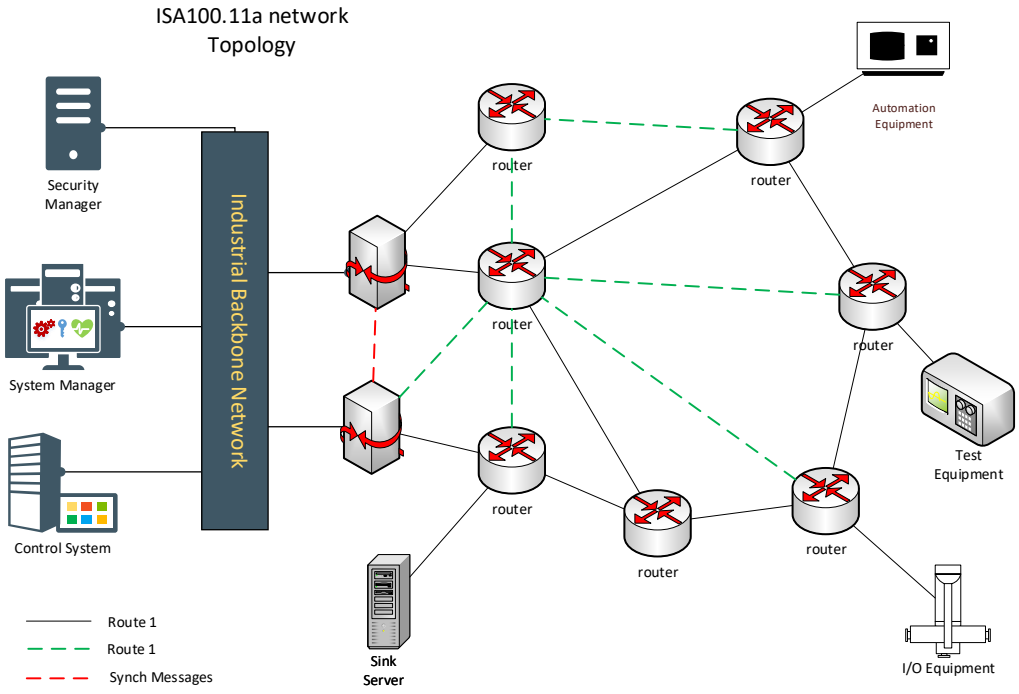


Figure **(3.3)** –Typical ISA10001a network

3.3.1.2 ISA100.11a

The International Society of Automation (ISA) worked on creating a standard for industrial wireless networks while WirelessHART was being developed. The ISA100.11a standard was ratified in 2009 [257], while the International Electrotechnical Commission (IEC) approved it as an international standard in late 2014 under the name *IEC 62734*. This standard by ISA supports various wireless industrial applications like process control and automation-type applications. It defines the protocol stack, system management, and security functions.

The ISA100.11a protocol utilises internet protocols like IPv6 and UDP and the 6LoWPAN routing protocol from Internet Engineering Task Force (IETF) set of

open standards for the Internet. It operates on the 2.4 GHz frequency range and employs network bridging and subnets, which can support large-scale deployments. Since it uses IPv6, there is no limit to its scalability. ISA100.11a networks consist of field and backbone devices, including non-routing I/O devices, handheld devices, and various automation equipment. These devices can be stationary, portable, or mobile. The network also comprises routers, gateways, a System Manager, and a Security Manager. The gateway connects to plant networks, and the typical network configurations include mesh, star-mesh, and star topologies, as shown in the Figure 3.3.

Various features have been implemented in ISA100 to achieve high performance and reliability. One notable feature is the synchronisation of timing using the international atomic time (TAI) in ISA100.11a networks, which ensures that all devices on the network remain in sync.

ISA100.11a networks are fully deterministic and use TDMA with configurable time slots ranging from 1ms to 500ms. Short, predictable traffic patterns such as M2M traffic are suitable for the maximum transmission time of 4ms. Longer time slots are available for larger payloads and traffic types, and the CSMA-CD protocol combines timeslot management and dyanmic slot allocation. Collision avoidance is supported by the clear channel assessment techniques from IEEE 802.15.4 protocol, which underpins CSMA-CD in ISA100.11.[258].

To improve reliability and reduce interference, ISA100.11 utilises frequency diversity techniques. It follows the IEEE 802.15.4 standards in the 2.4GHz range and has 16 channels. Devices communicate by hopping channels sequentially, increasing the likelihood of successful transmission. ISA100.11 implements ARQ

(Automatic Repeat Request) to ensure unacknowledged packet retransmission over a different channel and frequency.

ISA100.11 uses spectrum management techniques to ensure a reliable network by reducing interference with wireless systems that share the same frequency band. These techniques include channel deny listing and adaptive hopping, which monitor the spectrum's noise and proactively manage the network under changing conditions. Channel deny listing removes poorly performing channels from the hopping sequence. In contrast, adaptive hopping allows the network to make decisions locally based on data collected from the environment rather than relying on the central System Manager. This decentralised approach enables the network to adapt to local conditions [259].

Graph-based routing is used in ISA100.11a-based networks to support network reliability by creating path redundancy across the network. The System Manager configures the directed acyclic graph based on telemetry collected from field devices. The route information is continually updated and adapted based on prevailing conditions, although devices can also make adaptive routing decisions based on the local data. ISA100.11a network also uses Duocast, where a machine can simultaneously send a packet to multiple devices. This technique is more commonly used with field devices communicating directly with backbone routers, although it can be used deeper within the network. The use of Duocast exponentially increases the probability of successful transmission. The routing techniques in ISA100.11a networks are commonly known as self-form and self-healing networks, as they are continuously adapting and changing to the conditions of the network [260].

ISA100.11a adopts robust security mechanisms, including a two-layered architecture. It uses link-layer security for hop-to-hop encryption and authentication, where each router performs encryption-decryption and authentications. ISA100.11a employs encryption based on AES-128 block cyphers, leveraging symmetric keys. It also conducts transport layer authentication and encryption of data messages and session management between devices. The Security Manager system manages policy-based security in ISA100.11-based networks that provide timestamping.

Open Internet protocol standards are also a significant feature of ISA100.11. The network layer uses the 6LoWPAN, IPv6-compressed UDP packets [260]. The backbone router manages address translation, routing, and packet management. Moreover, the ISA100.11a standard allows large PDUs to support applications beyond M2M applications. Application PDUs of 1280 bytes is supported. This layer also covers all functionalities supported by the generic MAC layer.

ISA100.11a supports adaptive channel hopping, detection and recovery of message loss, clock sync, message addressing, local link addressing, message forwarding time, and integrity checking.

The differences between WirelessHart and ISA100.11a are apparent at the networking level. ISA100.11a leverages standardised or derivates internet-based technologies such as the IPv6 protocol and 6LoWPAN routing, supporting routing across the backbone, making the ISA100.11a networks inherently scalable, similar to the internet [261].

3.3.1.3 WIA PA & FA

The third and most recent specification for wireless communication for the process automation industry, WIA-PA and WIA-FA for factory automation is developed by the Chinese Industrial Wireless Alliance (CIWA). While predominately a Chinese standard, it has been accepted internationally. WIA uses the IEEE 802.15.4 specification of protocols. WIA-PA officially became IEC 62601 international standard in 2011.

WIA-FA technology is a set of wireless data transmission solutions for factory automation, specially developed for high real-time and high-reliability factory automation requirements. It is suitable for industrial wireless local area networks with high requirements for speed and reliability of factory automation to realise high-speed wireless data transmission.

As illustrated in Figure 3.4, WIA-PA networks have four device types. Device types include host, gateway, routers, and field devices. Field devices can be fixed or mobile devices. The host is responsible for system management, functionality, interfaces to system users, and interoperability with the industrial backbone network. Gateways enable interoperability and translation between the WIA-PA network and existing protocols, such as industrial Internet protocols. The gateway also provides network management functionality, including network management and security.

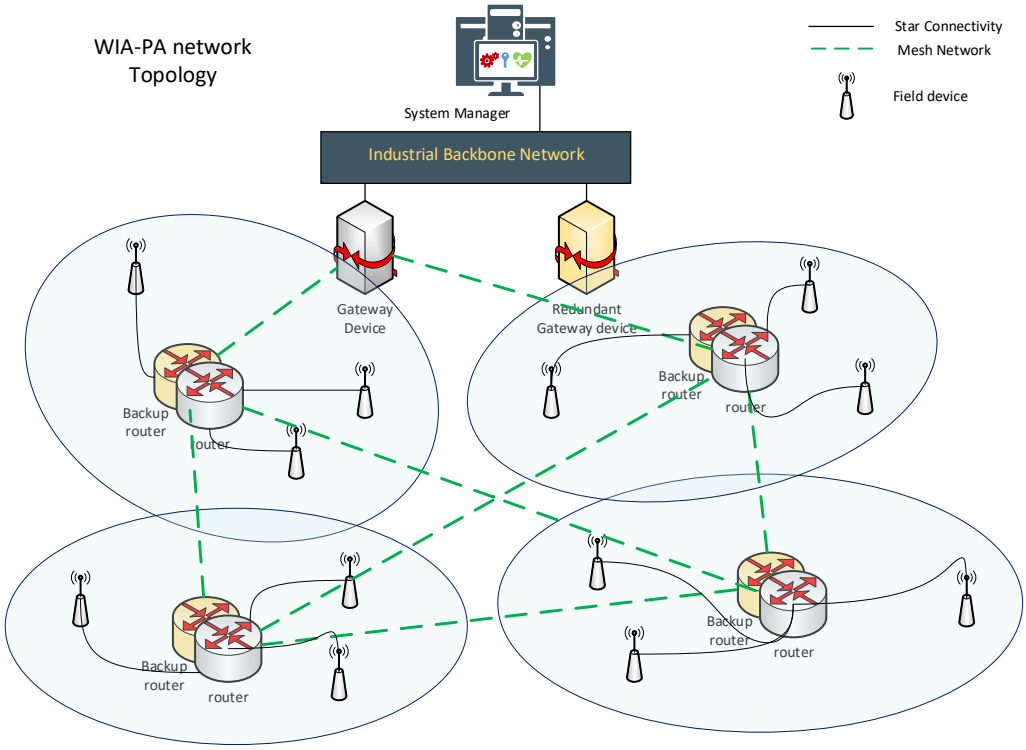


Figure **(3.4)** –Typical WIA-PA network

The purpose of routers in WIA-PA networks is to support network routing and enable communication between the network and field devices, such as sensors and actuators, which control and manage processes in a factory. WIA-PA networks use backup or redundant routers and gateways to enhance network reliability.

WIA-PA networks use IEEE802.15.4 PHY layer technology with 14 channels for data transmission. The superframe structure of the IEEE802.15.4 standard is used, consisting of active and inactive periods. Beaconing controls superframe transmissions between devices, while Contention Access Periods (CAP) and Contention-Free Periods (CFP) enable communication between mobile field devices and equipment. The idle period of the superframe enables inter-subnet

communication. The superframe has 32 timeslots of the overall network time base. Packet aggregation, known as superframes, reduces communication traffic and energy consumption but can cause latency due to the size of the superframe. Latency is crucial in industrial settings, though, more so than battery efficiency.

WIA-PA networks typically use a combination of mesh and star topologies. Mesh networking is used for communication between routers and gateways, while the star topology is used for communication between field devices and the router. This hybrid approach is known as cluster mesh or star mesh. WIA-PA also provides 128-bit AES encryption and centralised management of communication resources. The system manager assigns resources based on the overall needs of the network, defining time intervals and channels for machines to use. However, this approach is bespoke and can be problematic.

WIA-PA uses TDMA and adaptive frequency hopping (AFH) to improve network communication reliability, which is effective against external interference. However, local interference and node-to-node communication can be problematic due to the continuously changing internal interference. Additionally, nodes cannot determine whether the communication channel is clear, so they constantly scan the media for clear communication, which increases network traffic and power consumption.

3.3.2 Cellular based systems

Cellular-based technologies have been used in industrial settings in many guises for a long time. The 3rd Generation Partnership Project (3GPP) develops and manages this standard. Cellular technologies' performance, data rates, and usefulness increase with each new release of the standard [262]. Interest in cellular

networks has increased due to advances in 4G Advanced Pro, sometimes dubbed 4.9G, and currently 5G [263]. Significant innovations started with 4G LTE, improving coverage, data rate, and overall network performance [264].

The fifth-generation cellular standard 5G further develops and extends the technology innovations introduced in the 4G standard [265]. These peformance improvements incrase the dependability of cellular-based systems and, of significant interest to this work, heavily influenced the path of future Wi-Fi technologies. As 5G is the most recent standard, we focus on 5G technology.

Cellular networks comprise two main elements: radio access network, RAN and core network. RANs provide connectivity and access to individual devices to the core network at a fixed locations. RANs include masts, antenna arrays, and base station components, enabling connecting devices to the cellular network's location and core networks. Cellular networks have evolved from primarily voice-oriented to data-oriented networks [266]. Over their evolution the data carried by these networks has also developed from small packet networks (photos, email, etc.) to more extensive data packets (video, gaming, live streaming) [267]. As part of the 5G evolution, small cells play an essential role in 5G networks, particularly in industrial applications. Small cells are low-powered cellualr based radio access nodes that can cover smaller ranges and use less and are less costly to operate. [268, 269].

Low-latency and high-reliability over-the-air interfaces required new radio technologies to minimise time delays via the radio within a few TTIs (time transmit intervals). Additional enhancements, such as coding improvements, enable high reliability (e.g. one message is delayed or lost in every billion) [270].

Implementing virtual, dynamic, and configurable Radio Access Networks *RANs* used virtualisation and dynamic reconfiguration to enable to be highly configurble and support changing and dynamic network conditions. This functionality allows the mobile network to adjust to network traffic, faults, and dynamic changes to the network topology [271].

Small cells are miniaturised base stations that enable segmentation and network densification. Segmentation increases the small cell's capability to increase data capacity and speed. Different classes of cells used for other applications are illustrated in Table 3.2

Cell Type	**Cell Radius (m)**	**Users**	**Locations**
Macro Cell	8,000–30,000	>2,000	Outdoor
Micro Cell	200–2,000	100–2,000	Outdoor & Indoor
Pico Cell	100–200	30–100	Outdoor & Indoor
Femto Cell	10–100	<30	Indoor

Table **(3.2)** –Cellular base station types

The core network handles data, voice, and other telecom services. In 5G networks, the core network has evolved into a converged network responsible for voice, data and internet connectivity. One innovation in 5G is redesigning the network to support the distribution of the core network to improve the response time and consequently reduce latency [272].

Many of the advanced elements of 5G include network function virtualisation and the creation of logical networks onto the same physical network, known as

network slicing. This approach enables multiple virtual networks for applications and services on the same core network [273].

5G network design support such classes of emerging internet traffic, in particular, Massive Machine Type Communication *(mMTC)*, Enhanced Mobile Broadband *(eMBB)*, and Ultra-Reliable Low Latency Communications *(URLLC)* categories of traffic. Earlier cellular standards enabled the smartphone era and mass consumer cellular networks. 5G targets the needs of business and industrial applications [274].

There are three service categories of use for 5G [275]:

1. **Massive machine-to-machine communication (mMTC)** applications are commonly associated with IoT-type data. It addresses the connectivity of mass volumes of devices without human intervention at a scale not seen before. This functionality can revolutionise modern industrial processes and applications, including agriculture, manufacturing, and business communications. Connection density of up to 100 nodes per sq. meters is possible, making deployment of many devices in dense locations viable.

2. **Ultra-reliable low latency communications** are designed for mission-critical, real-time control applications like industrial control, robotics, vehicle-to-vehicle communications, and autonomous guided vehicles. uRLLC enables low latency and high-reliability applications that require one-millisecond user-plane latency. which is the lowest time taken for transferring a PDU across the physical layer. Reliability Packet Error Rate (PER) can be in the region of $10^{-}3$ and $10^{-}3$. This technology provides opportunities for a wide range of applications that require high levels of reliability and performance.

3. **Enhanced mobile broadband** provides significantly faster data speeds and greater capacity, with up to 10 Gbps data rates. The primary use of eMBB is improving wireless internet access for higher bandwidth applications; its value and benefit go beyond home use. Improvements in bandwidth and data rate also enable a wider variety of applications, such as AGV applications [19].

3GPP Technology	**Response Time (ms)**
LTE Systems (4G)	20
Enhanced Mobile Technology (5G)	4
Ultra-Reliable Low Latency Communications (5G)	1

Table **(3.3)** –Cellular response time evolution

3.3.3 The emergence of Private 5G networks

A crucial innovation of 5G networks is their use as private networks, which allows manufacturers and industrial users to own and manage their networks. Private 5G networks function as local area networks for the user and utilise cellular-based radio technology based on the 5G radio. In this evaluation, we focus on Non-Public Networks (NPNs) or private 5G networks, which are more comparable to the other wireless networks we discuss. [276].

A private 5G network includes a radio access network (RAN) integrated into a private network and consists of one or more base stations. These flexible base stations are expandable to provide additional coverage or capacity. The core part of the network is usually physically connected to the base station or through the existing network infrastructure.

Private 5G networks are customised for single or multiple industrial applications by segmenting the network to cater to different needs, such as closed-loop control or video streaming. [277]. Security will be of utmost importance in both current and upcoming networks. The security of 5G networks is based on the strong security foundation established by the widespread use of mobile networks, which has been built up o ver succesive releases of the 3GPP standards and is considered by most to be comprehensive [278].

Another critical feature of private 5G is the Guaranteed Quality-of-Service (QoS), which is crucial to industrial applications [279]. Another vital and emerging need is using and adopting mobile platforms such as mobile workstations, robotics, drones, and AGV [280]. 5G supports enhanced-mobility management for such applications [281, 282].

3.4 IEEE 802.11 & Wi-Fi

Wi-Fi technology's technical foundation is the IEEE 802.11 standard, an essential technology of recent years. Its influence is ubiquitous in all aspects of our daily lives.

Wi-Fi originated from the IEEE 802.11 standard group, which Vic Hayes spear-headed intending to reduce the expenses and intricacies of wiring cash registers during in the early 1990's [283]. Companies such as Apple, IBM, and Intel were attracted to the idea of wireless computer connections, which led to the popularity of Wi-Fi. As a result, the cost and availability of Wi-Fi technology increased rapidly.

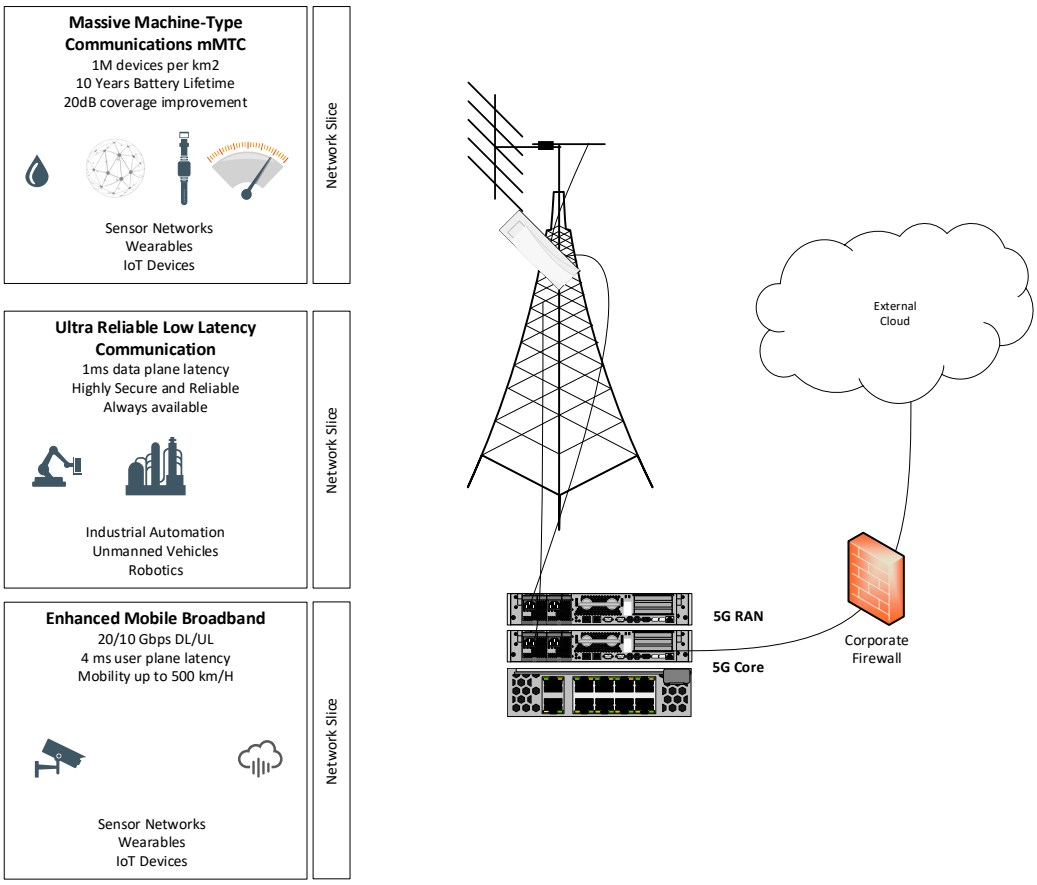


Figure **(3.5)** –A Private 5G network

Wi-Fi's widespread acceptance was mainly due to its utilisation of unlicensed spectrum, specifically the ISM bands. By leveraging this frequency range, Wi-Fi became easily scalable and affordable, making it a popular choice for implementation.

Wi-Fi has become a victim of its success. Its use of unlicensed spectrum has proven to be both beneficial and challenging. The shared-spectrum access and selection of medium are currently the biggest hurdles for Wi-Fi. The working group behind the 802.11 standards developed a simple MAC algorithm to simplify the implementation process. They chose the Channel Sensing Medium Access/-Collision Avoidance protocol, similar to the wired Ethernet standard's medium Access/Collision Detection (CSMA/CD) protocol. This decision made it easier for the technology community to adopt Wi-Fi.

Few people could foresee the overwhelming popularity of Wi-Fi and the explosion of use in the ISM bands. Many devices using the same frequency spectrum have resulted in significant congestion challenges [284]. Also, the ever-increasing use of data-intensive technologies such as video and streaming presents various challenges for Wi-Fi. Environments with a large volume of communicating devices exacerbate the problem. The network contention issues surrounding Wi-Fi drive the perception and reality that wireless technology, while convenient, can be unreliable in densely populated locations [285].

The popularity of Wi-Fi and its pervasive use across the shared spectrum of the ISM bands, particularly in the 2.4GHz band has resulted in a tragedy for the ISM commons [286]. The performance of Wi-Fi networks is highly dependent on the number of devices sharing the medium. Overall, Wi-Fi performance

highly depends on the network devices' interference. In a 2016 article from IEEE Spectrum magazine, the author outlines how Wi-Fi is a victim of its success and how congestion made the 2.4GHz unusable for specific applications [287].

Wi-Fi's popularity will grow significantly over the coming years. A 2020 report from Cisco Systems highlights that by 2023, there will be almost 15 billion M2M connections and M2M traffic will account for nearly 50 of all internet traffic in the same timeframe [288]. The report also illustrates the growing use and adoption of Wi-Fi over the coming years and the potential of Wi-Fi 6 for high-definition media. Additionally, the report highlights that the growth of Wi-Fi hotspots will increase by four holds. Supporting data from the UK regulator OFCOM highlights the need for additional spectrum to meet Wi-Fi demand [289]. Wi-Fi-based networks will remain a dominant means of data communications globally for the foreseeable future.

Over the last years, the IEEE High-Efficiency study group **Hew** has been actively working to improve the 802.11 standards, with apparent success. Their most recent release of the IEEE 802.11ax standard is a step-change improvement of Wi-Fi [290]. We contend that the progress within the middle allows Wi-Fi to penetrate the most challenging or operational use cases, such as those in industrial environments. The rate of performance improvement with the 802.11-based standards has been staggering. A 2021 article from Wi-Fi Now Journal illustrated the successive improvements and progress of data rates by approximately 1000 [291]. This trend closely approximates Moore's Law, which states CPU processing power doubles every two years.

Wi-Fi technology, which the IEEE Standards Association governs, has been a critical wireless technology over the last few years. It has enabled computing to be connected and untethered and has been a crucial catalyst in helping pervasive connectivity. Wi-Fi has become pervasive across IT applications; however, it has enjoyed a different success in operational OT applications. OT applications in industrial environments provide challenging environmental conditions for Wi-Fi operation. These conditions can include dust and dirt particles generated from machinery and extreme temperatures, shock, and vibration. Typically, the chipset technology deployed in harsh environments requires an extended operating range, static state cooling, and protection from moisture, dust, and other environmental challenges.

The future growth of Wi-Fi will be led not by human-to-human or human-to-to-machine communication but by machine-to-machine communications, M2M. M2M communications define devices communicating with each other without any human intervention. A 2020 report from Cisco Systems highlights that by 2023, there will be almost 15 billion M2M connections 2023. M2M traffic will account for nearly 50% of all internet traffic in the same timeframe [45]. It is worth noting that IoT and M2M are used interchangeably to describe the specific class or type of traffic.

3.4.1 A chronology of Wi-Fi

A brief chronology of the Wi-Fi standard helps highlight the evolution of the technology. Also, it illustrates how often technological advances build on each other

incrementally and consecutively on prior versions, while maintaining backwards compatibility.

- **IEEE 802.11a** is a wireless standard that uses the 5 GHz band providing a theoretical top data rate of 54 Mbps. It has a shorter range than 802.11b due to the higher frequency range.

  802.11a uses OFDM modulation consisting of 52 subcarriers, of which 48 channels carry data. It has a 20 MHz bandwidth, with an effective 16.6 MHz available when subtracting bandwidth used as guard bands between the channels.

  However, 802.11a systems had some challenges. Hardware costs were higher than IEEE 802.11b-based systems. The price of hardware using 2.4 GHz was lower due to the commoditization of 2.4 GHz-based technologies. The 5 GHz spectrum was only sometimes available as a global standard, which limited its use.

- **802.11b** Shortly after the release of IEEE 802.11a followed IEEE 802.11b. IEEE 802.11b was the first Wi-Fi standard adopted as a global standard. It uses the 2.4 GHz frequency band and has some advantages over its predecessor, notably cheaper and easier to develop [292]. Also, at that time, Wi-Fi technology was being integrated into laptop computers, providing momentum to the technology's adoption. In July 1999, the technology became a standard, and its proliferation took off. IEEE 802.11b had lower data rates than IEEE 802.11a but had improved performance and range. IEEE 802.11b used DSSS *(Direct Sequence Spread Spectrum)* modulation to

achieve a maximum data rate of 54 Mbps. The standard saw the introduction of Adaptive Rate Selection *(AR)*

- **802.11.g** Building on the success of the 802.11b, the IEEE 802.11G standards were released. IEEE 802.11g also operated in the 2.4GHz band, achieving a throughput of 54Mbps. IEEE 802.11g was also compatible with IEEE 802.11b, although the backward compatibility does degrade performance. 802.11g adopted OFDM modulation but also supported DSSS.

- **802.11n** was the next release of the IEEE 802.11 standards. The primary objective of IEEE 802.11n was to improve the speeds of Wi-Fi networks, which were beginning to carry more multimedia applications. IEEE 802.11n marked another step forward in the throughput of Wi-Fi networks, with a maximum data rate achievable at 600 Mbps. IEEE 802.11n also included other notable improvements, such as increased channel bandwidth and included advances in antenna technology. It also introduced Multiple-Input and Multiple-Output (MIMO). MIMO enables signals to travel on different capture paths *(*due to reflection or propagation) with multiple antennas, improving system performance by enhancing the effective signal-to-noise ratio. It also included updates to OFDM modulation, supporting many signal formats and high-throughout structure. Channel bonding was introduced which supports 40 MHz, enabling two adjacent 20MHz channels to bonded together.

- **802.11ac** The insatiable requirement for improved data rates and broad adoption of smartphones, tablets, smart TVs, and a host of connected devices was a primary objective in IEEE 802.11n. Wi-Fi was now fully mainstream

and dominant wireless communications technology. IEEE 802.11ac further extended the data rate of 802.11n by developing what was known as VHT. Very High Throughput enabling data rates of approximately 7 Gbps [293]. Once again, IEEE introduced a raft of innovations in the standard. IEEE 802.11ac was notable because the Wi-Fi Alliance released the standard over two releases, termed waves. The introduction of MU-MIMO enables data frame transmission to multiple clients simultaneously, bringing more spatial awareness for different users and supporting up to 8 spatial streams [294]. Spatial awareness refers to the ability of the MIMO system to distinguish between paths or directions of signal propagation, which enhances the Wi-Fi system performance.

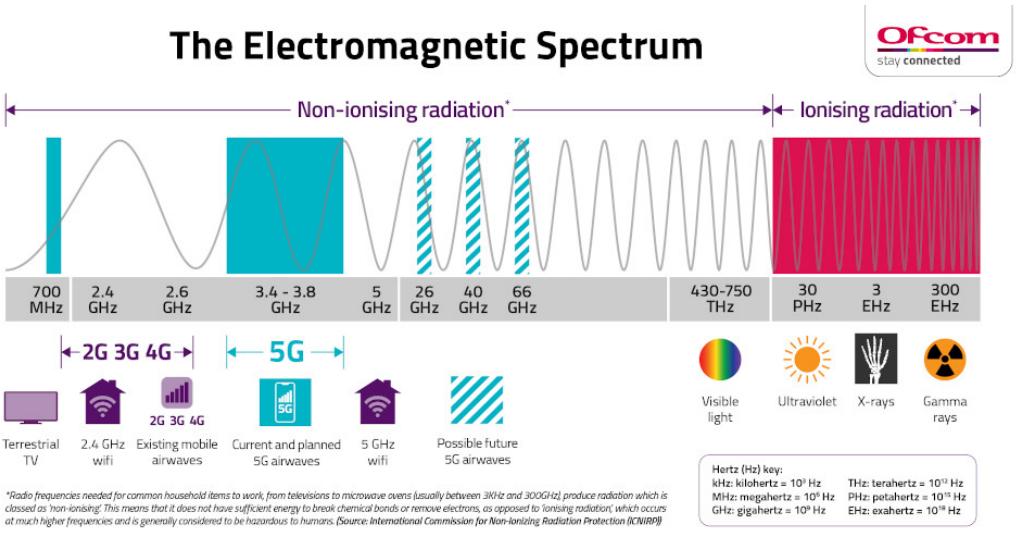


Figure **(3.6)** –Electromagnetic spectrum; source OFCOM

Improvements in radio technology enable designers to use more sophisticated DSP techniques to improve the efficiency of IEEE 802.11ac networks compared to earlier versions. For example, 256 QAM modulation enables

improved raw data rates, that rate is only possible by using 160 MHz bandwidth and all MIMO spatial streams [295]. Earlier releases of the IEEE 802.11 standards have typically used 20 MHz channels. 40 MHz channels are available in IEEE 802.11n. The 802.11ac standard leverages channel bandwidths of 80 MHz and includes options of 160 MHz, or two 80 MHz [296]. To enable increased bandwidth adaptively IEEE 802.11ac also included updates to the Protocol Data Unit, PPDU, to enable beamforming and multiuser support features [297].

- **802.11ad** With the advent of AR/VR and ever-increasing bandwidth demands, the IEEE deviced the IEEE 802.11ad standard to address applications requiring very high bandwidth with low latency. The IEEE 802.11ad standard, or WiGig, uses frequencies in the 60 GHz range. The use of the electromagnetic spectrum at 60 GHz supports significantly higher data throughput. The signal propagation characteristics are an advantage in 802.11ad. Given that signals do not travel far and are absorbed by the environments easily, they support channel coexistence without interference. IEEE 802.11ad markets itself through the Wireless Gigabit Alliance as **WiGig**. It leverages the PHY/MAC specification of IEEE 802.11ad. IEEE 802.11ad leverages the same MAC standard and can support interoperability between Wi-Fi networks operating in the 2.4 GHz and 5 GHz frequency bands. The maximum data supported is 7 Gbps. The typical distances of operation are up to 10m.

- **802.11af** White space is unused radio frequency spectrum. With television going digital, parts of the spectrum from 50 MHz to 700 MHz became

available. Interest in using this spectrum for communication began in the mid-2000s, but has since decreased due to controversies and global differences [298]. IEEE 802.11af aims to use the underutilized UHF portion of the spectrum

"White-fi" or IEEE 802.11af is a wireless communication technology that operates in the sub-1GHz frequency range. It transmits data over longer distances but has lower bandwidth. Dynamic control and adaptation are necessary to avoid interfering with existing television transmissions [299]. Geolocation information and sensing are used to configure the network dynamically [300]. Cognitive radio and geolocation databases enable channel hopping and avoid interference with occupied channels.

- **802.11ah** Many IoT applications require low data rate applications that must transmit data over longer distances. Technologies such as LoRa and Sigfox [57] address this need. IEEE 802.11ah is a competing technology that operates in the ISM band below 1 GHz, enabling data to travel much greater distances [301]. However, 802.11ah has higher latency or lower speed than popular Wi-Fi variants.

  IEEE 802.11ah-based systems use a Hierarchical Association Identifier(H-AID) to connect up to 8191 devices to a single AP [41]. H-AID is used in an Extended Service Set (ESS) to identify Basic Service Sets (BSS), which can be managed as a single logical network. IEEE 802.11ah networks use TIM and non-TIM stations, STAs. TIM STAs monitor for beacon frames sent, while Non-TIM STAs use a target wake time (TWT) feature to enable

the device to sleep, reducing signaling overhead in 802.11ah-based networks [302].

802.11ah networks include new MAC innovations for improved transmission efficiency. The format uses a more compact header format than legacy Wi-Fi, enabling the MAC header to be compressed [303]. The MAC mechanism in IEEE 802.11ah removes the channel access delay and the need for ACK transmission overheads [304].

- **802.11ax** In the next section, we provide a comprehensive overview of the 802.11ax standard, also known as Wi-Fi 6. Given its central importance to this thesis, we offer a detailed discussion in the following section

Table 3.4 compares the evolution of IEEE 802.11 standards.

3.5 802.11ax and Wi-fi 6E

IEEE 802.11-based technologies have proven very successful, despite being only partially efficient [305]. Most Wi-Fi innovations have improved data rates and increased channel bandwidth from PHY and MAC layers. These improvements effectively enabled Wi-Fi to meet the needs of its users by increasing capacity. However, given the insatiable demand and use of Wi-Fi, increased data rates and channel bandwidth did not address the fundamental inefficiencies in Wi-Fi networks.

A principle objective of IEEE 802.11ax technology is improving the efficiency and performance of Wi-Fi networks. Higher data rates and increasing channel size were paramount in previous standard releases. However, IEEE 802.11ax and Wi-Fi 6

	802.11	**802.11a**	**802.11b**	**802.11g**	**802.11n**	**802.11ac**	**802.11ax**
Year Ratified	1997	1999	1999	2003	2009	2014	2019
Operating Band	2.4 GHz	2.4GHz	5GHz	2.4GHz	2.4/5GHz	5GHz	2.4/5GHz 6GHz
Channel Bandwidth	20MHz	20MHz	20MHz	20MHz	20/40MHz	20/40/160MHz	20/40/80/160MHz
Peak PHY Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.8 Gbps	10 Gbps
Max Spacial Streams	1	1	1	1	4	8	8
Max MU Streams						4 (DL)	8 (UL-DL)
Modulation	DSSS FHSS	DSSS CCK	OFDM	OFDM	OFDM	OFDM	OFDM OFDMA
Max constellation	DQPSK	CCK	64-QAM	64-QAM	64-QAM	256-QAM	1024-QAM
Code Rate							
Num OFDM Tones			64	64	128	512	2048
subcarrier spacing			312.5kHz	312.5kHz	312.kHz	312.kHz	78.125kHz

Table **(3.4)** –Comparison of IEEE802.11 standards

notably differ because many features and enhancements target Wi-Fi networks' efficiency, scale and reliability. We will discuss these enhancements in detail and how innovations at the PHY layer, leveraging OFDMA, a multiuser variant of OFDM technology [306]. OFDMA enables more efficient channel usage by allocating blocks of subcarriers for different STA across different timeslots. OFDMA supports uplink and downlink transmissions, enabling simultaneous transmit and receive across many devices [307]. This new functionality fundamentally changes the operating model of Wi-Fi, where legacy Wi-Fi networks compete for channel access. This move toward coordinated access to the medium is a paradigm shift in Wi-Fi networks [308].

IEEE 802.11ax targets improvements in spatial frequency reuse. Conventional network planning typically seeks to avoid intra-channel and inter-channel interference by designing the network to separate the Basic Service Sets (BSS) from each other. A strategy borrowed from the sub-1GHz based systems, seen in IEEE 802.11ah, was to use BSS colouring to increase frequency reuse [309]. The BSS colouring principle uses a variable threshold that permits interfering signals if they originate from a BSS with a different colour. Colour is used to identify groupings of BSS, which will not interfere with each other. In 802.11ax-based systems, channel access assignments use colouring to distinguish overlapping BSS and intra-BSS frames. A Channel Clear Assesment (CCA) determines the minimum received power and can be dynamically adjusted to support more simultaneous transmissions.

802.11ax also introduces the 1024 QAM modulation, where a symbol carries 10 bits, enabling 25% more data in to be carried with a 802.11ax waveform [310]. High-order modulations require good signal conditions with a low noise floor;

	802.11n	**802.11ac**	**802.11ax**
Frequency range (GHz)	2.4,5	5	2.4,5,6
Channel Bandwidth (MHz)	20,40	20,40,80, 80+80, 160	20,40,80, 80+80, 160
Subcarrier spacing (KHz)	312.5	312.5	***78.125***
Symbol Time μs	3.2	3.2	***12.8***
Mu MIMO	No	Downlink	**Downlink and Uplink**
Coding	BCC (mandatory) LDPC (optional)	BCC (mandatory) LDPC (optional)	BCC (mandatory) LDPC (optional)
Data subcarrier modulation	BPSK,QPSK 16/64-QAM	BPSK,QPSK 16/64/256-QAM	BPSK,QPSK 16/64/256/1024-QAM

Table **(3.5)** –802.11ax Comparison to legacy versions

typically, the STA is close to the AP. MU-MIMO, introduced in 802.11ac, becomes much more prevalent in 802.11ax. MU-MIMO enables data transmission to multiple clients, simultaneously taking advantage of various antennas and creating narrow collision domains. In 802.11ax, MU-MIMO supports both downlink and uplink scenarios, providing time synchronisation and transmitter chain frequency alignment, which improves the efficiency and performance over the SU-MIMO of 802.11ax by a factor of 3X.

3.5.1 OFDMA

OFDMA is an evolution of OFDM, which supports multiple users by allocating a subcarrier for numerous users, enabling concurrent access to radio resources [311]. OFDM is a modulation scheme used in broadband and wireless communication. It breaks down a channel into orthogonal sub-channels carrying data on separate frequency carriers, ensuring efficient spectrum use. OFDM is useful in settings with reflections, as it resists fading and interference. It handles high data rates with low complexity, making it preferred in Wi-Fi and 4G LTE standards.

Before 802.11ax, Wi-Fi networks assigned a whole channel to individual users, where CSMA was used to avoid collisions on the channel. With CSMA, client devices listen to the channel to determine if the channel is free. If a client detects the channel is free, it sends its data, hoping that no other device is transmitting simultaneously. The transmitting device waits to receive an *ACK* to determine the packet was received correctly. Otherwise, the device will resend its packet. As discussed earlier, on congested networks collisions happen frequently, resulting in poor performance. In Figure 3.8, we also illustrate another issue with the Wi-Fi systems: each client device is allocated the total bandwidth of the channel, irrespective of the needs of the client device.

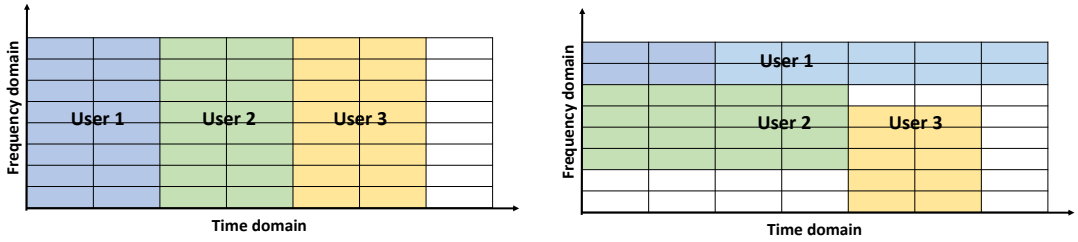


Figure **(3.7)** –difference between OFDM and OFDMA

OFDMA facilitates more efficient spectrum utilization by allocating sections of the available spectrum to distinct users. In an OFDMA system, the channel bandwidth is partitioned into smaller sub-channels, termed Resource Units (RUs), and finer frequency allocations. The functioning of OFDMA is depicted in Figure 3.7. This figure demonstrates that the Access Point (AP) allocates RUs to each client based on their bandwidth needs. This allocation process is dynamic, with each timeslot potentially having varied RU assignments. RUs are assigned during both uplink and downlink communications. In downlink communications, the

AP broadcasts across the entire channel, with client devices discerning the data intended for them. Conversely, client devices transmit concurrently on their designated RUs during uplink communications.

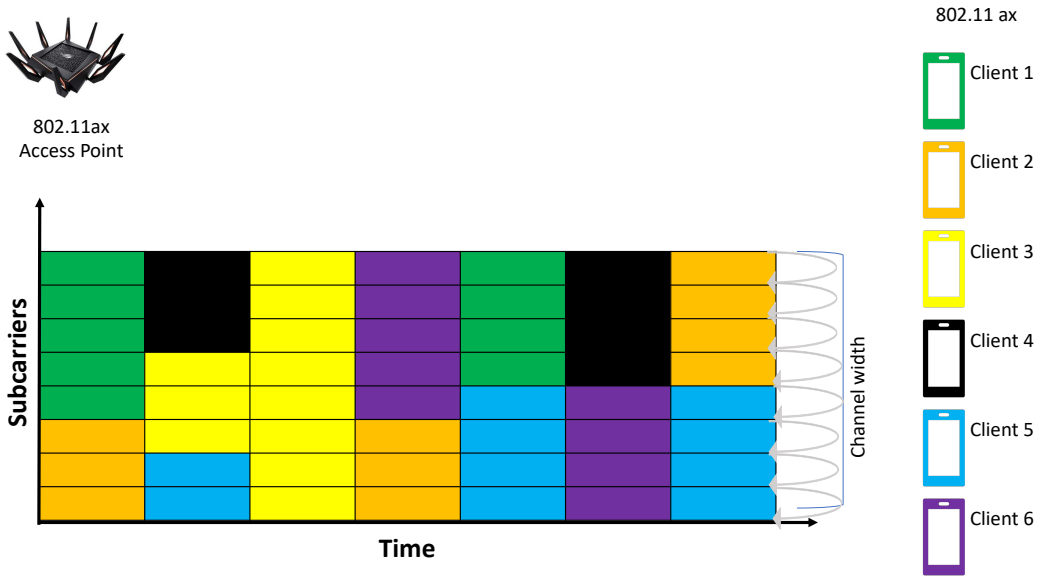


Figure **(3.8)** –802.11ax OFDMA operation

The 802.11ax standard introduces a longer symbol time of 12.8μs, in contrast to the 3.2μs symbol time of legacy systems. This extended symbol time results in a reduction of the subcarrier size and spacing from 312.5kHz to 78.125kHz. This reduction enhances channel robustness. The introduction of guard intervals of 1.6μs and 3.2μs offers **2X** and **4X** protection, respectively, against Inter-symbol interference (ISI) and the effects of multipath propagation, thereby achieving performance comparable to LTE-based technologies.

In OFDMA's downlink mode, an AP amplifies the transmission power for RUs with weaker signals and diminishes the power for stronger signals. While signal strength often correlates with distance, this is not always the case. Such dynamic

power management mitigates interference while ensuring consistent aggregate power across the frequency band. In uplink scenarios, the AP allocates RUs to multiple users and orchestrates their transmissions. The AP dispatches a trigger frame, guiding the Station (STA) in terms of timing, power levels, and frequency. As multiple STAs relay their data packets, the AP employs a channel matrix operation to segregate the data from each uplink. This means that the AP uses the knowledge of the channel (represented by the channel matrix) to distinguish and correctly interpret the signals coming from different STAs

BSS channels are segmented into subcarriers, which are smaller frequency allocations, and Resource Units (RUs). RUs are distributed among various STAs based on factors such as the hardware capabilities of the STA, prevailing channel conditions, and specific transmission service requirements.

In the 802.11ax specification, a 20MHz channel encompasses 256 tones, each separated by 78.125kHz. These tones, or subcarriers, facilitate data transmission within the wireless channel, as depicted in Figure 3.9.

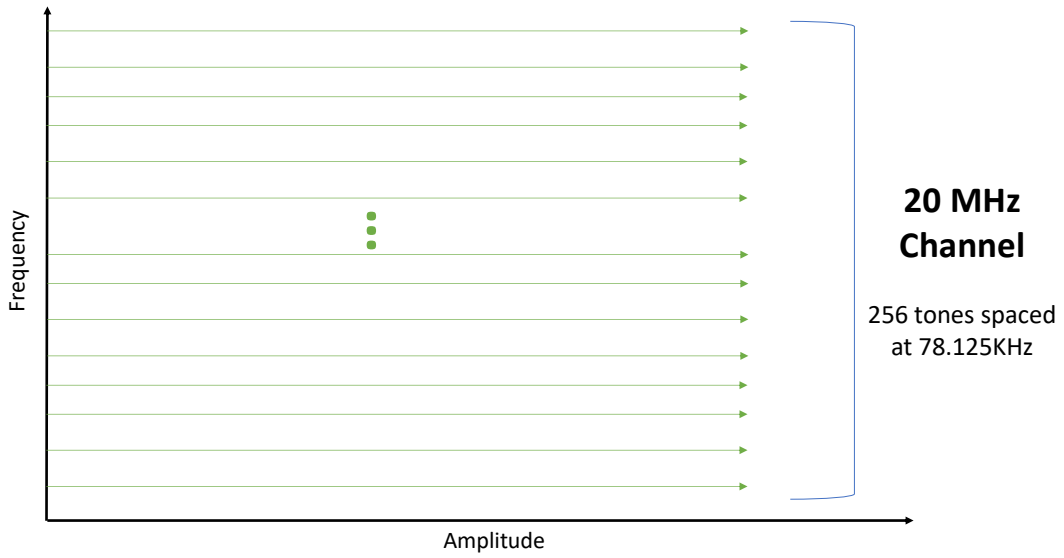


Figure **(3.9)** –OFDMA subcarriers

Out of the 256 available tones, some are reserved for pilot tones and guard tones, leaving 242 tones for allocation as RUs to client devices. The smallest RU is composed of 26×78.125kHz, equating to a bandwidth of approximately 2.03MHz. As illustrated in Figure 3.10, within a 20MHz channel, the smallest RU of 26 tones supports up to nine clients. The figure also presents various potential configurations for the channel. A notable advantage of OFDMA is its capability to combine different RU sizes, ensuring optimal channel utilization.

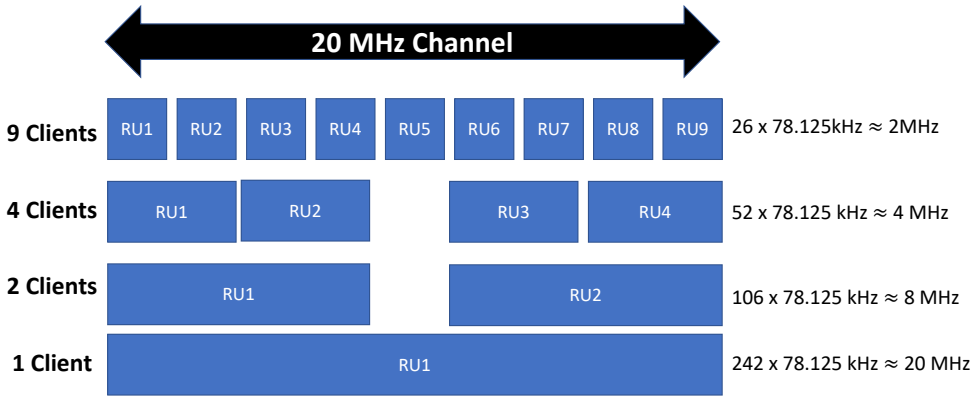


Figure **(3.10)** –OFDMA Resource Units allocation in frequency bands

Wi-Fi networks have incorporated strategies from mobile communication systems, notably from LTE networks, which have employed these techniques in recent years. This shift towards pre-scheduled communications ensures that participants in the 802.11ax network have a predefined transmission schedule for frames. Additionally, OFDMA enhances efficiency by distributing transmission overheads among multiple STAs.

Furthermore, the bolstered robustness of transmissions yields superior performance in environments characterized by diverse propagation models. For instance, a 20MHz channel consists of 256 subcarriers, referred to as tones. These tones are grouped to accommodate nine users concurrently. Channels with greater bandwidth can cater to an increased number of simultaneous users.

3.5.2 1024 QAM

Quadrature Amplitude Modulation (QAM) is a digital modulation technique where both the amplitude and phase of high-frequency carrier signals are modulated for data transmission. The transmitted signal can be visualized on a constellation plot

with in-phase (I) and quadrature (Q) components as axes. These two components are separated by a phase difference of 90°, rendering them orthogonal.

In QAM, multiple bits are grouped to form a symbol on the constellation plot, as depicted in Figure 3.11. Each symbol, termed a state, possesses a unique amplitude and phase, distinguishing it from other points in the constellation. The modulation scheme operates on binary data, and the number of potential bits for transmission is represented as $M = 2^N$. Here, M denotes the total possible combinations corresponding to N bits, which are the constellation points. Given that 2^N yields an integer, the total number of transmitted bits is $N = \log_2 M$. This modulation technique is also called M-ary QAM, where M signifies the number of bits in the constellation.

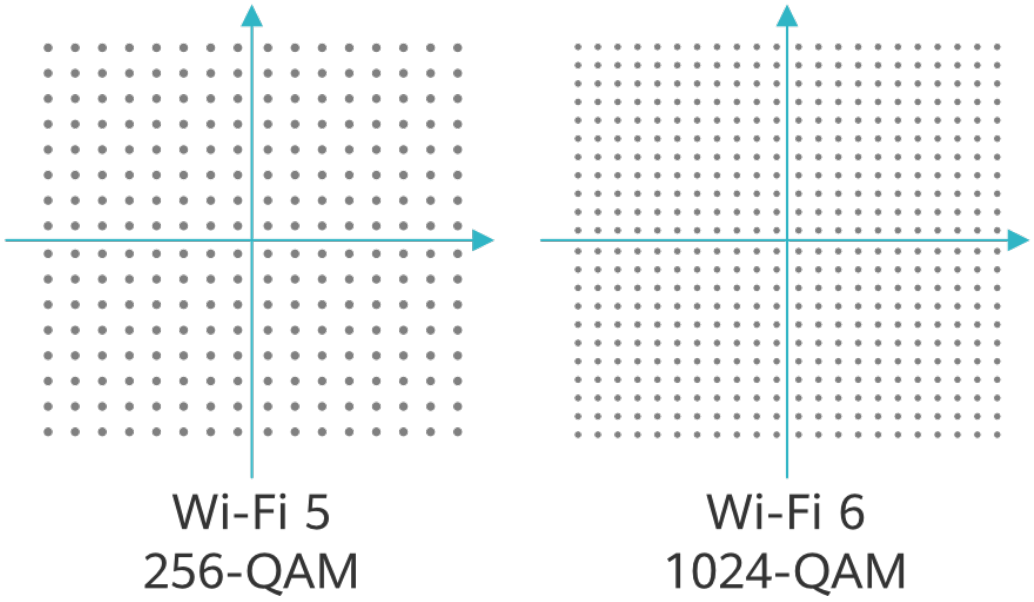


Figure **(3.11)** –QAM constellation plots showing the difference between Wi-Fi 5 and Wi-Fi 6[1].

[1]Source: `https://support.huawei.com/enterprise/en/doc/EDOC1100102755`

The 802.11ax standard introduces 1024-QAM, allowing fixed-frequency carrier waves to assume one of 1024 distinct states. Each symbol in this scheme represents 10 bits chosen from 1024 combinations. This adoption of 1024-QAM facilitates an enhanced data rate between APs and STAs. Furthermore, 802.11ax-based systems incorporate modulation and coding schemes (MCS) 10 and 11.

While 802.11ax retains support for lower-order modulations from its predecessors, MCS 10 specifically aims to augment spectral efficiency in environments boasting a high SNIR (35dB). These schemes are optional for both single-user and multi-user transmissions.

Such enhancements are primarily designed for devices near an AP. These environments must remain devoid of radio interference and maintain a low-noise floor.

3.5.3 MU-MIMO

Multiuser, Multiple-Input, Multiple-Output (MU-MIMO) technology, a significant feature of Wi-Fi 6, facilitates simultaneous access for users in both uplink and downlink scenarios. While MU-MIMO's inception was in 802.11ac Wave 2, it was confined to downlink transmissions from the Access Point (AP) to client devices. Its primary goal in Wi-Fi 6 is to enhance network efficiency, especially when multiple clients demand concurrent access.

Historically, in 802.11 networks, congestion arose as APs processed client requests sequentially. This sequential processing increased wait times as more devices sought AP resources. MU-MIMO addresses this bottleneck by allowing multiple clients to access AP functionalities concurrently.

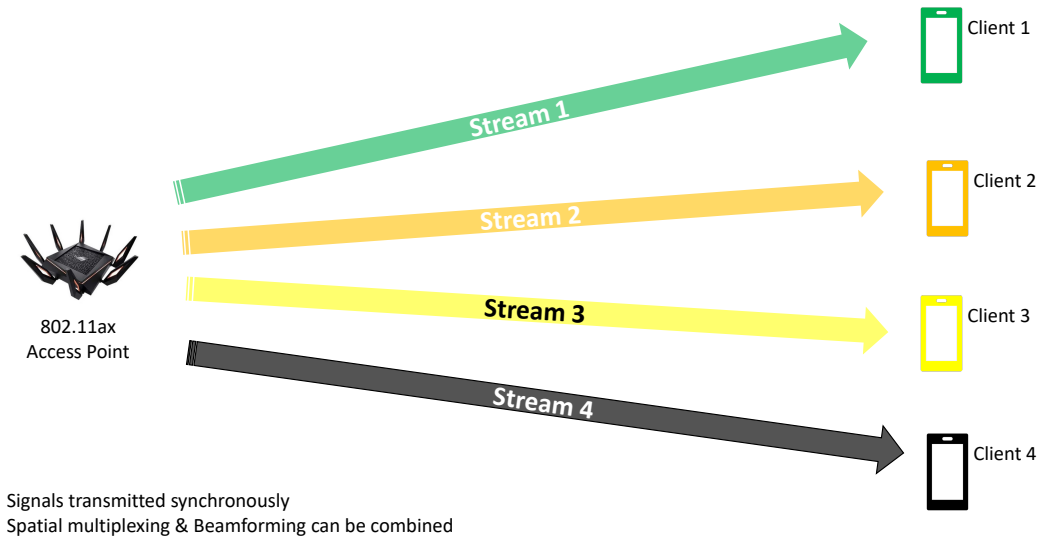


Figure **(3.12)** –Multiuser MIMO operation

As depicted in Figure 3.12, MU-MIMO partitions the available bandwidth into individual streams, distributing connectivity evenly among clients. The 802.11ax standard supports eight simultaneous MU-MIMO transmissions, each potentially using a unique Modulation and Coding Set (MCS) and varying spatial streams. During uplink operations, the AP gathers beamforming data from connected STAs, employing beamforming techniques to direct packets to diverse STAs spatially. The AP computes a channel matrix for each user, dispatching beams containing distinct packets for targeted STAs. When users simultaneously send back their packets, the AP uses the channel matrix to discern the information from each uplink beam.

MU-MIMO, in tandem with OFDMA, borrowed from cellular systems, enhances spectral efficiency and offers a bandwidth increase of up to 4X compared to 802.11ac systems. These technologies support concurrent transmissions from STA

to AP, reducing collision probabilities in high-density areas and thus elevating the overall throughput of 802.11ax networks.

While MU-MIMO proves invaluable in dense environments with competing client devices, its adoption has implications. Devices that harness MU-MIMO's uplink capabilities necessitate multiple antennas, leading to increased costs, size, and power consumption. In the realm of IoT, this demands careful trade-offs. However, the trade-off between performance and reliability might be more justifiable for industrial applications.

3.5.4 Enhanced PPDU formats

The IEEE 802.11ax standard introduces an enhanced Physical Layer Protocol Data Unit (PPDU) format, which brings several improvements over its predecessor in 802.11ac. This new format supports both legacy and multi-user environments, ensuring compatibility with previous Wi-Fi standards.

One of the significant enhancements in 802.11ax is the incorporation of OFDMA (Orthogonal Frequency Division Multiple Access) and MU-MIMO (Multi-User Multiple-Input Multiple-Output) technologies. These technologies necessitate substantial modifications to the PPDU, including advanced carrier sense techniques and support for simultaneous uplink and downlink data transmissions. The 802.11ax standard introduces five new frame formats, with a legacy preamble ensuring backward compatibility with older STAs. These formats are detailed in Table 3.6 and include:

- **HE-SU**: For single-user transmissions.

- **HE-MU**: Supports multi-user transmissions using OFDMA, MU-MIMO, or a combination. This format typically operates in downlink.
- **HE-ER-SU**: Designed for extended-range, single-user transmissions, featuring a power-boosted preamble.
- **HE-NDP PPDU**: Facilitates beamforming operations and channel probing.
- **HE-TRIG-PPDU**: Supports triggered multi-user uplink responses following an AP's trigger frame.

The role of the AP in 802.11ax is pivotal. It orchestrates scheduling using *trigger frames* for both uplink and downlink transmissions, guiding connected STAs. In CDMA-CA, channel reservation is established through an RTS-CTS handshake. The 802.11ac Wave 2 introduced MU-RTS frames, enabling synchronized operations across devices. These frames provide signalling data to uniquely identify participating STAs, which then respond with a CTS in a non-HT format.

The main uplink transmission modes in 802.11ax include:

- Single STA utilizing the entire channel.
- Multiple STAs transmitting on different channels.
- Multiple STAs sharing the same RU (MU-MIMO).
- Mixed MU-MIMO and OFDMA with STAs sharing the same RU allocation.

MU-MIMO operations commence with a channel-sounding function, determining the radio channel's state between the AP and STA. This Channel State Information (CSI) is crucial for MU-MIMO and OFDMA RU allocations. It allows the AP

to comprehend channel conditions across subcarriers, with STAs relaying their channel conditions to the AP.

PPDU Field Abbr.	Description	Duration (µs)
L-STF	Non-HT Short Training field	8
L-LTF	Non-HT Long Training field	8
L-SIG	Non-HT Signal field	4
RL-SIG	Repeated Non-HT Signal field	4
U-SIG	Universal Signal field	8
EHT-SIG	EHT Signal field	4
EHT-STF	EHT Short Training field	4
EHT-LTF	EHT Long Training field	Variable
EHT-Data	Data field carrying the PSDUs	Variable
PE	Packet Extension field	Variable

Table **(3.6)** –IEEE 802.11ax PPDU Frame structure

3.5.4.1 Trigger Frames

In IEEE 802.11ax, the Access Point (AP) is pivotal in managing, coordinating, and orchestrating network operations, especially in multiuser contexts. A key mechanism is the *trigger frame*, broadcasted by the AP for resource allocation and coordination of multiuser transmissions. This frame ensures synchronized uplink from multiple STAs and uses a split structure containing pre-HE and HE parts. The HE part is constructed to be mutually orthogonal between the triggered STAs, allowing the AP to distinguish each STA from the HE-TRIG-MI PPDU.

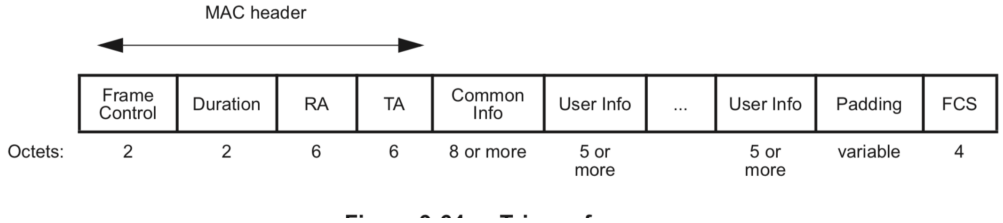


Figure **(3.13)** –802.11ax Trigger Frame

Trigger frames in 802.11ax include:

- Basic Trigger frame
- Beamforming Report (BFRP)
- Multiuser block ack request (MU-BAR)
- Multiuser request to send (MU-RTS)
- Buffer Status Report (BSRP)
- GCR MU-BAR
- Bandwidth Query Report (BQRP)
- NDP Feedback Report Poll (NFRP)

An NDP frame initiates the channel probing operation, with the receiver address set as a broadcast address. The AP sends the NDP frame, a MAC-specific feature, to facilitate radio channel probing. The STA employs a DSP feature called SVD to discern the channel's behaviour.

The frame control uses subfields consistent with other 802.11 systems to ensure backwards compatibility. The shared information field contains shared data for all triggered STAs, guiding their response to the AP.

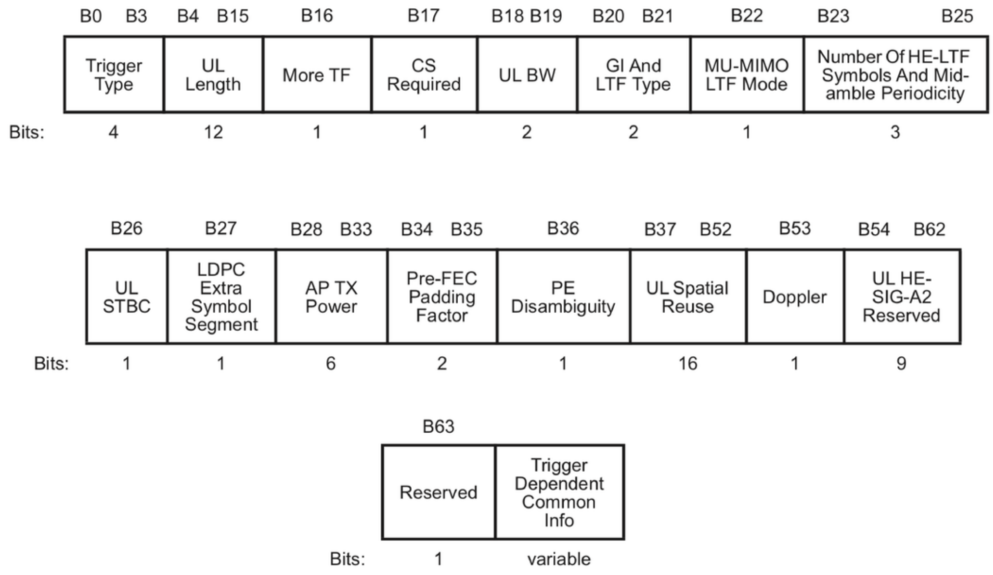


Figure **(3.14)** –802.11ax common information field

The user-specific field contains multiple user fields, indicating RU assignments. Each STA sends its data in the user information field, which includes details like the STA's 12-bit identification number, RU allocation, modulation and coding scheme, and more.

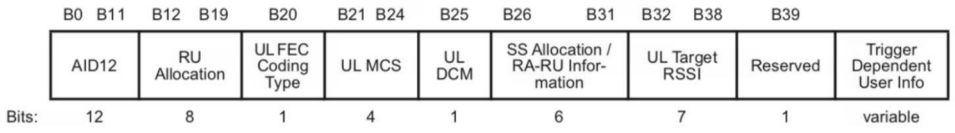


Figure **(3.15)** –802.11ax User information field structure

During data transmission, the AP directs frames to each STA via MU-MIMO or hybrid mode. The AP uses a Block ACK Request (BAR) to confirm successful transmissions. For uplink operations, the AP queries the uplink readiness of STAs using a BSR (Buffer State Report) poll frame. Upon receiving a BSR, the STA synchronizes timing and frequency offsets, adjusts its transmitted power, and

prepares the PPDU for transmission. The AP can send an ACK to each STA individually or via a broadcast frame.

3.5.5 IoT Device support

The IEEE 802.11ax standard introduces a strategic shift in channel utilization, particularly emphasizing the benefits of 20 MHz channels for Internet of Things (IoT) devices. Historically, 20 MHz channels were often overlooked in previous wireless standards due to perceived limitations in bandwidth and capacity. However, 802.11ax repositions these channels as an efficient solution for specific scenarios, supporting IoT devices with modest bandwidth requirements.

- **Device Differentiation**: While low-bandwidth devices, such as sensors and actuators, predominantly utilize the 20 MHz communication channel, devices with higher data demands opt for 40, 80, or 160 MHz channels. The 20 MHz-only mode operates across both 2.4GHz and 5GHz bands, with each 20 MHz channel comprising 256 subcarriers.
- **Enhanced Coverage**: One of the salient advantages of 20 MHz channels in 802.11ax is the extended coverage and range they offer compared to their wider counterparts. This is paramount for IoT devices, which might be deployed in challenging environments with low signal strength or physical obstructions. Narrower channels ensure these devices communicate more reliably, sustaining a robust network connection.
- **Interference Mitigation**: The 20 MHz channels in 802.11ax also play a pivotal role in curtailing interference from coexisting devices on the network. Since IoT ecosystems can be dense, with numerous devices vying

for bandwidth, the narrower channels can significantly mitigate interference, ensuring a stable and uninterrupted connection.

3.5.6 BSS Colouring

IEEE 802.11ax is designed to enhance Wi-Fi performance in dense environments, such as urban areas, transport hubs, and shopping centres, where interference is prevalent. The proliferation of access points (APs) in these areas, while facilitating connectivity, often leads to interference among APs.

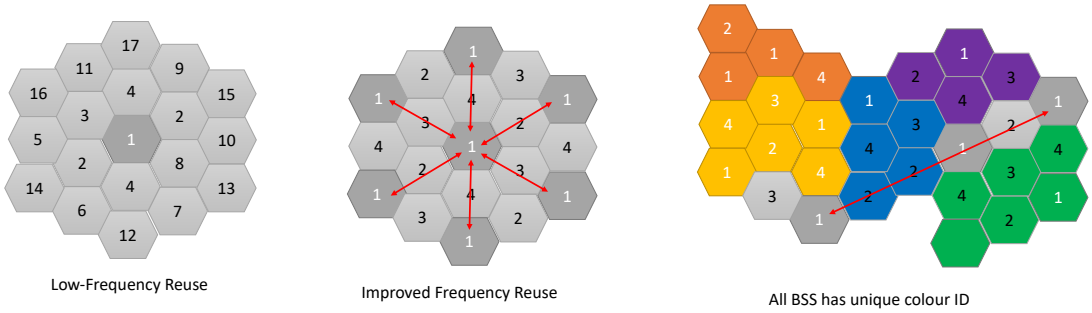


Figure **(3.16)** –BSS Frequency reuse, frequency reuse, and BSS Colouring

To address the challenges posed by dense Wi-Fi deployments, 802.11ax introduces BSS (basic service set) colouring and spatial reuse. BSS colouring assigns a unique "colour" identifier, a 6-bit number, to each AP, allowing multiple APs to operate on the same channel without interference. This "colour" is carried in the signal preamble or SIG field. When a device detects a signal, it checks the BSS colour to determine network affiliation, enabling concurrent transmissions from different networks.

802.11ax also refines the traditional CSMA (carrier sense multiple access) protocol with dynamic sensitivity control (DSC). DSC allows adaptive clear channel assess-

ment (CCA) thresholds, optimizing network performance by reducing co-channel interference. The introduction of overlapping BSS packet detect (OBSS-PD) threshold further enhances spatial reuse, allowing devices to use the channel even in the presence of other signals, provided the signal-to-noise ratio (SNR) is acceptable.

The network allocation vector (NAV), a CSMA/CA protocol feature, acts as a virtual timer, indicating channel availability. 802.11ax introduces a dual NAV system, which uses two NAV timers: one for intra-BSS and another for inter-BSS or OBSS frames. This dual system ensures compatibility with legacy devices and prevents interference from overlapping networks.

In conclusion, 802.11ax's combination of BSS colouring, spatial reuse, and dual NAV significantly enhances spectral efficiency, making it well-suited for dense environments.

3.5.7 Target Wake Up Time

The integration of Wi-Fi in Internet of Things (IoT) applications has historically been impeded by the substantial power consumption associated with Wi-Fi-based IoT devices. Preceding iterations of Wi-Fi were predominantly reliant on continuous mains electricity or necessitated frequent battery replacements, rendering them suboptimal for many applications.

The IEEE 802.11ax standard heralds a paradigm shift by introducing the Target Wake Time (TWT) feature, which ostensibly augments power conservation and network efficiency. TWT facilitates a dormancy mode for stations (STAs) during inactive transmission periods, optimizing power utilization. Initially conceptu-

alized in the 802.11ah standard, TWT is particularly pertinent to IoT devices, characterized by their modest bandwidth requirements and intermittent traffic patterns.

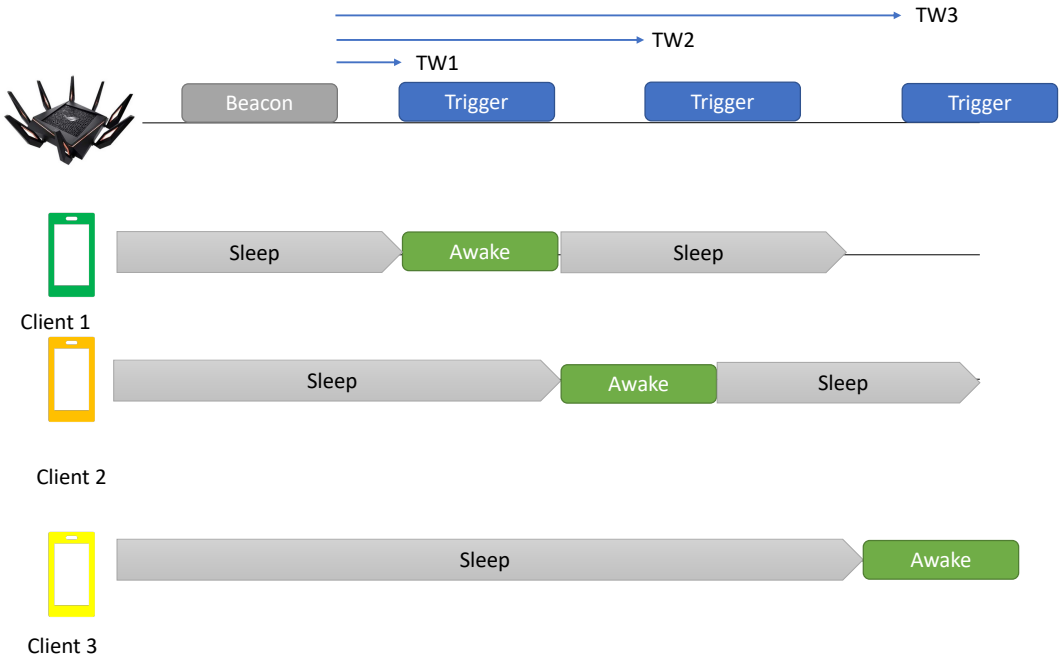


Figure **(3.17)** –802.11ax Target Wake up Time

Within the TWT framework, client devices negotiate specific wake intervals with their associated Access Point (AP), delineating precise transmission and reception epochs. These intervals can either adhere to a predetermined schedule or be contingent upon specific events. During inactivity, the STA reverts to a quiescent state, engendering significant power savings and attenuating network interference. This modus operandi engenders power conservation and mitigates channel contention, thereby bolstering network reliability [312].

TWT operates in two distinct modes:

- **Individual Mode**: An STA directly negotiates with its AP, stipulating wakeup epochs, intermissions, and designated communication channels.
- **Broadcast Mode**: In this mode, the AP orchestrates a communal TWT session for an ensemble of STAs, employing beacon frames to disseminate operational parameters.

The negotiation process exhibits variability, with requesters either **SUGGESTING/REQUESTING** or **DEMANDING**, and responders oscillating between **ACCEPTING**, proffering an **ALTERNATE**, **DICTATING**, or **REJECTING**. An affirmative **ACCEPT** response culminates in establishing a session.

In addition, 802.11ax proffers the capability for dynamic power modulation for transmitted frames between an STA and its AP, thereby enhancing spatial reuse and curtailing intra-BSS interference. This reduces the benefit of battery-dependent devices and optimizes the spectral efficiency of Wi-Fi networks in high-density scenarios [313].

3.6 Conclusion

Wireless technologies have become essential tools for automation and digitization in today's industrial landscape. This paper offers a detailed examination of the current state of wireless industrial networks, highlighting their strengths, potential growth areas, and challenges faced in industrial settings.

Wireless industrial network technologies have been reliable and robust, providing consistent connectivity even in challenging environments. However, these technologies have faced data rates, scalability, and adaptability challenges. Cellular

technologies are gaining traction in industrial settings due to their reliability and wide coverage. The emerging 5G technology promises high-speed data transfer, minimal latency, and the possibility of creating private networks. Such infrastructure supports real-time control, predictive maintenance, and critical industrial applications.

Wireless industrial networks play a vital role in developing robust Industry 4.0 applications. However, these networks confront several challenges that require appropriate attention. Many industrial networks still employ outdated wireless protocols, which hinder optimal performance, reliability, and connectivity. Furthermore, incompatibility issues with legacy industrial protocols pose a significant obstacle to seamless integration with modern technology.

Cellular and legacy wireless systems operate on closed, proprietary architectures that limit innovation and adaptability, hindering Industry 4.0. The move towards more open RAN networks is underway, but progress is slow. Legacy systems challenge the integration of evolving technologies with Industry 4.0 applications like IACS and digital twins, thus hindering interoperability.

Communication protocols are vital in data communication and sharing across industrial settings. However, the underutilization of advanced protocols such as MQTT Sparkplug limits their effectiveness and efficiency. Similarly, the limited adoption of event-driven architectures (EDA) in wireless industrial networks restricts real-time decision-making capabilities, affecting the responsiveness and adaptability of systems in scenarios like PHM and IACS applications.

A lack of consistent application and adherence to wireless protocols and standards negatively affects operational efficiency and effectiveness, particularly in PHM

and digital twin applications. Existing networks often lack the flexibility and scalability necessary to adapt to the evolving technological demands of modern industrial applications.

Developing wireless industrial networks presents a major challenge due to the lack of community involvement. The absence of community-driven development and initiatives hinders technological advances and innovative solutions in the wireless industrial ecosystem. This is mainly due to the bespoke, proprietary, and niche nature of wireless industrial networks, which limits the creation of a large-scale ecosystem to drive the technologies forward.

Our analysis of Wi-Fi, focusing on IEEE 802.11ax and Wi-Fi 6E technologies, reveals that they have significant potential for industrial IoT applications. Wi-Fi 6E offers advanced features such as high data rates, better spectral efficiency, and improved performance in congested areas. This puts Wi-Fi-based systems in an advantageous position to become a cornerstone for future industrial wireless networks. Furthermore, the widespread use and adoption of Wi-Fi brings many benefits, including cost-effectiveness, ease of management, and availability of Wi-Fi technologies and expertise. Additionally, the ease of integrating Wi-Fi into existing infrastructures means that the tools for management and maintenance are common and economical for use.

The future of wireless industrial networks looks promising and full of potential. As these technologies continue to develop, they are set to play a pivotal role in advancing Industry 4.0, leading to more interoperable, efficient, and interconnected industrial systems.

Chapter 4

Radio propagation testing for Industrial Wireless Networks

This chapter outlines the results of radio propagation testing carried out during the Spring of 2023 at the Irish Manufacturing Research facility in Mullingar, Ireland. This chapter details the following contributions:

- **Development of channel-sounding methodology for 6 GHz based wireless industrial networks :** Our research proposes a channel-sounding methodology that enables accurate and efficient wireless channel characterisation in industrial environments. This contribution provides a framework for testing future wireless industrial networks. By providing a detailed understanding of the channel, our methodology can improve the reliability and performance of wireless industrial networks. We contribute to the channel characterisation of wireless industrial environments.

- **Investigation of Wi-Fi at 6GHz in an industrial environment:** In our research, we investigate the effects of various types of industrial interference on Wi-Fi at 6GHz. Our contribution provides a deeper understanding of the effects of industrial interference on wireless channels. It highlights the importance of mitigating these effects in industrial environments. This research can potentially significantly improve the reliability and performance of wireless industrial networks.
- **Evaluation of an industrial based Wi-Fi network in the 6 GHz spectrum:** Our research evaluates the performance characteristics of 6 GHz spectrum, an emerging resource for wireless communications that is particularly important for industrial applications requiring high-performance, reliable, and interference-free communications. We conducted extensive field testing and experiments to evaluate the performance of the 6 GHz spectrum in industrial environments. Our contribution provides valuable insights into the potential of the 6 GHz spectrum for industrial wireless communications. We also discuss the implications of using 6 GHz and propose several recommendations that may contribute to improved performance and reliability of 6 GHz-based wireless industrial networks.

4.1 Introduction

Radio propagation testing is critical for wireless industrial network design and deployment. The deployment of wireless communication systems has increased in the industrial environment, providing significant benefits to industrial processes in terms of increased efficiency, flexibility, and automation.

The industrial environment presents a high degree of variability, with large metal structures and machinery that can reflect and absorb radio signals, causing multipath fading, signal degradation, and increased noise levels [314]. These challenges can result in reduced signal quality and increased signal dropouts, leading to decreased network performance, downtime, productivity, and financial losses [315]. Detailed and thorough testing is essential to ensure that wireless systems deployed in these environments meet the desired performance specifications and are suitable for the intended applications.

Radio propagation testing is essential to successful, reliable wireless deployments in industrial settings [316]. Evaluating the network's performance in a controlled environment makes it possible to identify and resolve any issues before deploying networks in real-world industrial environments.

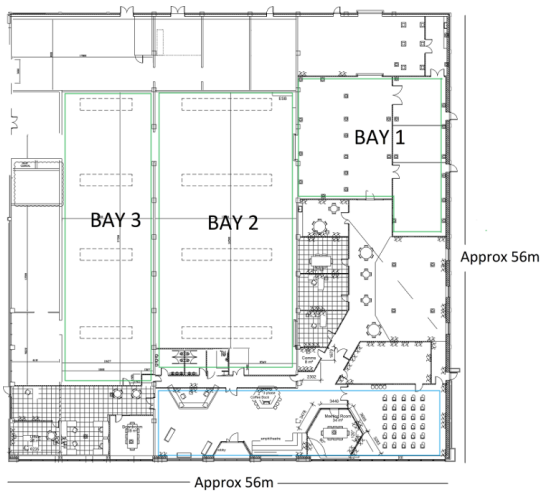
The lack of empirical data on radio propagation in industrial environments significantly hinders the development of optimal wireless industrial networks. Despite this, there is a growing recognition of the importance of radio testing, and researchers have been increasingly exploring and characterising the RF environment in these settings [317].

One of the critical components of radio propagation testing is channel sounding, which involves measuring the channel impulse response, power delay profile, and other parameters that describe the wireless channel characteristics. These measurements can provide a deep understanding of the behaviour of radio signals in industrial environments, including multipath effects and the impact of obstacles on signal propagation [318]. The Rician K factor is another important parameter to quantify the level of line-of-sight (LOS) and non-line-of-sight (NLOS) components in a wireless channel. The K factor is essential in analysing industrial wireless networks, particularly those required to provide reliable communication through complex environments [319].

4.2 Test site overview

Given the widely different environments in industrial environments, a comprehensive understanding of the physical environment is essential. Lab-based experiments provide some initial analysis; however, a thorough investigation of an environment's actual RF propagation characteristics is necessary to ensure the system will operate in the specific environmental conditions of an industrial setting [320, 321].

In other application or deployment scenarios, existing empirical models may suffice. For example, a commercial office space configuration and setup are often similar. They follow standard norms of layout and design to comply with ergonomic and architectural best practices. The similarities give offices a high degree of homogeneity across the office and commercial settings. Consequently, many RF propagation models can be readily used confidently to in less complex and dynamic enviroments [322].



(a) IMR Test site, floor plan

(b) IMR Test site, Bay 3, visual

Almost in stark contrast sits industrial operations and factories. Even today, more substantive research on different manufacturing configurations and setups needs to be done [323]. One of the most notable contributions to state-of-the-art is the work conducted by National Institute of Standards and Technology (NIST) in this space [324].

We aim to expand upon NIST's work and contribute to RF propagation testing in conducting radio propagation testing in the 6GHz spectrum. Furthermore, we devise a channel-sounding test apparatus for RF propagation testing.

Moreover, most of NIST's testing was conducted in what might be termed traditional industrial locations, such as a machining environment for automotive or steam plants. Our work focuses on emerging manufacturing trends and new processes, such as reconfigurable and additive manufacturing.

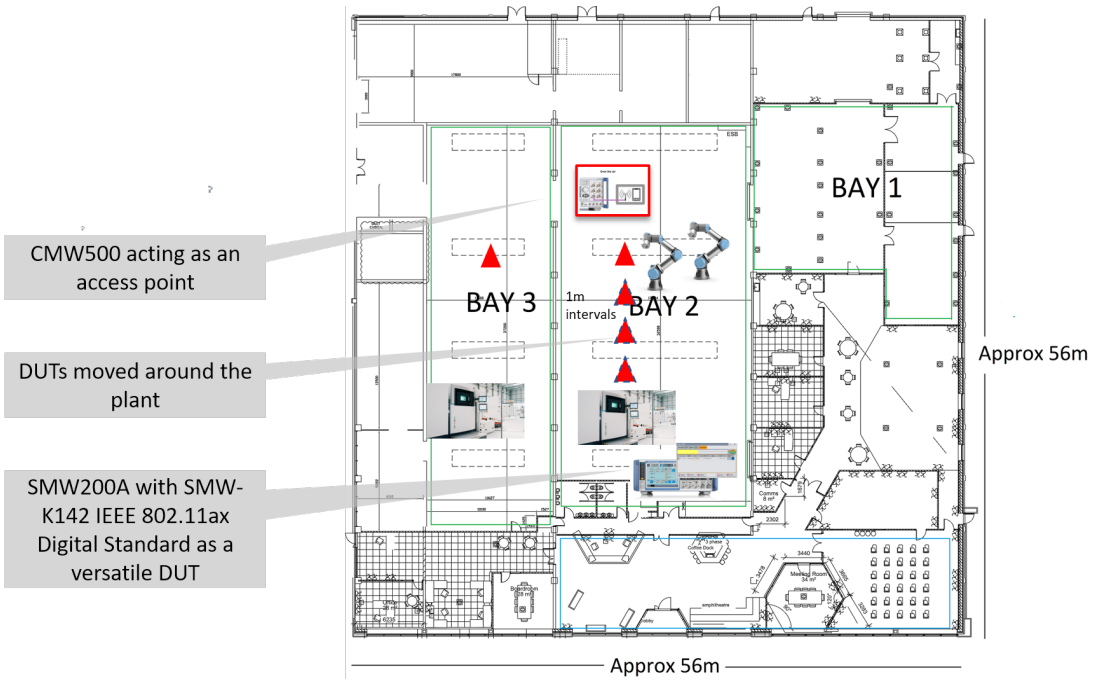


Figure **(4.2)** –IMR Network test layout

The testing we conducted at Irish Manufacturing Research, an operational test facility to test early emerging technology innovations focused on modern manufacturing configurations such as flexible work cells and associated technologies. We elected to use a pilot line used for medical device manufacturing. The line comprises three cells. The three cells are printing, finishing and inspection.

- **Printing**: The printing cell, shortened from 3D printing, contains the additive manufacturing (AM) printer used in medical device production. Parts are created layer by layer to make a completed part. Medical devices such as surgical implants, surgical guides, prostheses, and bio-manufacturing have grown in use and popularity and are becoming increasingly mainstream.

- **Finishing**: The finishing cell is a post-printing process used to remove excess materials or build-up from the printing process and to ensure conformity and correctness of the surface texture of the printed part. The finishing cell uses a collaborative robot (CoBot)-style system to remove abnormalities or minor defects from printed parts
- **Inspection**: The inspection cell ensures all printed and finished pieces are completed with their design parameters and the final product quality. Advances in machine vision and AI-based technologies enable automated in-situ inspection of a part, requires little human examination, and pre-trained defect models conduct assessment

The testing configuration is illustrated in Fig. 4.3. The RX test apparatus was located where an existing Wi-Fi AP is located. We tested in 1m increments, moving the TX from the RX. NIST contends that a typical factory work cell range is 10 m.

The maximum range we covered was 25 m. The distance end-to-end of the bay was slightly greater than 30 m. However, obstructions at both ends of the bay allowed us to measure a maximum distance of 25 m. At each 1 m waypoint increment, we triggered our testing system to collect the data discussed in the forthcoming sections.

4.2.1 Channel sounding testing

In radio propagation testing, *Channel sounding* characterises the radio channel. Data collected from channel sounding is used to optimise the design and performance of wireless networks, ensuring that they operate effectively and provide

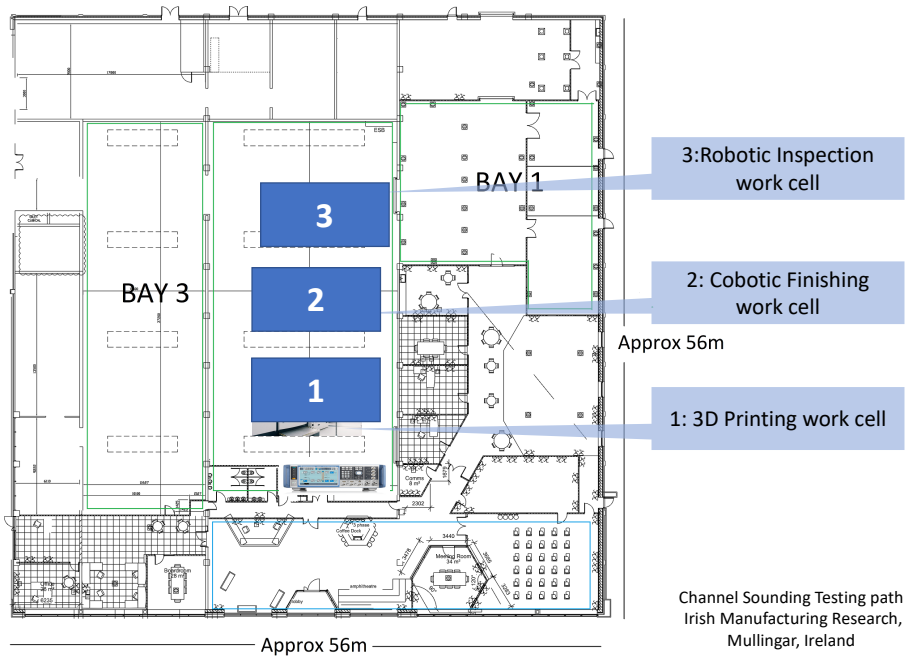


Figure **(4.3)** –Testing bay and manufacturing cells

reliable communication. Given industrial environments' dynamic and highly reflective nature, channel sounding is an essential testing process.

A *channel* refers to the path or multiple paths through which information is transmitted between a sender and a receiver, commonly referred to as the RF (Radio Frequency) channel in wireless communications. When designing wireless systems, mathematical simulations approximate the conditions of the target environment [325]. These conditions encompass aspects like the physical surroundings and the frequency of the RF band, which are crucial in ensuring that the system meets its performance and reliability standards. Other essential parameters, such as multipath effects, fading, and path loss, are analyzed and evaluated during this design phase. Collectively, these factors shape the characteristics of the RF channel.

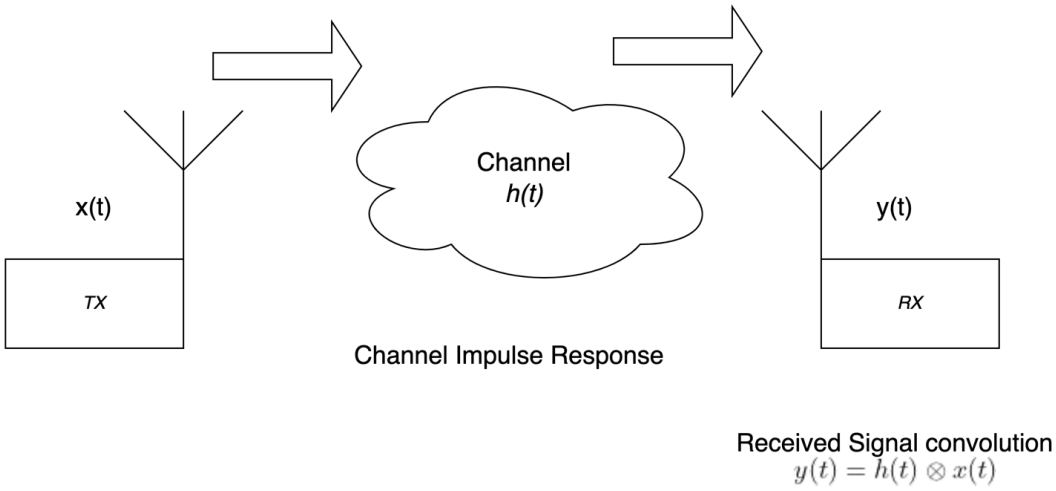


Figure **(4.4)** –Channel sounding operation

Channel sounding is a set of measurement techniques used to understand the characteristics of an RF channel [326]. It involves the decomposition of the radio propagation path into multipath elements. Channel sounding is a technique used to determine the impulse response of a communication channel. The channel impulse response (*CIR*) is one of the most critical characteristics in defining the communications channel, enabling insights into a channel's effect on radio signal transmissions. Industrial environments will have all manner of distortions caused by diffraction and scattering from machinery and equipment, along with reflections introducing signal echoes into the radio channel [327].

A *channel sounder* is a system that detects electromagnetic waves in a communication channel. It determines a channel's time-variant frequency response and time-variant impulse response. Channel sounding tests transmit band-limited impulse Tx and record the signal upon arrival at the receiving location Rx. How-

ever, in many real-world scenarios, directly employing this methodology can be challenging due to several reasons:

1. **Regulatory Constraints**: Transmitting strong impulses might violate regional or national regulations, especially if the impulse spans multiple licensed or unlicensed bands.

2. **Interference with Other Systems**: High-power or wide-bandwidth impulses can interfere with other ongoing communications, leading to disruptions and inaccurate measurements

3. **Environmental Variability**: Dynamic factors like moving objects or changing weather conditions can affect propagation characteristics, making consistent measurements challenging.

4. **Multipath Propagation**: Signals taking multiple paths due to reflections in industrial settings can cause interference, complicating the true channel characterization.

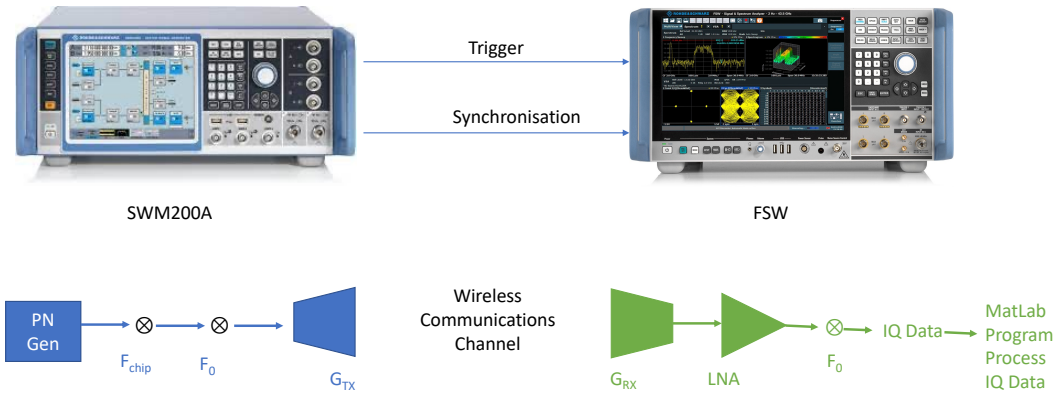


Figure **(4.5)** –RF sounding sequence

Sounding testing can be in static or dynamic modes. Static mode refers to a setup where both the transmitter and receiver are fixed at locations in the test environment. In dynamic scenarios, one of the Rx and Tx terminals move. In an industrial setting, both modes of operation would be typical. While mobility is becoming increasingly prevalent, many elements of a manufacturing environment would remain relatively static, such as APs and larger machinery, plant, and equipment. We require separate receive and transmit terminals in mobile radio propagation tests. Our testing uses a preamble-based approach using known symbols received at the Rx from the Tx sounder devices [328].

4.3 Channel sounding system design

A high-level design of our sounding system is outlined in figure 4.6, with all of the components used in our experiments detailed in Table 4.1.

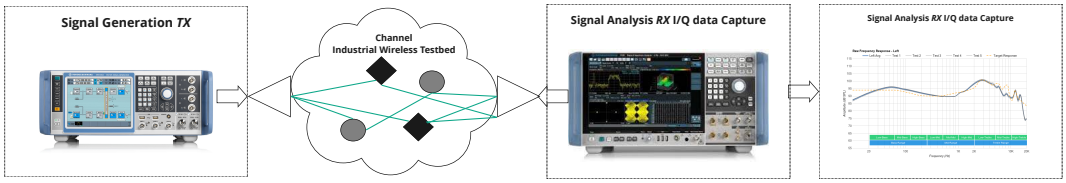


Figure **(4.6)** –High-level RF measurement setup

Our system uses a *triggered* mechanism between the transmitter and receiver. The system is connected via two coaxial cables between a vector signal generator and a Spectrum analyser in our setup. A 10 MHz reference output synchronises the spectrum analyser to the signal generator. This ensures synchronisation between

the instrumentation and prevents sampling clock and frequency offsets between the receiver and transmitter.

Equipment Type	**Manufacturer**	**Purpose**
Vector signal generator	Rhode and Schwarz	Generation of waveform data across frequency bands of interest
Signal and spectrum analyser	Rhode and Schwarz	Capture of spectrum and waveform data. Processing data into I/Q data for data analysis
Channel sounding Software	Rhode Schwarz	Perform data analysis on I/Q data captured from spectrum analyser
MatLab Software	Mathworks	Analysis of metrics and measurement of key metrics and processing of associated measurements

Table **(4.1)** –Inventory of test equipment used for sounding system

Triggering a sounding test initiates the measurement process of the channel sounder system. The process involves sending a signal from a command from a waveform generator. The waveform generator is programmed with the appropriate RF parameters for testing. The transmitter generates and transmits an RF signal into the channel under test. The system receives the signal after it has propagated

through the channel and produces an I\Q waveform file, which contains complex sample values of the waveform signal captured.

The I\Q files must be further processed, processed, and analysed to gather insights into the channel's performance, such as path loss, gains, and multipath effects.

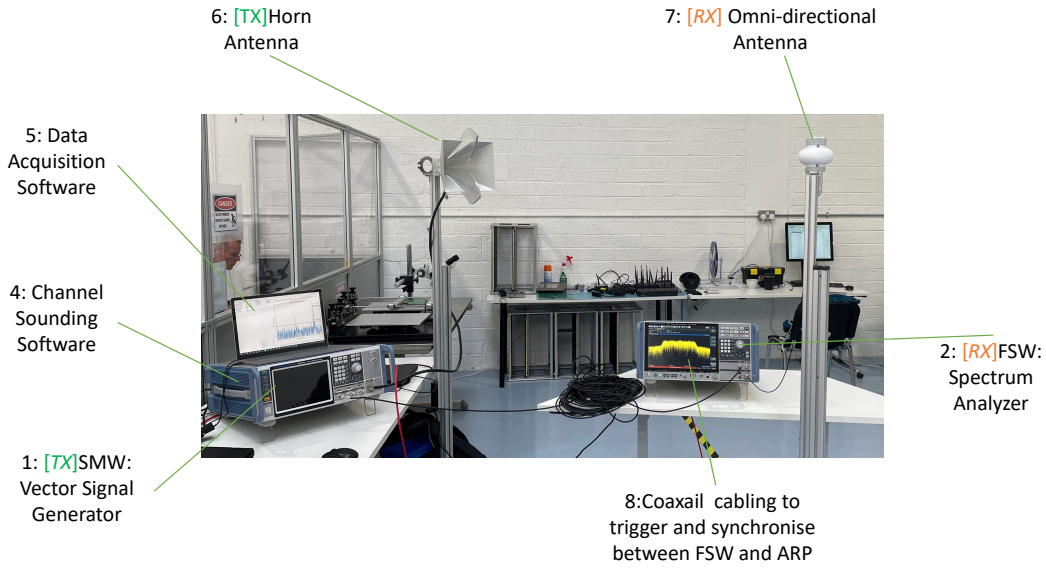


Figure **(4.7)** –RF sounding system layout

We constructed a mobile acquisition unit to house and collect data from the factory along a defined route marked out. The route path is illustrated in Figure 4.9. The predetermined paths were selected as representative locations of mobile traffic to ensure a substantial diversity of coverage of the factory floor, supporting the ability of flexible and modular configuration on the factory floor [329].

4.4 Radio propagation testing process

This section details the testing and measurement process we implemented to conduct radio propagation testing at IMR. Firstly, we provide a brief discussion and calculations used to evaluate each critical channel metrics we considered as part of our testing. The metrics and testing sequence are presented in the flow diagram illustrated in Figure 4.8. We also show the metrics' results for frequencies and ranges for IEEE802.11ax-based networks.

The International Telecommunications Union recommendation ITU-R P.1407-8 provides the basis for testing multipath propagation and channel measurements in this section [330]. As mentioned above, we also use NIST's Industrial Wireless testing work [58]. Fig 4.8 outlines a workflow of our testing process and steps.

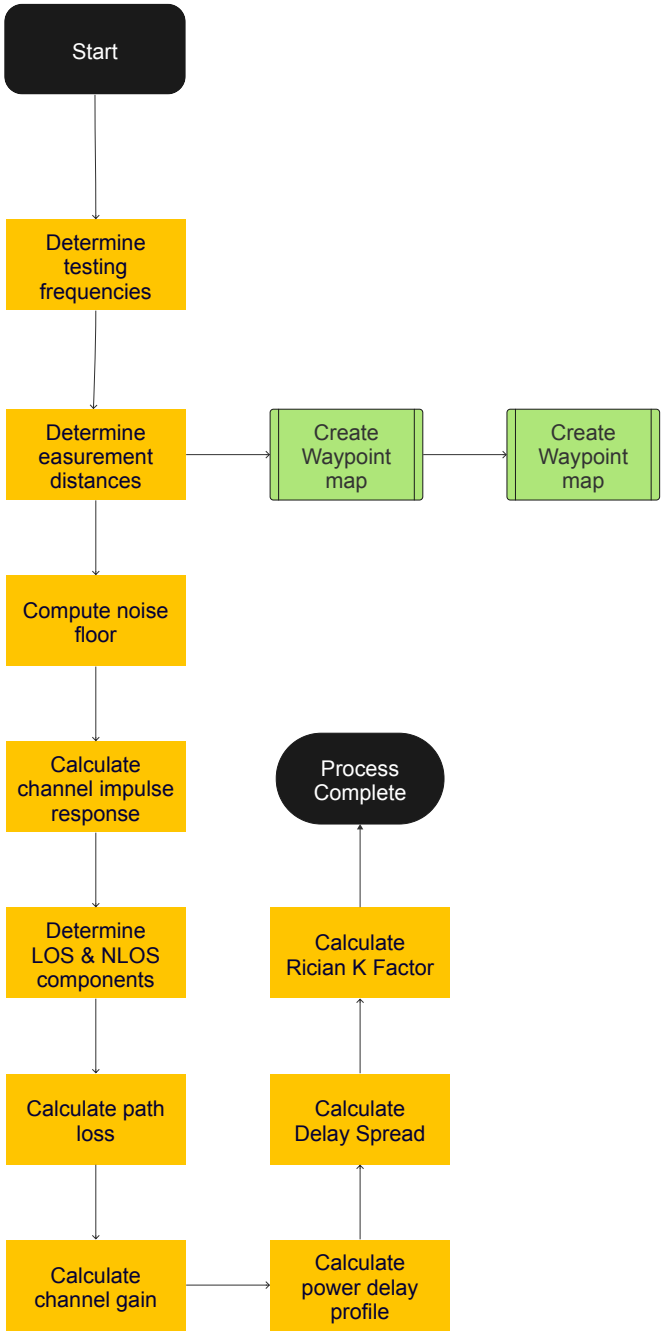


Figure **(4.8)** –RF measurement process flow diagram

4.4.1 Data Collection and Measurement Process

Our measurement testing collected data at fixed waypoints within the test area. We assessed the communication from fixed transmitting points (Tx) to fixed receiving points (Rx).

Several factors influenced our range selection criteria. Guidance was derived from previous authoritative studies conducted by NIST in the US. ETSI also provides illustrative European ranges based on various application scenarios and useful references [331]. Additionally, we visited IMR, conducted a factory inspection, and interviewed their engineers to discuss different configurations and setups, further validating our selected ranges.

The chosen ranges cover a range of manufacturing configurations possible for Bay 3 of IMR, encompassing multiple factories and flexible manufacturing layout scenarios. Each design covers an area measured in square meters (m^2). Therefore, we assume the range to be proportional to the square root of the area ($\sqrt{x}$). Data collection involved gathering data at each marked checkpoint along the test route. The checkpoints are illustrated in Figure 4.9, with red dots indicating their locations. The red box marks the position of the Tx. While the RX was mobile, the Tx remained stationary during measurements. We moved the RX in 1-meter increments during measurement. Raw measurement data is stored in the MATLAB measurement file format, organized in folders labelled by distance (e.g., 5m and 6m). Each folder contains measurement files ($.mat$), which include metadata, physical parameters, and sounding data.

The measurement runs required the assistance of two individuals. One person moved the RX test rig and aligned it with the markings, while another triggered the test from the Tx and organized the results into the respective files and folders.

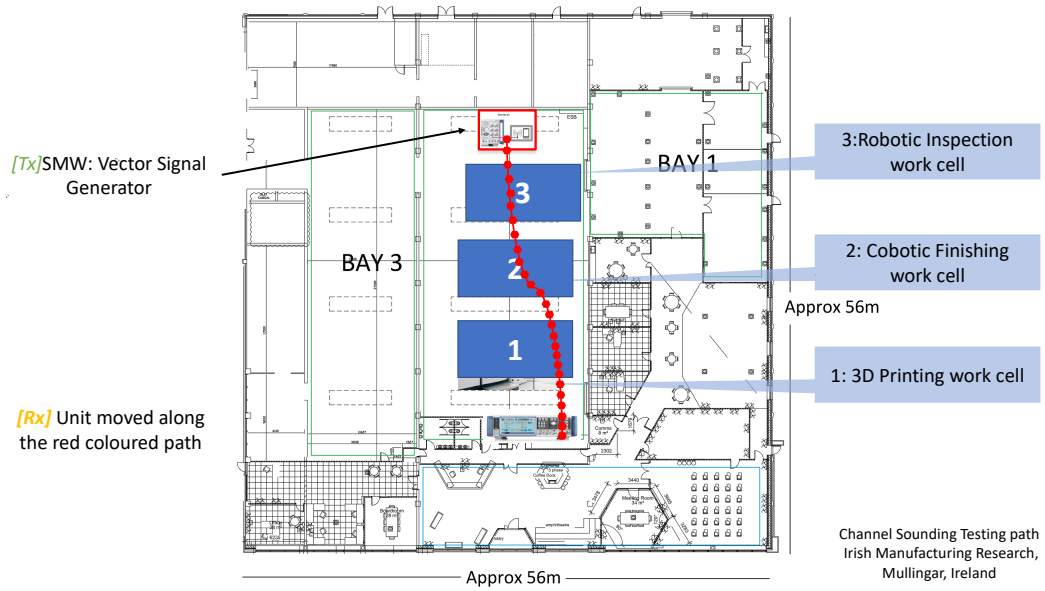


Figure **(4.9)** –RF sounding test route and waypoints

4.4.2 Channel Sounding Waveform Selection

We selected *maximal-length sequences* (M-sequences) for our channel-sounding waveform testing. M-sequences are pseudorandom binary sequences used in channel sounding for Wi-Fi and similar WLAN systems. They are generated using a linear feedback shift register (LFSR) circuit, with the sequence length being 2^{N-1}, where N is the number of stages in the LFSR circuit.

M-sequences offer autocorrelation properties, ensuring low correlation between a sequence and its delayed version, except at a specific delay corresponding to the sequence's length. This characteristic is crucial for channel sounding, enabling

the receiver to distinguish between the transmitted signal and any reflections or multipath components.

M-sequences provide a known reference signal from the Tx to the RX for Wi-Fi channel sounding. The RX correlates the received signal with the reference signal to estimate the channel response. The variation in delay between the transmitted and received signals allows for channel impulse response estimation. Furthermore, the information extracted provides insights into channel characteristics, such as delay spread and frequency response. M-sequences have a low peak-to-average power ratio (PAPR), making them well-suited for wireless communication systems that efficiently utilize available bandwidth and power.

4.4.3 Calculations

This section details the calculations used to process the data from the sounding testing. The calculations are derived from the ITU recommendations on *Multipath propagation and parametrisation of its characteristics* [330]. The calculations were coded in MATLAB, and the code is available in Appendix.

4.4.3.1 Channel Impulse Response calculations

The first measurements we determine are that of the Noise floor N and Channel Input Response c_m.

The noise floor is given as the average power of the noise present over a specific time window duration T. The square of the received signal $c(t)$ is captured at point t, providing the signal's power. The power values are summed over the

entire time window, then divided by the time window duration, providing the average value and thus the noise floor. It can be expressed as:

$$N = (1/T) * \sum |c(t)|^2, t = 0 to T \tag{4.1}$$

or

$$N = \frac{1}{T} \sum_{t=0}^{T} |c(t))|^2 \tag{4.2}$$

The noise floor thresholds are set at $10dB$ above the noise floor. The peak power threshold is 20 dB from the peak power, per the ITU recommendations [330]. These thresholds provide the range $c_m$in which samples are collected and calculated. The noise floor N was auto-generated from the R&S FSW.

Our system collects samples between the ranges of the calculated 10 dB above the noise floor and inside the 30 dB bounds of the CIR peak power. Upon calculating N, a *modified* CIR c_m is computed for the values between N and the peak of $c(t)$, denoted by $\tilde{c}(t)$, and calculated as:

$$\mathrm{c}_m = \begin{cases} c(t), & |c(t)|^2 \geq N_1 \quad and \quad |c(t)|^2 \geq P_2 \left|\tilde{c}(t)\right|^2 \\ 0, & else \end{cases} \tag{4.3}$$

where:

c_m : Channel Impulse response meeting within thresholds

$c(t)$: Denotes the real or complex-valued CIR

N_1 : Denotes the noise floor thresholds

P_2 : Denotes peak power threshold

$\tilde{c}(t)$: Peak of c_t

N : Computed noise floor

Algorithm 1 CIR data sampling algorithm

procedure SELECTCIRSAMP(r, cir)
  $k \leftarrow []$
  $nf \leftarrow$ NaN
  $cir1 \leftarrow$ NaN
  $pk_pwr \leftarrow$ NaN
  if $r < 3$ **then**
    return
  end if
  $pk_pwr \leftarrow 10\log_{10}(|\max(cir)|^2)$
  $nft \leftarrow 10$
  $pkt \leftarrow 1/1000.0$
  $cir \leftarrow cir(1 : \lfloor 0.8 \cdot \text{length}(cir) \rfloor)$
  $cir_mag2 \leftarrow (|cir|^2)/\max(|cir|^2)$
  $nf \leftarrow \text{mean}(cir_mag2(\lfloor 0.8 \cdot \text{length}(cir) \rfloor : \lfloor 1.0 \cdot \text{length}(cir) \rfloor))$
  $k \leftarrow \{i \mid (cir_mag2(i) > nf \cdot nft) \wedge (cir_mag2(i) > pkt)\}$
  $cir1 \leftarrow 0$
  $cir1(k) \leftarrow cir(k)$
  return k, nf, $cir1$, pk_pwr
end procedure

4.4.3.2 Line of Sight Calculation

Signal transmission can occur in one of two modes: Line-of-Sight *(LOS)* transmission, where the signal travels in a straight path between nodes, and non-line-of-sight *(NLOS)* transmission, where the signal path is obstructed by obstacles causing reflections or refractions [332].

The path between nodes is considered to be *LOS* if the magnitude of the first peak is less than the magnitudes of subsequent peaks. Given the collected sample set $c(t)$, we represent the first peak as $\tilde{c}_1(t)$. We define the identifier C to be

either *LOS* or *NLOS* by assigning 1 to *LOS* values equaling $\tilde{c}(t)$, and -1 to *NLOS* values.

$$C_{LOS} = \begin{cases} 1, & \text{if } \max(|\tilde{c}(t)|) = |\tilde{c_1}(t)| \\ -1, & \text{otherwise} \end{cases} \tag{4.4}$$

Algorithmically, this is expressed as:

Algorithm 2 Identification of a Line-of-Sight Scenario

Require: $\tilde{c}(t)$: Received signal at time t

Require: $\tilde{c_1}(t)$: Reference signal assumed to be present in a LOS scenario

Ensure: C_{LOS}: Identification of a LOS scenario

1: Find the maximum magnitude of the received signal, denoted as $max(|\tilde{c}(t)|)$.

2: **if** $max(|\tilde{c}(t)|) = |\tilde{c_1}(t)|$ **then**

3: Set $C_{LOS} = 1$.

4: **else**

5: Set $C_{LOS} = -1$.

6: **end if**

7: Output the value of C_{LOS}.

4.4.3.3 Channel gain calculations

Channel gain information can be used to improve a system's multiplexing gain, and sending data to multiple receivers simultaneously is a crucial part of the measurement process [333].

$$(\gamma) = 10\ log \sum_{t=0}^{T} |c_m|^2 - G_{\boldsymbol{Tx}}\ (dB) - G_{Rx}(dB), \tag{4.5}$$

where:

γ	= is the power gain in dB
$\sum_{t=0}^{T} \lvert c_m \rvert^2$	= the sum of the squared magnitudes of the transmitted signals over time
G_{Tx}	= transmitter antenna gain in dB
G_{Rx}	= transmitter antenna gain in dB

4.4.3.4 Path Loss Calculation

Path loss is a fundamental concept in wireless communications, representing the reduction in signal strength as it travels through the environment from the transmitter to the receiver [334]. It is denoted by PL and measures the attenuation of a propagating electromagnetic signal in decibels (dB). The distance between the transmitter and receiver antennas is measured at 1-meter intervals along the Euclidean distance, with f representing the signal frequency in Hz. The channel gain at each point is marked on the map in Fig. 4.3.

Mathematically, path loss is expressed as:

$$PL(dB) = P_{\text{tx}}(dBm) - G_{\text{Tx}}(dBi) - G_{\text{Rx}}(dBi) - G(dB) \tag{4.6}$$

where:

PL = Path loss in dB

G_{Tx} = Transmitter antenna gain in dBi

G_{Rx} = Receiver antenna gain in dBi

$G(dB)$ = Other power gains in dB

$G(dB)$ is a catch all terms tat accounts for other gains that are not directly attriubutable to transmitter power of antenna gains.

This path loss formula is essential for quantifying the signal attenuation as a wireless signal propagates through various mediums, such as walls, pillars, or machinery. By understanding the path loss characteristics of a wireless channel, it is possible to estimate the expected signal strength and quality at a given distance between the transmitter and receiver. Path loss parameters vary significantly depending on the propagation environment, such as rural versus urban areas, environmental mobility, and carrier frequency [335]. Therefore, a solid understanding of path loss is crucial for characterizing the propagation environment [336].

4.4.3.5 Power Delay Profile

In wireless communications, signals can be transmitted from a transmitter to receivers via multiple paths, resulting in variable signal travel distances due to reflections or obstructions by obstacles. The difference in propagation time between the longest and shortest paths is known as the "delay" and is a critical parameter in many communication systems' performance metrics.

The Power Delay Profile (PDP) is a modelling technique for characterizing multipath channels. It illustrates the signal power for each multipath component against their propagation delays. PDP plots are often generated as the spatial

average of the Channel Impulse Response (CIR). The power delay profile equation is given by:

$$PDP = \sum_{i=1}^{N} |(c_m)_i(t)|^2 \tag{4.7}$$

where:

PDP = Power Delay Profile

N = Number of delay or multipath components

$(c_m)_i(t)$ = CIR value at the time corresponding to the i^{th} delay path at time t

Delay spread, denoted as S, measures the dispersion of the impulse response. It is a valuable metric for understanding signal propagation characteristics, especially in digital receiver design and transmission reliability prediction.

Two essential parameters for characterizing the frequency channel derived from the PDP are the "mean delay" and the "RMS delay spread." The mean delay ($\bar{\tau}$) is the power-weighted average of the excess delays measured by the test sequences, and it is calculated as:

$$\bar{\tau} = \frac{\sum_{t=0}^{T} t \left|c_{m(t)}\right|^2}{\sum_{t=0}^{T} |c_m(t)|^2} \tag{4.8}$$

The RMS delay spread (τ_{rms}) quantifies the variability of the mean delay and is calculated as:

$$\tau_{rms} = \sqrt{\frac{\sum_{t=0}^{T} (t-\bar{\tau})^2 \left|c_{m(t)}\right|^2}{\sum_{t=0}^{T} |c_m(t)|^2}} \tag{4.9}$$

4.4.3.6 Rician k-Factor calculation

The Rician channel model is commonly used to characterise wireless communication channels. The Rician K factor, expressed as the ratio of direct-path and scattered paths, assesses link quality [337]. Modern wireless communication systems such as Wi-Fi are designed to adapt their transmission parameters dynamically. However, their adaption is typically predicated on the use of channel statistics. Rician K-factor is one of those statistics and impacts spectral efficiency, bit error rate and fade rates. These factors significantly affect the performance of wireless communication systems, especially ones requiring the highest performance possible, such as industrial wireless networks. Mukherjee et al. outline the empirical models can vary significantly from real-world deployments and illustrate the impact can impact the capacity of a channel by 13% [338]. The Rician model simulates both Line of Sight (LOS) and Non-Line of Sight(NLOS) components between transmitter and receiver. This channel model implements real-time fading observed in a wireless communication system.

The Rician K-Factor, K, is the power ratio between the LOS and scattered components and can be expressed as:

$$K = \frac{P_{LOS}}{P_{LOS} + P_{NLOS}} \tag{4.10}$$

where:

K = Rician K factor

P_{LOS} = is the power of the LOS signal

P_{NLOS} = is the power of the NLOS signal

The Rician K factor can be further extrapolated as:

$$K_dB = 10\ log \frac{\hat{x_1^2}(t)}{\frac{1}{I-1}\sum_{i=2}^{I} \hat{x_1^2}(t)} \tag{4.11}$$

where:

K_dB	= Rician K Factor in decibels (dB)
$c_1(t)$	= power of the line-of-sight component of the received signal at time t
$\sum_{i=2}^{I} \hat{c_i^2}(t))$	= total power of the scattered components of the received signal at time t
I	= total number of scattered components in the received signal

4.5 Radio Propagation Test Results

Wi-Fi 6E has introduced the use of the 6 GHz spectrum. Our testing focuses on this spectrum, which is still in the early adoption stage. Thus, the body of knowledge is developing compared to the traditional Wi-Fi frequency bands of 2.4 GHz and 5 GHz. The 2.4 GHz frequency band is heavily utilized, resulting in co-channel interference, leading to its reference as 'garbage'. Similarly, the 5 GHz frequency band is also subject to interference [339]. We focus our testing on newer spaces with less congestion and less interference, a vital advantage of the 6 GHz spectrum. Furthermore, given the recent release of 6 GHz to the community from telecommunications regulators, there is a need for analysis of the use of this spectrum in a range of application areas, such as wireless industrial networks.

Table 4.2 presents a comprehensive list of the parameters, values, and measurement units utilized in the testing process. The table includes the carrier frequency, antenna configuration, and the sequence type filename used for testing.

Parameters	**Values**	**Units**
Center Frequency	6000	Megahertz (MHz)
Transmitter Clock Rate	160	Megahertz (MHz)
Receiver Sample Rate	200	Megahertz (MHz)
Sequence Type	PN_16_bit.mat	Pseudo Noise (16 bit)
Sequence Length	65535	Bits
CIR Update Rate	409.59	Microseconds (μs)
Echo Resolution	6.25	Nanoseconds (ns)
Measurement Type	Triggered	

Table **(4.2)** –Test parameters, values, and units

4.5.1 Channel impulse response

The channel impulse response (CIR) diagram illustrated in Fig. 4.10 visualises the response of the communication channel to an impulse signal from our sounding system detailed in 4.3. The graph shows the magnitude of the response shown in decibels (dB) and the phase of the channel's frequency response as a function of time and is generated from the triggered sequence used during the testing process. Provides valuable information about the characteristics of the communication channel. The diagram and associated data are derived from the IQ data files generated by the sounding system.

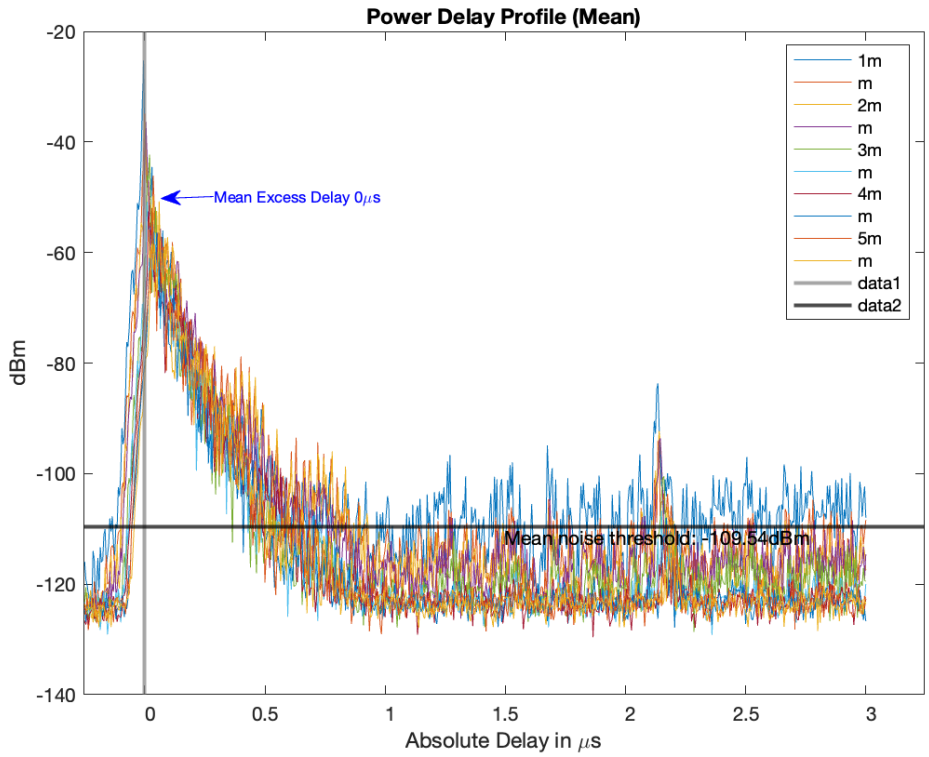


Figure **(4.10)** –Mean Channel impulse response for 1-10m at IMR

The mean excess delay and noise threshold are important parameters derived from the channel impulse response (CIR) diagram. These parameters provide critical information about the vital channel for designing communication systems. Mean excess delay represents the average delay between the arrival of the direct signal and the appearance of the scattered signals. It is the average time for the different paths the signal can take to reach the receiver. Mean excess delay determines the maximum in the system without causing inter-symbol interference (ISI). If the symbol rate is too high, the different paths can interfere with each other, distorting the signal. Typical values of mean excess delay are specific to different environments; in industrial settings, typical mean excess delay ranges from ns to

μs. Based on our observations, the data collected is consistent with typical excess delay values in industrial environments.

The noise threshold defines the minimum signal power required to overcome the noise in the channel. The minimum signal power is needed to achieve a specific signal-to-noise ratio (SNR) at the receiver. This parameter is important because it helps to determine the maximum distance over which a signal can be transmitted without being degraded by noise. If the signal power is below the noise threshold, the signal will be lost in the noise. The CIR diagram illustrates the mean values of collected sounding tests at their respective distances. The mean noise threshold is recorded at $-109.54dBm$. Typical indoor environments are usually around -90 dBm; therefore, the noise environment could be moderately noisy. However, industrial environments with widely varying noise thresholds due to heavy machinery, high voltage or specialised industrial equipment. have noise thresholds between $(-70dBm - 110dBm)$.

4.5.2 Channel Gain and Path Loss

Channel gain and path loss are other metrics that can significantly impact the performance of wireless communication systems. The channel gain represents the ratio of received signal power to the transmitted signal power, while the path loss represents the attenuation of the signal power over distance. Channel gain is the reciprocal of path loss. Due to obstacles, reflections, and blockages, industrial environments are challenging for wireless communication systems. These factors can lead to significant path loss and variations in channel gain over distance. For example, in a typical manufacturing facility, the channel gain can vary by up

to $30dB$ over a distance of 10m due to signal reflections and blockages caused by metal structures and equipment. Path loss is concerned with signal loss over distance and is also sensitive to distance, interference, and obstacles. The results of the channel gain calculations are outlined in Table 4.3.

Distance (m)	**Min Gain (dB)**	**Max Gain (dB)**	**Mean Gain (dB)**
1	-50.73	-50.72	-50.72
2	-56.71	-56.55	-56.62
3	-59.05	-58.91	-58.99
4	-59.93	-59.91	-59.93
5	-61.44	-61.42	-61.43
6	-63.15	-63.14	-63.14
7	-65.13	-65.12	-65.12
8	-67.82	-67.79	-67.81
9	-68.88	-68.82	-68.84
10	-67.31	-67.29	-67.30
11	-65.90	-65.89	-65.90
12	-69.49	-69.46	-69.48
13	-68.36	-68.35	-68.35
14	-73.22	-73.19	-73.20
15	-70.36	-70.35	-70.35
16	-70.64	-70.61	-70.62
17	-71.31	-71.22	-71.25
18	-73.56	-73.32	-73.49
19	-77.11	-76.27	-76.68
20	-77.67	-77.24	-77.42
21	-72.36	-72.31	-72.34
22	-72.23	-72.15	-72.19
23	-74.99	-74.81	-74.89
24	-74.57	-74.49	-74.52
25	-77.58	-76.96	-77.26

Table (4.3) –Gain Data for a 6 GHz Wireless Industrial Network

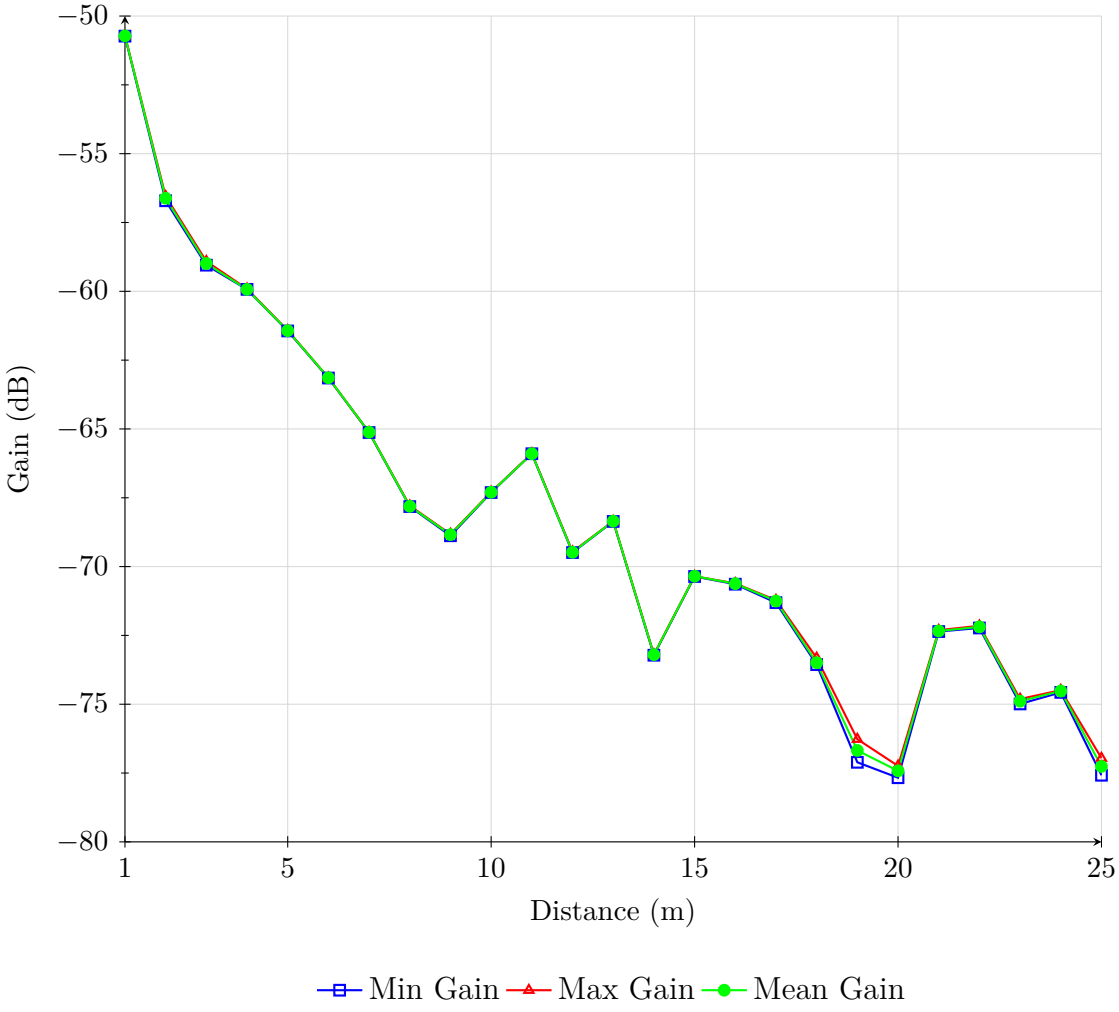


Figure **(4.11)** –Plot of gain versus distance

4.5.2.1 Observations

In Figure 4.11, the gain is plotted against the distance, and it is noteworthy that the similarity between the Min Gain, Max Gain, and mean gain is very close. This indicates that the variation in the gain values across the measurements is small, highlighting the channel's behaviour is stable and predictable. This consistency is a valuable feature for wireless industrial networks as it implies the signal strength

is uniform across the measurements. It can also strongly indicate a predictable network, vital for a wireless industrial network.

When the distance between the transmitter and the receiver goes from 1 to 25 meters, the mean gain decreases from -50.72 dB to -77.26 dB. This shows that the signal strength reduces with increased distance, which is typical due to the propagation loss. The data on signal gain shows inconsistencies at different distances. At 10 meters, the mean gain measures -67.30 dB, but it drops to -69.48 dB at 12 meters before rising to -68.35 dB at 13 meters. This pattern indicates that the layout and obstacles in the industrial environment heavily impact signal propagation. These findings have important implications for a 6 GHz wireless industrial network.

4.5.2.2 Implications

- **Path Loss Models and Network Planning**: It is crucial to model path loss accurately when planning a network at 6 GHz due to the decrease in mean gain with distance. Higher-frequency signals like 6 GHz experience more significant path loss than lower frequencies like 2.4 GHz and 5 GHz. This means 6GHz signals weaken more rapidly over distance and are more susceptible to obstacles. A recommendation to network designers **must consider the 6 GHz band's path loss models specific to the industrial environment to ensure the facility receives sufficient signal strength**.
- **Obstacle-Aware Network Design**: The fluctuations in the gain data also emphasise the need for an obstacle-aware network design. Careful

consideration should be given to positioning APs, antennas, and network devices with the obstacles present in the industrial environment. This can minimise the impact of obstacles on signal propagation and ensure reliable communication.

- **Path Loss Models and Network Planning**: It is crucial to model path loss accurately when planning a network at 6 GHz due to the decrease in mean gain with distance. Higher-frequency signals like 6 GHz experience more significant path loss than lower frequencies like 2.4 GHz and 5 GHz. A recommendation to network designers **must consider the 6 GHz band's path loss models specific to the industrial environment to ensure the facility receives sufficient signal strength**.
- **Adaptive Transmit Power Control**: Given the fluctuations in gain data, adaptive transmit power control techniques may be beneficial in optimising network performance. The network can maintain a reliable communication link by dynamically adjusting the transmit power based on channel conditions while minimising interference and conserving energy.

Path loss in industrial environments can also be high, particularly at higher frequencies. For example, in a typical oil and gas refinery, the path loss at 5 GHz can be as high as 140 dB over 100 meters due to signal attenuation and reflection from metal structures. Similarly, in a mining environment, the path loss at 2.4 GHz can be as high as 100 dB over 50 meters due to obstacles and signal blockages.

4.5.2.3 Observations

- **Increasing Path Loss with Distance:** Generally, as the distance increases, the path loss also increases, which is consistent with the behaviour of wireless communication systems. However, there are some fluctuations in the path loss values, likely due to obstructions or environmental multipath effects. There are local minima in path loss values, such as at distances 8m and 9m, and local maxima at distances 13 m and 18 m. However, these variations, such as the equipment illustrated in Figure x, cannot be discounted; they could also be due to specific environmental conditions at those distances, such as obstacles or changes in the propagation medium.
- **Fluctuations in Path Loss:** The path loss values do not show a consistent trend, such as a smooth increase or decrease with distance. This inconsistency may be due to various obstacles, reflecting surfaces, and multipath effects in the industrial environment, affecting the propagation of the wireless signal.

4.5.2.4 Implications and Recommendations

- **Network Planning:** A general theme of this work is the criticality of network planning when designing and deploying a wireless network in an industrial environment; it is crucial to account for the varying path loss values and their effect on communication performance. Proper planning and site surveys can help identify the optimal locations for access points and wireless devices to ensure reliable and robust communication.
- **Adaptive Modulation and Coding:** Due to the fluctuations in path loss values, it is recommended to use adaptive modulation and coding schemes

to optimise the communication system's performance. Adaptive techniques can adjust the modulation and coding rates based on the current path loss conditions, enhancing the network's ability to adapt to varying channel conditions.

- **Periodic Monitoring and Optimization:** Given the dynamic nature of industrial environments, performing periodic monitoring and optimisation of the wireless network is essential. Regular assessments can help identify changes in the path loss profile and adjust the network configuration accordingly, ensuring optimal performance and reliability.
- **Robustness to Environmental Changes:** Industrial environments can be prone to significant changes, such as moving large equipment or adding new infrastructure. Designing a robust wireless network for these environmental changes is critical to maintaining reliable communication and minimising the need for frequent network adjustments.

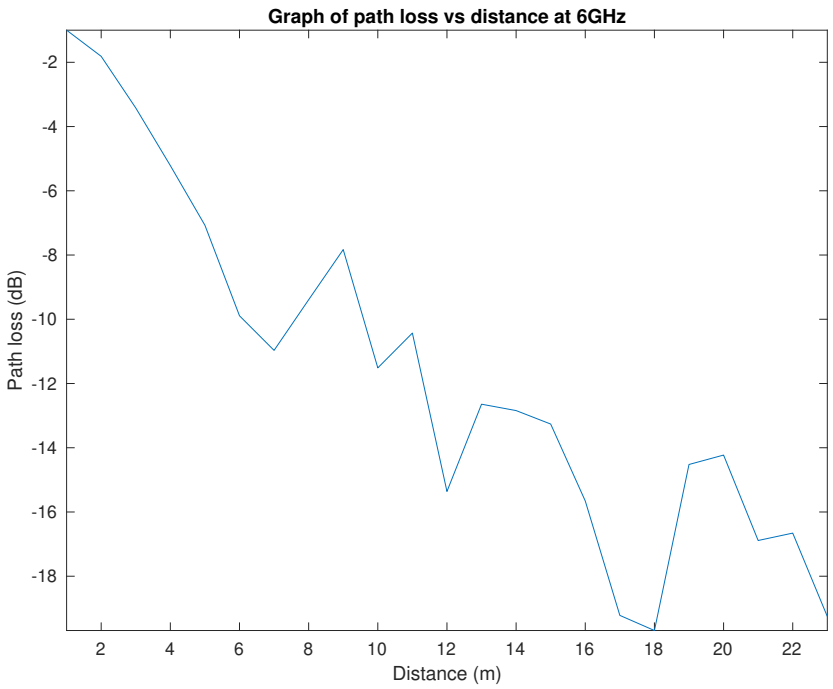


Figure **(4.12)** –Path Loss diagram for IMR

4.5.3 Delay Spread and Power Delay Profile

Delay spread and power delay profile are vital parameters to characterise the wireless channel. Delay spread refers to the time delay between the arrival of a radio signal's first and last signal component at a receiver. Numerous factors delay the transmitted signal's time, including multi-path propagation, reflection, diffraction, and signal scattering. Delay spread is derived from the channel's impulse response testing by the triggered sequence response process. A high delay spread indicates a highly dispersive channel, which means multiple paths of the propagation of the signal cause delays. These paths are caused by reflection and refraction from environmental objects, causing different path lengths and signal strengths for each path. These different paths will arrive at the receiver with

Distance (m)	Path Loss (dB)
3	-1.814363295
4	-3.421387347
5	-5.215618123
6	-7.073072847
7	-9.891353997
8	-10.96851721
9	-9.392461986
10	-7.830829546
11	-11.5129819
12	-10.42962455
13	-15.3607794
14	-12.64412227
15	-12.84289671
16	-13.26224913
17	-15.6569998
18	-19.21909157
19	-19.68997905
20	-14.52104478
21	-14.22794049
22	-16.88767062
23	-16.65723891
24	-19.25154442
25	-19.98784361

Table **(4.4)** –Path Loss Data for IMR at 6 GHz

different phases, amplitudes and arrival times. This presents challenges for the receiver, which has to distinguish between the signal from the multiple reflections and noise.

Industrial environments are typically highly dispersive, where the signal bounces off walls and floors, and a wide variety of large (and often metallic) objects is every day. The delay spread in industrial environments can be significant, sometimes in the region of μs and ms.

The practical application of understanding the delay spread and PDP can help determine a range of optimisation techniques ranging from placement of devices and antenna types to adopting different modulation and coding techniques as

countermeasures to the delay characteristics of the environment. The numbers are detailed in Table 4.5

Distance	RMS Delay Spread	Max Excess Delay	Min Excess Delay	Mean Excess Delay
3	9.17	20	5	4.97
4	9.48	25	10	10.7
5	10.5	30	10	12.5
6	11	35	15	16.9
7	12.1	30	15	17.6
8	15.2	40	20	24.8
9	17.3	35	25	28.3
10	14.9	50	30	31.2
11	13.7	50	30	30.9
12	18	60	35	37.3
13	16.9	55	35	38.6
14	24.4	80	40	47
15	17.5	50	45	46.9
16	16.9	55	50	53.1
17	17.2	70	50	55.9
18	23.9	85	55	63
19	31.3	85	55	68.6
20	29	90	60	72.9
21	19.3	90	65	71.4
22	18.4	90	65	69.9
23	23.3	95	75	80
24	21.4	90	75	79.7
25	26.4	105	75	85

Table (4.5) –Measurement data for various distances

The power delay profile *(PDP)* represents the relative power levels of the signal components arriving at a receiver as a function of time delay. It provides further information about the characteristics of the radio channel, such as the number of signal paths, the path loss, and the delay spread. PDP is also obtained using the channel sounding system by measuring the signal's power at different time delays.

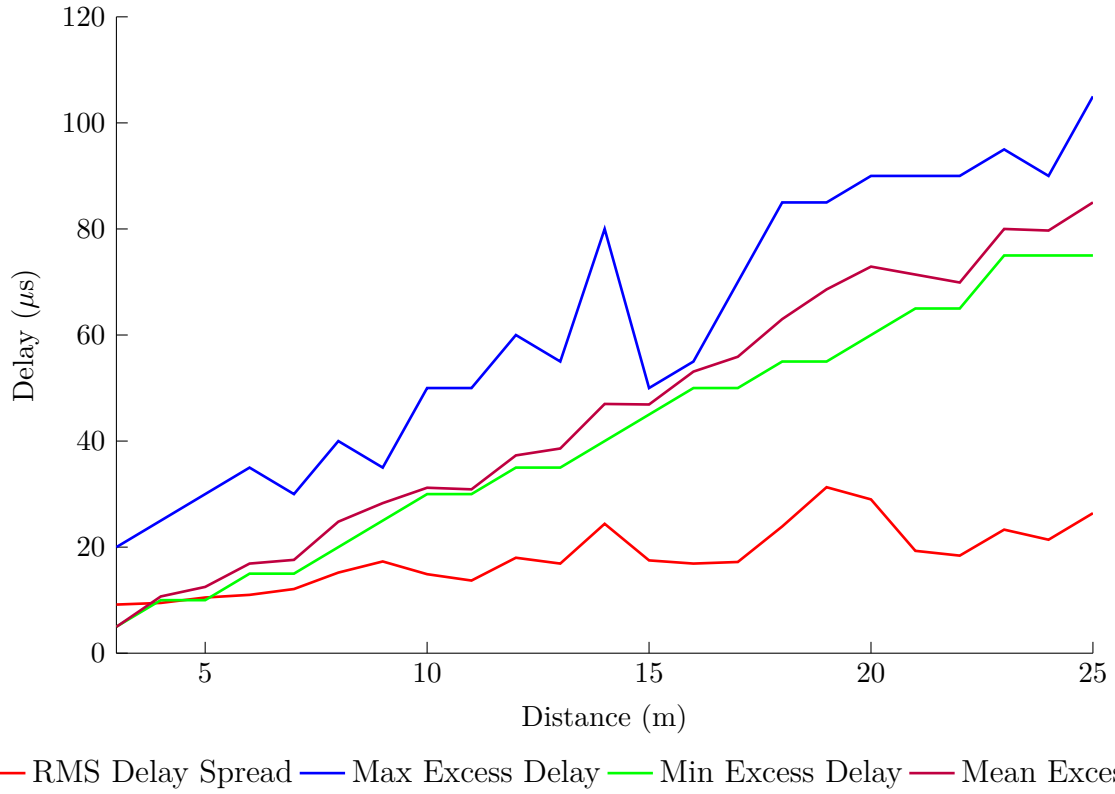


Figure **(4.13)** –Delay measured from the experimental set-up

4.5.3.1 Observations

The RMS Delay Spread exhibits a clear upward trend as the distance between the transmitter and receiver increases from 1m to 25m, reaching 9.17 and 26.4, respectively. This data implies that the channel dispersion worsens with distance, leading to more significant ISI effects.

The Maximum Excess Delay behaves differently from the RMS Delay Spread. It does not follow a linear pattern with distance and varies as the distance increases. At a 7m distance, it is 30. However, at 14m, it increases to 80 before dropping to 50 at 15m, firmly pointing out that the longest delay paths are affected by

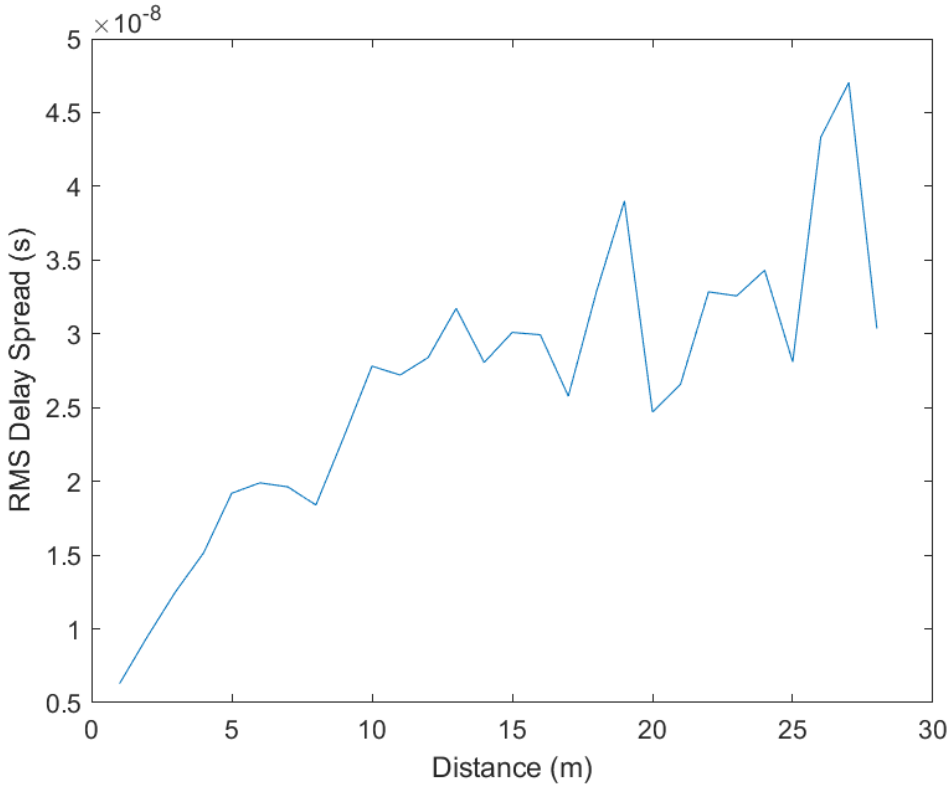


Figure **(4.14)** –Delay spread calculations for IMR

the layout and obstacles in the industrial environment. Therefore, a personalised channel-sounding analysis is necessary instead of standard models.

The mean excess delay similarly experiences a noticeable increase from 4.97 to 85 as the distance between the transmitter and receiver increases from 1m to 25m, and indicates that the average delay experienced by the signal components grows with distance, thereby underscoring the importance of carefully considering this variable in any wireless communication system design.

4.5.3.2 Implications

- **Line-of-Sight (LoS) Communication**: The 6 GHz band has a higher frequency and smaller wavelength than the 2.4 GHz and 5 GHz bands, which can result in weaker penetration capabilities through obstacles. Maintaining a clear line-of-sight (LOS) between the transmitter and receiver is crucial for reducing the impact of multipath propagation and signal attenuation, as evidenced by the increasing RMS Delay Spread and fluctuating Maximum Excess Delay in the data. Therefore, placing APs in LoS locations is even more critical at the 6GHz band.
- **Access Point Density**: Given the complex channel characteristics at 6 GHz and the increasing RMS delay spread with distance, deploying a higher density of access points would be advisable in industrial facilities to ensure reliable communication. This can help mitigate the increased signal dispersion and potential for ISI at greater distances.
- **Dynamic Beamforming and Beam Steering**: Considering the fluctuating maximum excess delay with distance, dynamic beamforming and beam steering techniques become critical for 6 GHz-based wireless industrial networks. By directing the radio signals towards the intended receivers and adjusting the beams in real-time, it is possible to adapt to the changing channel conditions and improve signal quality and network performance.

4.5.4 Multipath fading and Rician K factor

Multipath fading occurs when signals are transmissions from a transmitter to a receiver and experience multiple reflections, diffractions, and scattering from objects in the environment. Multipath fading is the variation of the signal strength due to the constructive and destructive interference of the signal paths. Rician fading is a multipath fading phenomenon when a dominant line-of-sight (LOS) component is present along with scattered components. The Rician K factor is a parameter that characterises the strength of the LOS component relative to the scattered components. It is defined as the ratio of the power in the LOS component to the power in the scattered components.

In industrial settings, there are often multiple reflective surfaces. The Ricain K factor is a valuable tool for determining the direct line of sight (LOS) and interference caused by reflected signals. Since multipath reflections can cause interference, it is crucial to know these values when designing communication systems.

We use the equation in 4.4.3.2 to determine the LOS and NLOS components. The LOS path indicates the direct path between TX and RX, with no obstructions, whereas an NLOS path will have reflections or obstacles between the TX and RX. Expected K factor values for LOS range from 0 to 12, and NLOS can range from 1 to 50. The results we captured from our testing in IMR are displayed in table 4.6.

Distance	K-factor(LoS)
3	NaN
4	NaN
5	11.79
6	11.67
7	15.95
8	6.96
9	16.32
10	8.43
11	12.67
12	12.21
13	9.67
14	8.66
15	NaN
16	15.44
17	7.63
18	6.77
19	9.61
20	3.57
21	14.87
22	13.39
23	2.95
24	7.16
25	6.27

Table (4.6) –Summary Statistics for K-Factor results

We use a methodology that combines physical transmission simulation with impulse signals, modulated to fit WiFi standards. This allows us to approximate the

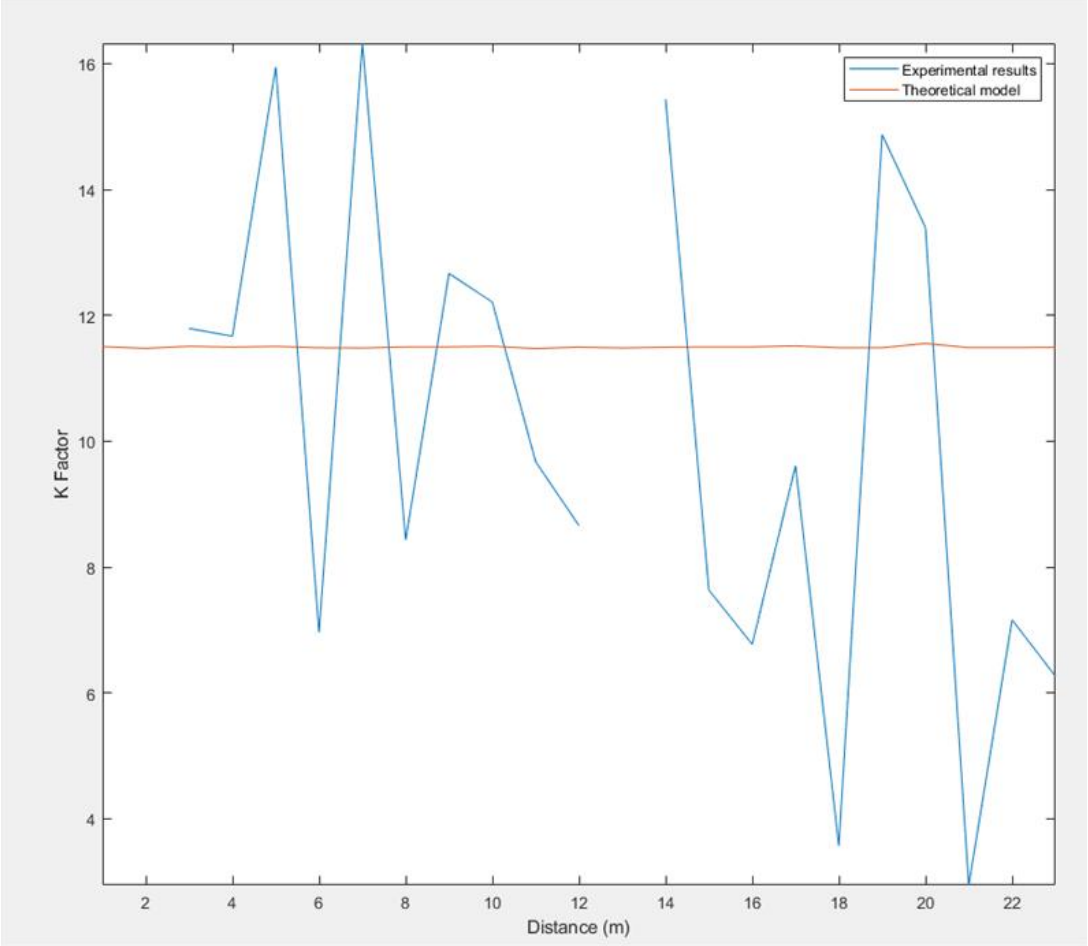


Figure **(4.15)** –K-factor chart for IMR

complex reality of industrial settings closely. By applying this signal through a simulated model, we plot a series of theoretical K factors, as seen in Figure 4.15.

Our empirical K factor data, which we collected at IMR, precisely quantifies the line-of-sight (LOS) versus non-LOS (NLOS) propagation components.

As shown in Figure 4.15, there are significant differences between the simulated values and empirical data, highlighting the variation between simulated K factor values and empirical data. Whereas the simulated data is approximately consistent

at 11.5dB, the empirical data exhibits much greater variability. This difference further illustrates the variation between standard theoretical values and actual data recorded from our field tests.

Upon analyzing the K-factor data collected, we observed that some values were marked as NaN (Not a Number). These NaN values occur during a divide-by-zero condition during the K-factor calculation. When the K-factor approaches infinity, the Line of Sight (LOS) component dominates over the multipath components, and the scattered or multipath components tend to have zero power. In contrast, the LOS component's power remains finite and non-zero.

We can attribute these effects to two factors. Firstly, highly directional antennas enhance the direct LOS path between the transmitter and receiver while suppressing the multipath signals, resulting in the K-factor approaching infinity. Secondly, when the transmitter and receiver are located close to each other, the LOS component can be significantly stronger than the scattered or multipath components.

4.5.4.1 Observations

- **Line-of-Sight (LoS) Dominance:** Missing values (NaN) occur at distances 3, 4, and 15, which can be attributed to obstructions in the Fresnel zone. The Fresnel zone is a critical region where the radio signal's path encounters obstructions that cause an almost infinite path loss, making it impossible to calculate the K-factor. Nevertheless, higher K-factor values (e.g., 16.32 at 9m and 15.95 at 7m) indicate stronger LoS components in the wireless

channel, which can lead to better communication performance at those distances.

- **Multipath Effects:** The K-factor values generally fluctuate across the range of distances, indicating that the propagation environment experiences varying multipath effects. Lower K-factor values (e.g., 2.95 at 23m and 3.57 at 20m) reveal weaker LoS components and the dominance of multipath effects. These conditions may result in more significant signal degradation and decreased communication performance.

4.5.4.2 Implications

- **Network Design:** Identifying areas with higher K-factor values can help strategically place critical wireless devices in industrial networks, ensuring reliable and robust communication links for time-sensitive and mission-critical applications. In industrial environments, prevalent physical obstructions will affect the communication link. Proper planning and placement of wireless devices can mitigate the impact of obstructions on the K-factor and overall network performance.
- **Multipath Models:** When designing and deploying communication systems for wireless industrial networks, it is essential to consider the varying multipath effects to enhance reliability and stability. Adaptive modulation and coding schemes can significantly improve the network's ability to withstand these fluctuations.
- **RF Mapping:** Mapping areas with lower K-factor values may be necessary. Given its dynamic nature, an argument could be made for conducting this

type of analysis periodically in an industrial environment. Additionally, countermeasures such as diversity schemes or equalisation can help mitigate potential reliability issues in the network.

4.6 Conclusion

In this chapter, we conducted RF propagation measurements in the frequency bands of the IEEE 802.11ax standard. These tests were performed at 6GHz frequency bands in Mullingar, Ireland, by the Irish Manufacturing Research team.

We also outlined a test and measurement architecture for radio-frequency propagation testing in industrial environments. Additionally, we described an analytical framework and associated algorithm for collecting industrial environments and computing RF propagation data, which can be used or extended in similar settings and frequencies.

Operating a communications system in industrial environments is challenging, especially with the highest performance and reliability standards. To meet such stringent requirements, operators must thoroughly understand the target environment. We tested the channel characteristics of a modern manufacturing environment at the IMR facility.

Our testing, conducted at the 6GHz frequency band, is essential in understanding the performance of the 802.11ax standard in industrial environments.

The analysis highlights the significance of conducting radio propagation testing for wireless industrial networks. The variations and disparities in industrial settings emphasise the need to design a wireless communication system that

caters specifically to the environment at hand to meet performance requirements. Our findings further emphasise utilising channel sounding in challenging RF environments.

In addition, when using the 6GHz frequency band, which has a higher frequency and shorter wavelength, it is imperative to design the network according to the specifics of this particular band. We suggest implementing technological approaches such as beam forming and transmission control strategies to significantly enhance the network's performance.

Chapter 5

Wi-Fi based industrial wireless network solution design

This chapter details the design and architecture of a new industrial IoT system. The systems design targets low-latency and high-reliability applications. However, the solution is extensible and reusable to address any application areas beyond industrial. The open, standards-based design means the system can be easily extended and repurposed for different applications. Numerous contributions are in this chapter:

- **Edge architecture**: We present a novel architecture for edge computing that enhances wireless communication between edge devices and the cloud by enabling efficient and reliable data processing and analytics at the edge. This architecture addresses critical challenges in wireless industrial networks and IoT, such as latency, bandwidth, and security. It has the potential

to improve the performance and efficiency of wireless industrial systems significantly.

- **Synthetic sensing**: The architecture also includes the design of a sensing device, which extends the field to synthetic sensing into industrial applications.
- **Interoperability framework**: We devise an interoperability protocol to facilitate seamless integration of newer edge devices with legacy systems without extensive modifications to the existing infrastructure, we propose a mechanism for converting data from the popular IoT protocols and builds upon the work of *Nolan and Kelly* in interoperability [340]. This approach improves the current interoperability and flexibility of industrial systems,
- **Novel database design**: We contribute to the Industrial IoT and Edge computing field with a unique database system that effectively extends the efficacy of the IEEE 1451.4 TEDS standard. This innovative solution is highly adaptable and can be used in various industries and applications, demonstrating remarkable versatility. Our database system provides a solid foundation for future research and advancements in Industrial IoT Edge computing by creating a comprehensive and flexible database system.
- **Open source implementation:** Finally, we detail an innovative open-source and highly adaptable system implementation leveraging the synergies of YAML and container-based technologies. This novel implementation enables users to remotely configure and fully customise their edge computing system and IIoT implementation, thereby helping to evolve the field into software-defined industrial functions virtualisation reality.

5.1 The evolution of Industrial computing

The continued digital transformation of industry and the growing adoption of the IIoT is impacting industrial systems design and implementation. The ongoing convergence of OT-IT technologies encourages using general-purpose and open-source technologies on the factory floor [341]. The transformation of industrial networking architectures from proprietary protocols to open standards makes exchanging data from different systems much more straightforward [342].

This interoperability, significantly enabled by the IIoT technologies, extends beyond the factory floor. It allows systems to be connected and shared globally, integrating supply and value chains in a real-time, interoperable fashion. The technological evolution of industrial systems from proprietary systems to open-source, standard protocols is vital to changes across the industry [343, 344, 345].

Across many industrial segments, traditional networking architectures use the client\server or poll-response patterns [346]. The architectures of industrial automation are evolving to adopt technologies which have become popular in the broader IoT. For example, the `pub/sub`-messaging and event-driven architectures are arguably the architecture pattern of choice for many IoT applications. `pub/sub`sub provides greater flexibility than client-server architectures. The migration towards the `pub/sub` sub is evident across various industries, and it will most likely be the architecture of choice for the foreseeable future.

Some of the more notable protocols include Message Queueing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP) and XMPP (Extensible Messaging and Presence Protocol). DDS (Data Distribution Service) and OPC-

UA time-sensitive networking (TSN) target time-critical or deterministic systems [347, 348]. While extensive, the latter two suffer from the perspective of being complex to implement [349, 350]. Given the breadth of options, which is the correct protocol to choose?

Today, many protocols are used to support data communication in industrial applications. Many popular protocols originated from automation equipment providers such as Allen-Bradley, Schneider, and Siemens and are proprietary. Many proprietary protocols, such as the HART protocol or Modbus, have become open. TCP\IP (Transmission Control Protocol) and IP (Internet Protocol) have become popular across industrial applications such as *PROFINET* and Modbus TCP/IP. Most legacy protocols have developed a mechanism for integrating IoT and IIoT base `pub/sub` sub and event-driven architectures.

One reason for this evolution is reduced communication complexity, as publishers and subscribers communicate via a broker. The reduction in point-to-point communications simplifies communication. Messages and push-based data delivery also lessen the need for polling across the system, which improves response times and message latency. Secondly, a broker decouples the relationship between publisher and subscriber. This feature enables heterogeneous devices to implement functionality independent of each other. This flexibility allows for easier change management and publishers and subscribers to develop and change functionality without cascading changes across the system. Finally, as industrial systems become more modular, flexible, and dynamic, the `pub/sub`sub model supports changes, upgrades, and reconfiguration with little or no overhead. New publishers can publish messages on a topic. A topic is a string that serves as a destination

idenitifer for messages. Topics are also used to categorize and route messages within MQTT messaging systems.

The Eclipse Foundation published a report in 2021 outlining MQTT as the fastest-growing protocol for Internet of Things applications [351]. Given its popularity in the broader IoT, MQTT would also be desirable for IIoT solutions. The data would support that position [352].

5.2 System Design and Architecture

The proposed system uses open-source, widely used technologies popular across many IoT applications. They contrast with many of the technologies traditionally used in industrial applications. We discuss using the MQTT messaging technology, specifically the Sparkplug framework [353]. We outline why Sparkplug balances scale and definition, enabling flexibility for publishers and clients. This aspect of interoperability is essential in industrial applications, as the decoupling of publishers and subscribers makes integrating between different suppliers and systems much more effortless. This interoperability defines the promise of the IIoT.

We also discuss container technologies and their benefits in scaling and building modular-based systems, enabling end-users enhanced flexibility in operating and managing such architectures. In addition, the application of event-drive architectures enables a system to evolve and scale, which historically has been a significant challenge in industrial applications. Also, containers allow much more significant heterogeneity and choice of application, enabling applications to operate on the

same hardware and systems, which traditionally have been single vendors and challenging to operate and manage.

5.2.1 Event driven Architecture technologies: MQTT and Sparkplug

One of the key criticisms of OPC-UA has been the complexity of integration of OPC-UA in manufacturing environments [354]. In parallel, the popularity of the MQTT protocol has grown significantly across many industries [355]. MQTT is widely considered the default protocol for IoT. IBM developed MQTT in the late 1990s to enable connectivity for remote devices like satellites and small infrastructure. Over time, MQTT has gained popularity among the IoT development community due to its lightweight nature, making it easy to implement on various devices, including those with limited resources. MQTT is also flexible enough to be used across different applications, from low-bandwidth networks to cloud-based systems, making it a highly versatile protocol. As MQTT grows in popularity, many people are experimenting with its suitability for industrial applications. MQTT's strengths are its ease of implementation and the relative simplicity of its protocol specification, which contrasts with the industry-standard OPC-UA protocol. MQTT promotes maximum flexibility in how developers can define the namespace structure and payload specifications. However, the resulting flexibility makes it unsuitable for manufacturing.

MQTT is arguably the *de-facto* messaging protocol of the IoT and is already popular in IIoT applications. MQTT supports decoupling data producers through the `pub/sub`sub-model model, enabling data exchange across the internet. MQTT

makes it easier for heterogeneous data producers and consumers to interoperate and share data.

In industrial applications, MQTT was gaining different levels of traction, partly due to the perceived challenges in interoperability between vendors and the purported lack of reliability features inherent in the MQTT protocol itself. One of the reasons for MQTT's popularity was the flexibility in topic naming and data formatting. MQTTs' lightweight implementation also meant that state awareness was limited to using the last-will and testament (LWT) functionality, which is insufficient for industrial applications, where a more comprehensive approach to managing the state and equence of messages is cirtical to the operation of such systems.

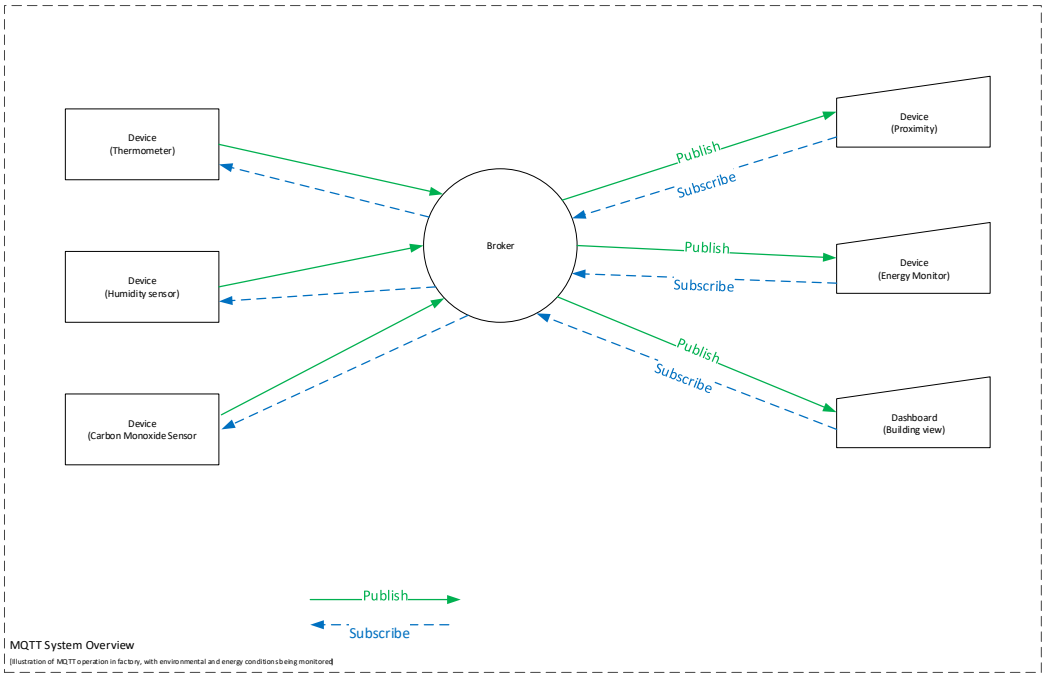


Figure **(5.1)** –MQTT operation overview

The SparkPlug specification, defined in 2019, extends the MQTT protocol to support the integration of data from industrial equipment, sensors, and vendors. This enables ecosystem players to interoperate their equipment and provides IIoT application support.

SparkPlug builds on and extends the MQTT protocol by including functionality that was not originally included in MQTT. This addresses some of the limitations of MQTT, such as its lack of support for state management and its limited payload format.

The current version of SparkPlug is **SparkPlug B**. All participating systems in a SparkPlug implementation share a standard data format and interpretation framework. This allows for more robust state management and higher levels of reliability than MQTT natively. It also significantly reduces the complexity and administrative overhead of many industrial deployments.

- **Extended MQTT Functionality**: Sparkplug extends the functionality of MQTT clients. It includes new features and defines explicit messaging for industrial applications, which we will discuss shortly. In a Sparkplug system, there are two critical MQTT clients. Edge of Network
- Edge of Network (EoN) Nodes: These nodes facilitate gateway functionality, supporting communications with legacy devices. An *EoN* node can also function as an intelligent device or sensor node equipped with sufficient computing capabilities to publish data and metrics directly to a Sparkplug-enabled network.

- **Application Node**: An application node is a software client that sends and receives data and commands on the network. A primary application, which we discuss in more detail, and other optional clients, can be present on the network, such as a data historian. Other gateways can also be clients on the network, enabling legacy device or systems integration.

- **Topic namespace**: A topic namespace is a structured message, similar to a file system folder and file structure, which acts as an address and enables data sharing. Sparkplug uses a standard topic format; this helps eliminate the variability from vendor implementations. Each Sparkplug topic will include the following preamble `spBv1.0`, which denotes that the data is Sparkplug B version 1 compliant. This identifier enables the discovery of data on networks transmitting the format. The next item contains the $GroupID$, user-defined, describing a logical grouping of MQTT nodes sharing data. The Sparkplug specification predefines message-types. The message type can *state information*, commands, or *data* from any actor on the system.

  In SparkPlug, a standard format for topic paths uses the following structure. [1]

  `spBv1.0/<Group ID>/<MESSAGE TYPE >/<Edge Node>/<Device ID>`

  Edge Node ID is a user-defined descriptor that must uniquely describe a specific MQTT node participating in the system. The device ID is also user-defined and directly identifies a device connected to an Edge Node.

[1] SparkPlug code uses the font and colour convention throughout this thesis

- **State Management**The idea of Birth and Death messages is crucial in Sparkplug to enable state monitoring. Death messages use the last will feature of MQTT. Birth and death messages would allow subscribers to notify what data may become stale.
- **Payload structure** Payload Sparkplug B defines a standard, structured, data-rich, yet efficient payload format. The core payload uses Google's protocol buffers (protobuf) specification to represent complex data [356]. By leveraging protobufs, users can avail themselves of the underlying functionality in most mainstream languages. Payloads contain a range of metrics and support for complex and user-defined data types. Sparkplug uses the JavaScript Object Notation (JSON) format.
- **Primary Application** The notion of a 'primary application' is central to Sparkplug-based implementations. Typical MQTT networks have many applications; however, in Sparkplug-based systems, an application node such as a SCADA system or IIoT host system will act as a primary system. The primary application sends commands and logs system data and acts as the central orchestrator of issuing control commands in the system. The direct application will also issue birth and death certificates to the network by leveraging a $STATE$ topic.

5.2.2 Virtualisation Technology: Containers

Virtualised infrastructure has grown in popularity and recently also in industry. One commonly used system type is virtual machines (VMs). These systems use a hypervisor to run on bare-metal infrastructure and contain the guest OS

application code and all associated libraries inside the VM. On the other hand, container images only contain the application code and associated runtime libraries needed to run the application, assuming the host machine provides the underlying operating system services. These container-based technologies allow for modular and extensible systems, as stated in a study by [357].

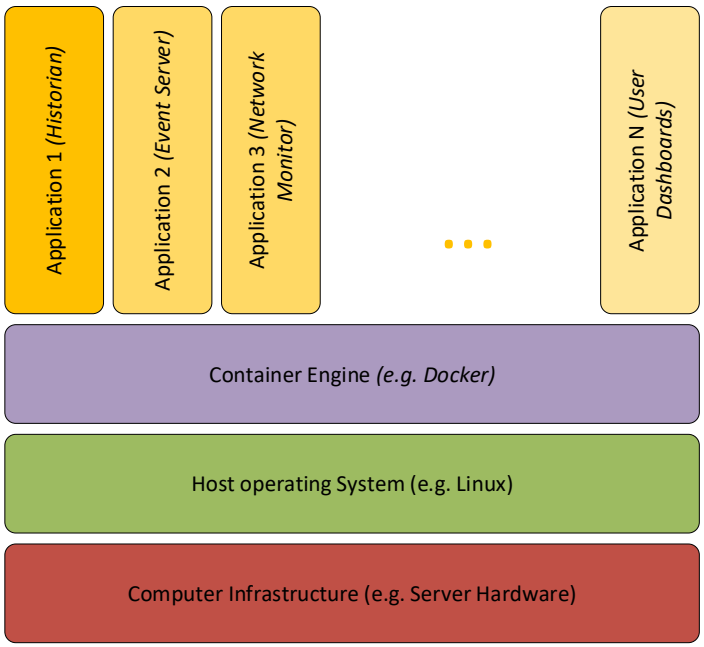


Figure **(5.2)** –Container technology architecture

Docker is one of the most popular technologies for managing and deploying containers [2]. Containers are executable objects that package applications, services, configurations, and dependencies. This process, called containerisation, abstracts service applications from the underlying infrastructure, allowing them to be ported

[2]https://www.docker.com

Listing 1 Docker build command for an example PostgreSQL Database

```
$  docker build -t example_postgresql
```

easily to other platforms. Multiple containers can run on a single host, sharing the same operating system while operating as isolated and secure services.

Compared to virtual machines, containers are lighter, requiring less disk space and memory. They can be started and stopped much faster since the entire operating system does not need to initialise. While containers offer increased flexibility, there may be a performance penalty for running in a virtual environment [358].

Containers allow for easy movement between nodes, domains, and infrastructure, such as cloud or edge computing, making them versatile and capable of running anywhere. Additionally, managing containers through tools like Kubernetes integrates them into the IT environment, reducing the need for specialised installation and configuration. Kubernetes helps in automating the deployment, scaling, and management of those containerized applications. They often work together to provide a streamlined process for deploying applications in a scalable and manageable way. Furthermore, the efficiency and flexibility of containers result in increased productivity when deploying, managing, and providing industrial infrastructure, which is vital for Industry 4.0 applications.

Docker images contain executable application code and related development tools, libraries, and dependencies. All docker containers use a Docker file that instructs how to build a docker image when created by calling the *dockerbuild* command illustrated in Listing 1 1.

Listing 2 Docker run command for an example PostgreSQL Database

```
docker run --rm -P --name pg_test eg_postgresql
```

Running the PostgreSQL database involves calling the *dockerrun* command as illustrated in Listing 2

In our application, we are building a system comprised of multiple containers residing on the same host. We use *Docker compose* to automate the application architecture and configuration. We specify the services and configuration settings for the system in a YAML file [3]. Importantly, our configuration file defines persistent storage for our databases and historians. A snippet of our code is presented in listing 3, and the entire file is available in Appendix A.

Using container technologies allows for greater flexibility and portability, making it easier to utilise computing infrastructure. Containers are portable between environments, which allows for dynamic infrastructure reconfiguration. This feature makes them ideal for improving performance and reducing end-to-end latency by allowing application code migration from the network's edge to the cloud. Additionally, container technology supports the easy addition or modification of subscribers and publishers in `pub/sub`sub-based architectures.

5.2.3 System design details

Our system architecture leverages an event-driven architecture (EDA) utilizing the publish-subscribe `pub/sub` pattern to facilitate seamless data sharing among

[3]https://yaml.org

Listing 3 Code snippet of Docker Compose YAML file

```
grafana:
image: grafana/grafana-enterprise
container_name: grafana
restart: always
ports:
- "0.0.0.0:3000:3000"
volumes:
- grafana-storage:/var/lib/grafana

Prometheus:
image: prom/Prometheus
container_name: Prometheus
restart: always
Volumes:
- prometheus-storage:/var/lib/prometheus
ports:
- "0.0.0.0:9090:9090"

version: '3.7'
volumes:
timescaledb-data: {}
portainer_data: {}
ignition-data: {}
grafana-storage: {}
prometheus-storage: {}
networks:
marktest-network:
driver: bridge
```

all system participants. The rationale behind opting for an EDA is multi-faceted, encompassing several strategic advantages delineated below:

1. **Interoperability and Modularity:** EDA fosters interoperability between a diverse array of technology components, thereby ensuring cohesive functionality without compromising the individual modularity of each element. This approach is pivotal as it permits facile alterations and technological advancements, safeguarding the system against obsolescence and facilitating a non-disruptive transition during upgrades.

2. **Efficiency and Resource Optimization:** By transitioning from a poll-based response mechanism to event-triggered data transmission, EDA significantly mitigates unnecessary network traffic and computational resource expenditure, engendering a more responsive and resource-efficient system capable of managing larger data volumes with reduced latency.

3. **Multi-consumer Support:** The intrinsic `pub/sub` pattern in EDA allows a single event to be simultaneously consumed by multiple consumers. This simplifies the system architecture and facilitates richer data analytics and insights, fostering a rich ecosystem where different components can process events in distinct manners without necessitating customized code.

4. **Real-time Analytics and Insights:** EDA is conducive to real-time analytics, a pivotal feature in modern IIoT systems. It ensures that events are analyzed and responded to in real time, facilitating immediate action and enhancing the system's agility and responsiveness to changing conditions.

5. **Scalability:** EDA is inherently scalable, capable of accommodating an increasing number of event producers and consumers without a linear increase in complexity. Such scalability is vital in dynamic environments where systems must evolve to meet changing demands.

6. **Fault Tolerance and Reliability:** Coupled with the `pub/sub` pattern, EDA can be designed to be fault-tolerant, ensuring system reliability and continuous operation even in the face of component failures. This is achieved through features such as message queuing, which guarantees message delivery even in temporary network failures.

7. **Enhanced Security:** Adopting an EDA allows for implementing robust security measures such as end-to-end encryption of events, thereby ensuring data security and compliance with regulatory requirements.

Given these substantial benefits, an event-driven architecture emerges as a robust foundation for our system, promising a scalable, efficient, and future-proof solution that can adapt to changing technological landscapes while delivering real-time performance and insights. The system uses the SparkPlugB protocol to allow for two-way communication between devices. Devices can connect to the system's infrastructure using MQTT version 3.1 or communicate through an Edge of Network (EoN) gateway device, as defined in the SparkplugB specification.

Fig. 5.3 provides a detailed overview of the system architecture and its interaction with third-party systems. The dotted line box indicates the system's boundary and contains an Edge device, the Edge of Network Node, and a local gateway server. The system is modular, with different subsystems working together to achieve its goals. The SCADA/IoT host is the primary application that issues commands to the system and manages its state, including enabling `BIRTH` and `DEATH` messages. We will provide more information on this topic later.

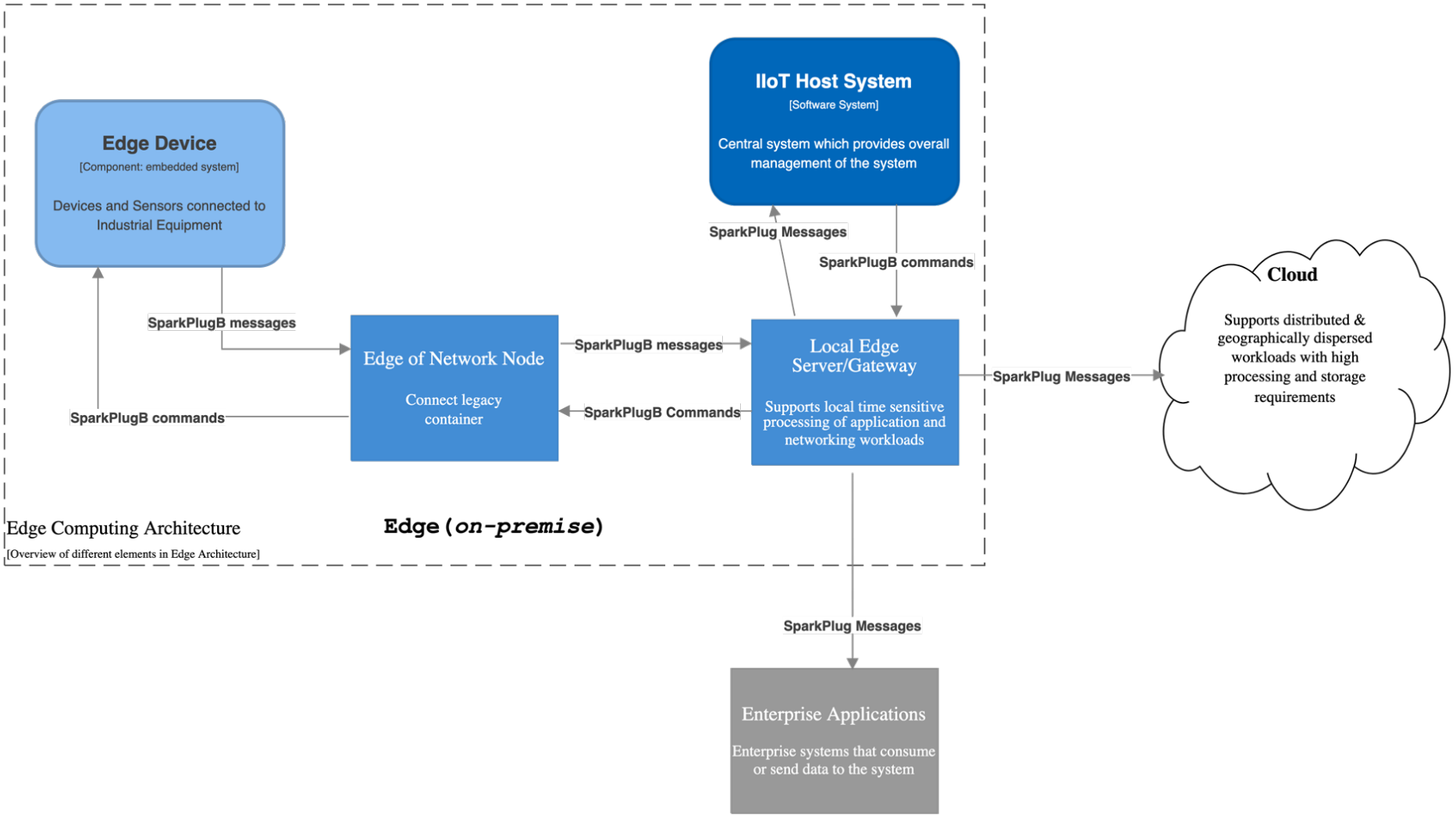


Figure **(5.3)** –High-level System Architecture

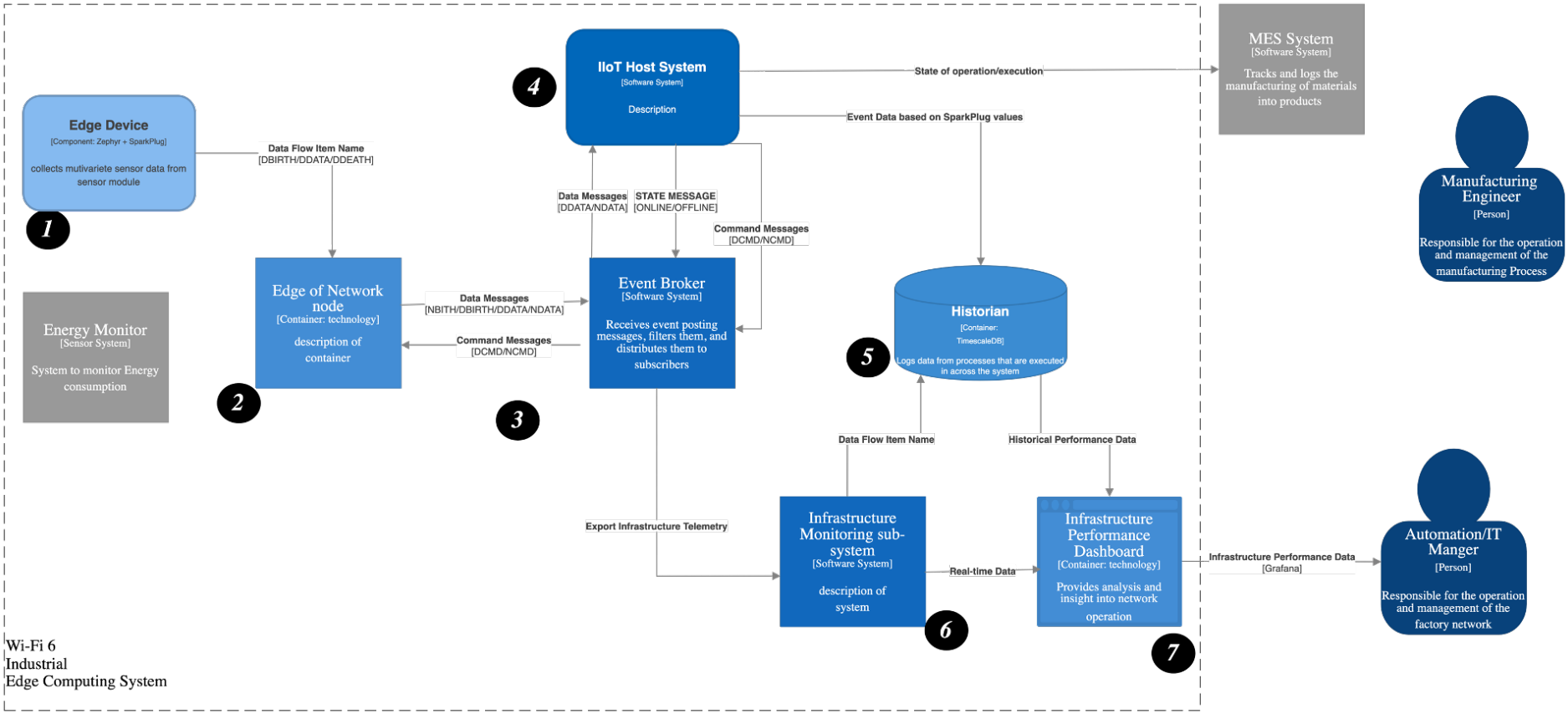


Figure **(5.4)** –System Architecture with numbered subsystems

5.2.4 Key system components

The system is made up of the following components. We detail each component in the following list

5.2.5 Key System Components

Our system is composed of several key components, each of which we outline below:

1. **Edge of Network Node (EON):** This node, adhering to the SparkplugB standards, operates both as a gateway and a protocol translator. It facilitates the integration with field devices and automation equipment, including but not limited to motors, pumps, drives, PLCs, and sensors. Moreover, it supports the direct wiring of industrial I/O and instrumentation, thereby aiding in process monitoring and control. In the system diagram, these functionalities are represented by grey boxes, which symbolize the various sensing devices connected to the EoN node. This setup ensures SparkPlugB functionality through efficient message passing and connectivity.

2. **Event Broker:** Serving as a linchpin in the system, the event broker is an MQTT-compliant server that oversees message transmission between the devices within the system. By facilitating a shift from the client-server model to a more scalable `pub/sub` system, it ensures the seamless decoupling of publishers and subscribers, enhancing the system's scalability.

3. **Data Historian:** This component is a specialized database that aggregates data from field devices, machines, and process systems, such as SCADA or MES, storing it as time-series data for future reference and analysis.

4. **Infrastructure Manager:** Tasked with monitoring the system's overall performance and operations, the infrastructure manager gathers data from the connected infrastructure, including all containers and devices. A more detailed discussion on this component is reserved for Chapter 6.

5. **System Management Dashboard:** This dashboard offers a unified platform for system management and monitoring, providing insights and control through a single interface.

5.3 Edge Device

The sensing strategy we have adopted builds on the work of Laput et al. from Carnegie Mellon University [359]. In their work titled *Synthetic sensors: Towards general-purpose sensing*, the authors propose a design for general-purpose sensing. The authors present their method and results based on sensing in a home environment.

Our design advances the design outlined by Laput et al. in Fig. 5.5. We made our board compatible with the Arduino ecosystem, making our board interoperable with a wide variety of microcontrollers and IoT development kits. Our design enables greater ease of experimentation and extensibility to other boards or sensors, thereby supporting a broad spectrum of analogue and digital sensors. This extensibility also supports an extensive array of shield-type add-ons, which

are standard and widely available. We believe flexibility is essential in industrial applications, where one size fits all is rarely possible.

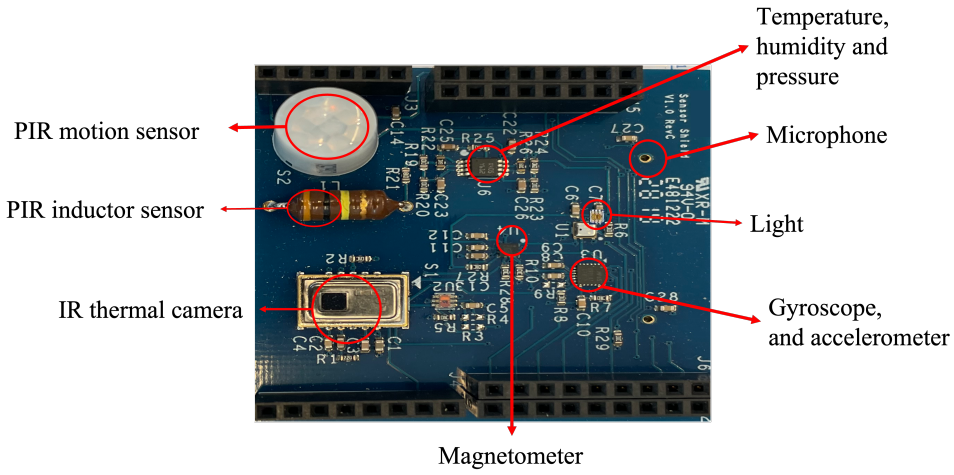


Figure **(5.5)** –Arduino-based sensor module

Another critical factor in our design is the ability to use the board with different computing infrastructures. Our design considerations assumed that our system must support a variety of microcontroller architectures. Whereas the Carnegie Mellon design uses USB as an interface to a microprocessor architecture, sending data via Wi-Fi, our strategy focuses on processing the data in a microcontroller architecture. Numerous popular systems provide low-cost computing, memory and storage. Many of these technologies and platforms are used today, such as the Raspberry Pi [4] and Beagle Bone systems [5]. Many of these boards support industrial-rated requirements such as extended temperature ranges.

In addition, many of these platforms increasingly provide hardware and software support for AI functionality and machine learning frameworks. The combination

[4]https://www.raspberrypi.com/for-industry/
[5]https://beagleboard.org/bone

of enhanced onboard sensing and advanced computing enables higher frequency direct sensing and inferential sensing or soft-sensing from data fusion from multiple sensors [360]. These sensing modalities refer to using algorithms and mathematical models to estimate unmeasured or inadequately measured variables in a system based on the correlations with other, more easily measured variables. This approach leverages existing sensor data to infer information about conditions or parameters that are not directly measured, often facilitating real-time monitoring and control in industrial processes. Soft sensing can enhance system efficiency and safety by providing timely insights derived from the synthesis of data from various sources, thereby allowing for a more comprehensive understanding of the system dynamics. It is a crucial tool in modern industrial systems, helping to optimize performance and anticipate issues before they become critical.

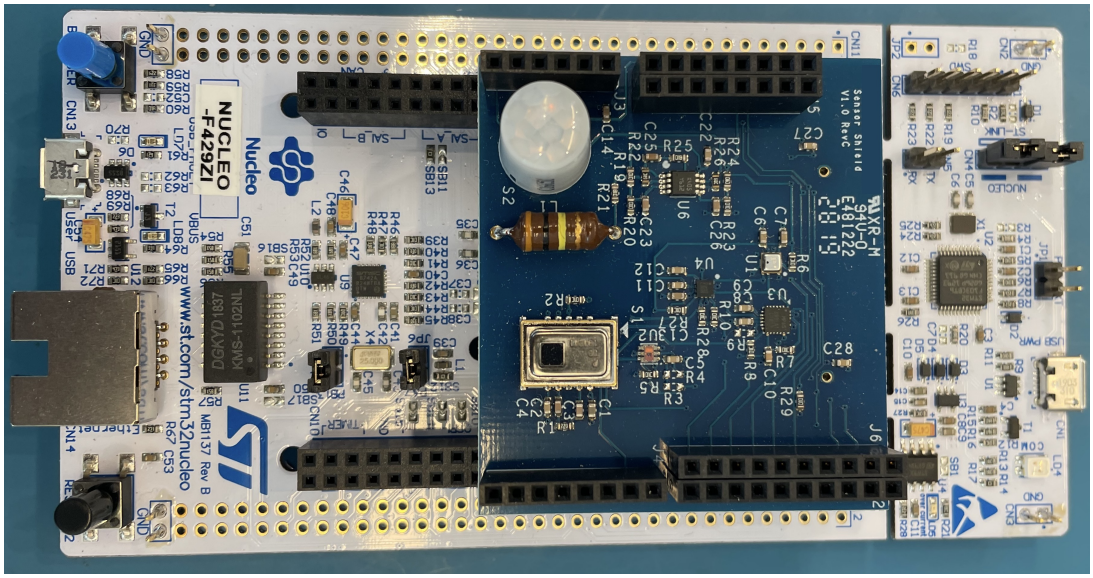


Figure **(5.6)** –Zephyr-based Node system

The base system uses an ST Nucleo-144 development board, a popular platform for designing and developing prototype systems. The sensor node also runs a real-time

operating system called Zephyr, which the Linux Foundation supports. Several potential selections are available in the design [361]. However, we selected Zephyr because of its extensive support of third-party hardware, active and engaged community, and codebase's pedigree. The board also provides pin compatibility for Arduino-compatible boards, using pin header mapping from the Arduino ecosystem. The use and adoption of the Arduino ecosystem further extend the system's compatibility, enabling a wide variety of I\O and connectivity technologies and compatibility with Arduino-compliant devices.

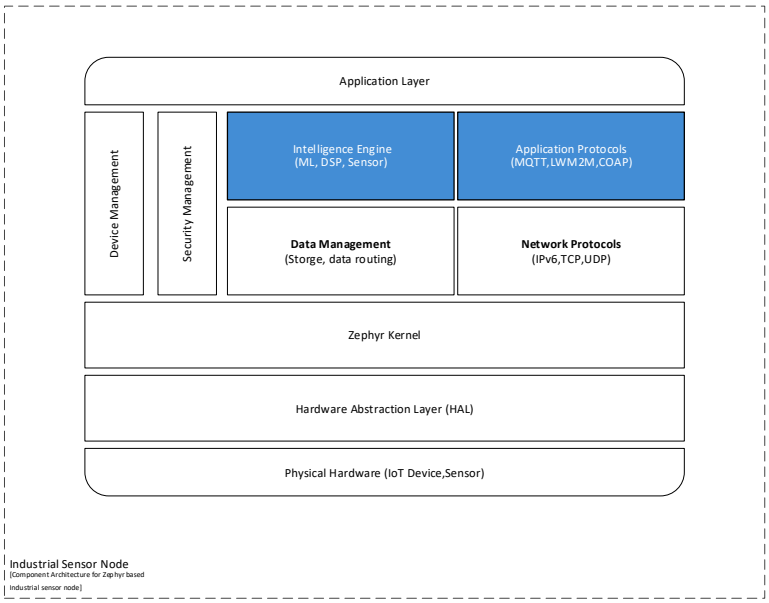


Figure **(5.7)** –Edge of Network Node Component Architecture

This sensor node has Wi-Fi connectivity and a defined interface for seamless communication. Its design can be classified as a high-performance embedded

sensor node, known for its ability to process data at a rate of Giga instructions per second. It also utilises high-speed I/O interfaces to facilitate fast data transfer. Additionally, this sensor node employs a multicore approach for efficient data processing, with a co-processor model dedicated to handling sensing data. In contrast, the multicore approach manages networking and general-purpose computing tasks such as writing data to disk or managing the operating system.

5.3.1 Edge of Network Node

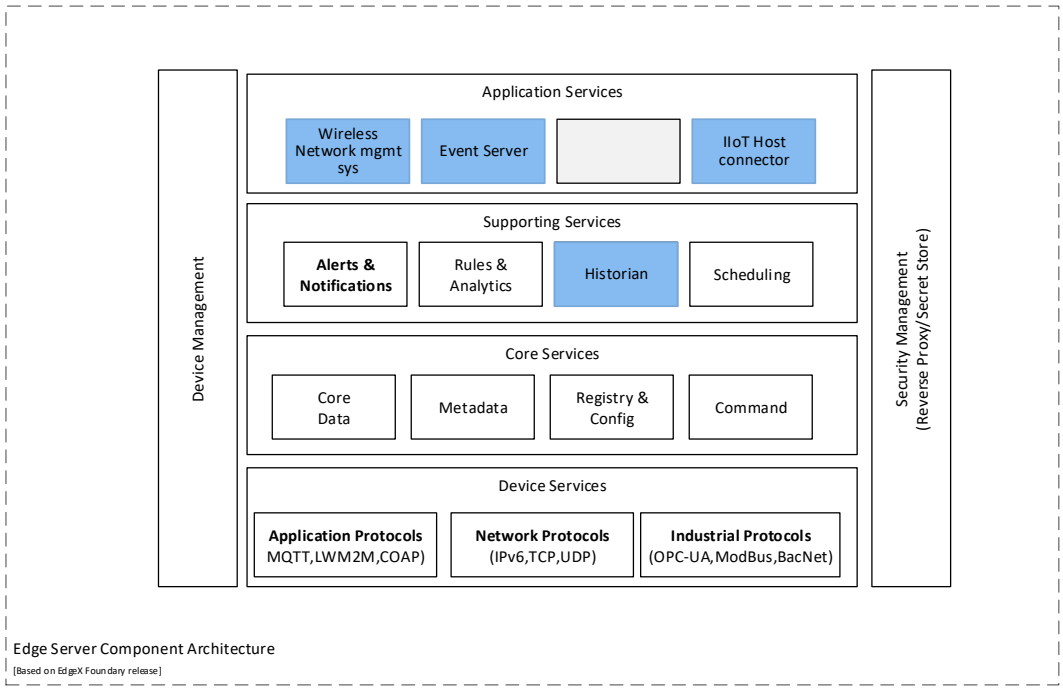


Figure **(5.8)** –Edge Server Component Architecture

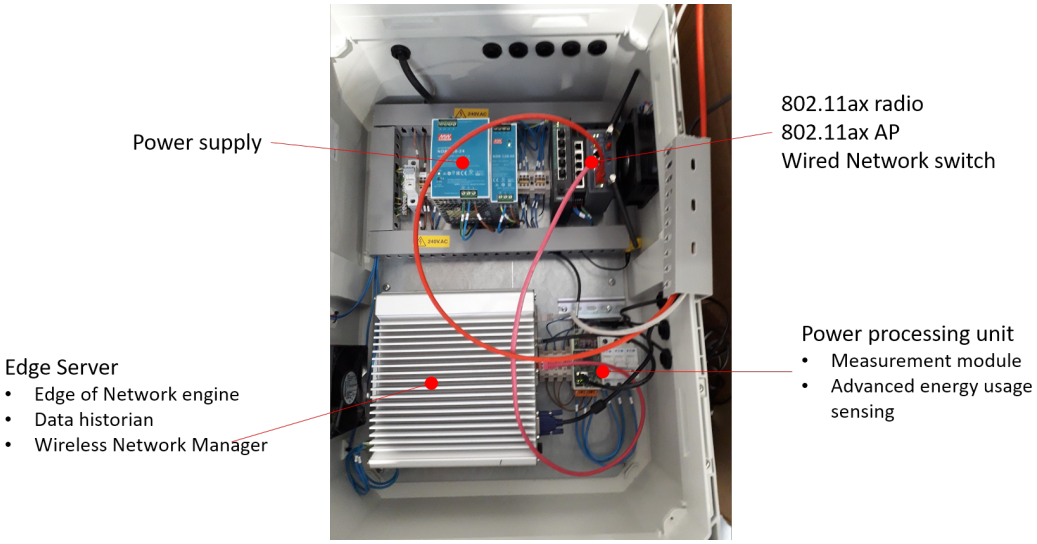


Figure **(5.9)** –Edge Server Installed system and key components

5.3.2 Message Broker

An event-driven architecture (EDA) is a type of distributed computing that allows different systems to communicate and exchange data. This pub/sub pattern differs from the request-response pattern in HTTP, which requires a client to initiate a request and a server to respond with the requested information. In event-driven systems, interactions are events, such as a change in state or an update in one system that triggers an action in another system. For example, a temperature sensor reaching a threshold or an operator updating data through an HMI could be considered events that trigger other actions.

A few key components are involved in an Event-Driven Architecture (EDA). Firstly, an event producer or publisher generates or detects an event and sends a message to an event broker or manager. The purpose of the broker is to handle the routing, filtering, and processing of messages from publishers to subscribers. It also manages the communication between publishers and subscribers asynchronously.

On the other hand, a subscriber is a system that wants to receive and act on events. Topic-based subscriptions are the most commonly used subscription model in pub/sub systems. A subscriber can receive data on one or multiple topics or subjects. The broker's primary responsibility is to distribute data to the list of subscribers who have subscribed to a particular topic, allowing for easy addition and removal of publishers and subscribers without the need for significant system changes.

The reason for choosing an EDA-based pub/sub model is its ability to cater to multiple systems that require access to the same data. The `pub/sub` model can also handle large volumes of data collected from field devices and machinery at a high velocity. It also supports the expansion of new sensors or devices without requiring significant implementations due to the inherent loose coupling in EDA systems.

5.3.3 Primary application -SCADA IIOT Host

The Host Application is a server that oversees and manages edge nodes and devices. An MQTT Client application subscribes and publishes messages defined in this document in a Sparkplug instance. Typically, in SCADA/IIoT infrastructure implementations, only one primary SCADA/IIoT host node monitors and controls a group of Sprarkplug EoN nodes. The Sparkplug design choice revolves around using a single critical host application.

Despite the single host design, using multiple MQTT SCADA/IIoT nodes in the infrastructure as a consumer or as a backup to the primary host is possible; this configuration allows publishing devices to react to changes in the primary host's

status. For instance, if the SCADA system disconnects, the publishing devices can take appropriate action, such as caching or stopping data transmission. The Host ID enables devices to take action based on the system's requirements by setting the *IsPrimaryApplication* flag to **True**. The enterprise and site are mapped to the *group_id* and separated by ., with a three-letter notation used to describe the site. For example, "mul" represents the Mullingar facility of Irish Manufacturing Research. Additionally, we use a similar convention for Area and Line, mapped to "add" and "polish," respectively, to describe the polishing line of an additive manufacturing line. Finally, we map the cell to a *device_id* to an Edge device.

Currently, there are few options for hosting SparkPlug applications, which is unsurprising considering its early development stage. However, we have decided to use the Ignition application from Inductive Automation] [6].

5.3.4 Management and Applications

System management and applications are responsible for utilising the data and managing the system. They extend the system's functionality and provide services to other users. This solution includes three applications, with two being discussed in detail: the primary application and the historian. The third application is outlined in Chapter 6.

The management and applications handle system management and utilise data to provide applications based on the system's data. The primary application follows the Sparkplug specification and acts as the control node. It receives data from the system and needs to know the status of connected devices for proper

[6]https://inductiveautomation.com/ignition/edge-iiot

command execution and historical data retention. This approach also implements a historical data repository.

5.4 Data Historian

A data historian is a database that collects time-series data from field devices, machines, and process systems like SCADA or MES. They gather structured data by measuring specific production or machine variables such as defect counting or machine cycle times. Over time, data historians have evolved and now offer essential features like compatibility with various industrial plants and equipment, industry-specific analytics, and visualisations for data exploration. They also added disk and data management capabilities, making them reliable for industrial applications [362].

Companies often have limited options when it comes to collecting data from historians due to strict licenses and variable costs. Historians need to be more adaptable in order to integrate data from various sources and systems. However, modernizing historian technology can be a costly and time-consuming process. Additionally, their proprietary nature can limit their usefulness and require specialist or vendor-specific integration partners for updates and upgrades [363]

5.4.1 TimeSeries Databases

A timeseries database collects, stores, and organises time-based data that is continuous and sequential. This type of database is commonly used in industrial settings to gather information from machines and sensors sequenced in time [364].

Time-series data is widespread across various industries, but the recent surge in IoT and sensor technology has increased the demand for time-series databases. In recent years, open-source software and time-series databases have become increasingly popular, with major companies like Amazon and Google making them available. Bader's review and comparison of TimeSeries databases is a comprehensive resource on the topic [365]. The authors highlight the importance of ongoing performance benchmarking, which Mostafa et al. provide for many popular time series databases and a testing framework [366].

Although open-source time-series databases were not initially intended for industrial use, they have gained significant popularity. These databases can handle structured, unstructured, and non-relational data, making them highly versatile [367]. Additionally, open-source time-series databases have been designed to manage large volumes of high-frequency data, with some versions outperforming traditional historians by a considerable margin [362]. These databases are also easy to integrate with multiple data sources, thanks to their well-defined open APIs. Furthermore, open-source technology allows for sharing new features and capabilities, which tends to be less frequent and comprehensive with traditional historians [368].

Popular time-series databases include InfluxDB, Graphite, Prometheus and TimescaleDB. We selected to use TimescaleDB as the engine of choice for our architecture. The above systems are well-established open-source technologies, with InfluxDB being the most popular time series. The reason for using Timescale DBis that TimescaleDB supports SQL queries and is built upon the popular

Postgres database engine. The compatibility with PostgreSQL is the primary reason for selecting TimescaleDB as the time-series database.

TimescaleDB is a time-series database different from InfluxDB. It uses a Hypertable that partitions data into multiple underlying tables based on time, allowing it to act as a single logical table with high-performance characteristics. Users have the flexibility to configure data ordering based on their specific needs. Additionally, TimescaleDB utilises continuous data aggregation, which enhances the performance of temporal operations like *min, max*, and *hourly* by reducing the need for large table scans and improving response time.

TimescaleDB is an extension to PostgreSQL, which makes it compatible with standard SQL features like ANSI SQL, indexing, and joins. This functionality means that a single system can support both time-series and relational databases, making it more convenient for managing multiple information needs. Additionally, TimescaleDB supports extensibility to other systems, such as PostGIS, for location data, enabling the geo-location of devices.

However, while convenience and extensibility are important, TimescaleDB must also provide the performance expected of a proper time-series database. Many organisations claim performance supremacy over their offerings, but TimescaleDB has improved over InfluxDB in tests run using the Time Series Benchmark Suite (TSBS). It's worth noting that the TimescaleDB organisation conducted these tests and were not from an independent source. However, the benefits of TimescaleDB are not just performance. TimescaleDB provides many adopters with a means to marry conventional SQL and relational systems without requiring time-consuming

code refactoring. TimescaleDB provides performance, compatibility, and scale, making it a suitable choice for industrial applications.

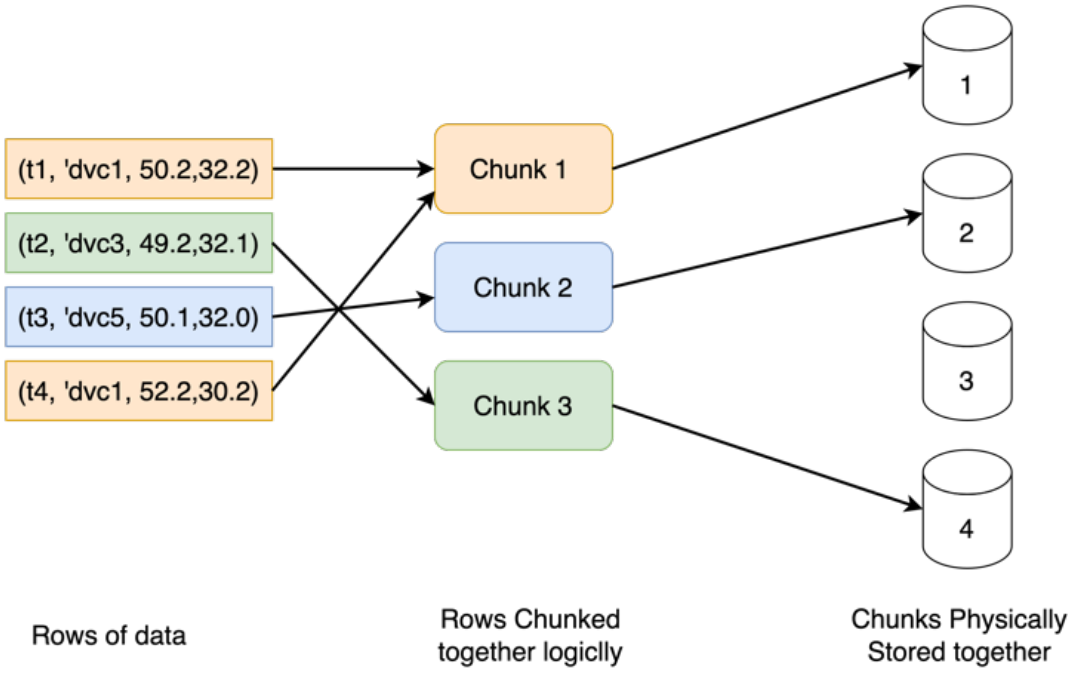


Figure **(5.10)** –Data storage in Timescale DB

5.4.2 Database architecture

The following database design criteria acted as design considerations in the development of the database.

- Stores time series data/metrics collected from heterogeneous sensors and device types.
- Telemetry (metrics) will be collected from many systems and arrive at different times.

- Metrics are generally one data point (e.g. temp and humidity are not reported at the same time but rather individually and will have a different timestamp)
- The information model must support telemetry from different system types and must be able to evolve metrics that are collected and will expand over time.
- The system is open, and additional inputs will be supported over time (e.g., today, we collect temp, humidity, system metrics such as CPU; tomorrow, a sensor may be added that monitors CO2 and system metrics such as RAM).
- Telemetry data and associated metadata will be consumed via dashboards and third-party systems. For example, the operations dashboard and the IIoT host application will consume from the database.
- The system must support ANSI standard SQL

We solved a particular problem in database design by adopting a relational model. This approach ensures full the relational databse functionality which other methods may not offer. A relational database is still the most suitable solution despite current database design and architecture trends. It provides structured data storage, robust querying capabilities. Using this model, we maintain relational integrity and provide the necessary context for the objects in the database. Our data model complies with the IDEF1X standard outlined by Adelsberger [369]. To ensure optimal extensibility for various applications, machines, and infrastructure, we have opted for generalised naming conventions rather than Record_ids, which are unnecessary in a proper relational design.

5.4.3 Entity descriptions

We briefly describe and define the tables in the following list.

- **telemetry Category:** Refers to the different categories of systems that can be collected and extended to any source recording data. While the noun refers to remote, the system itself could be a category, or other examples could include wireless, environment, process, or machine type. The telemetry category is a reference entity used to classify different sensor types.
- **Sensor Type:** The Sensor Type entity contains information about specific sensor types related to Telemetry Category. For example, accelerometers could be used in various machines in an industrial setting. Combining the Telemetry category and sensor type helps distinguish different sensors. The sensor type can follow a convention such as IEEE 1451.4 Transducer Electronic Data Sheets (TEDS) or be a user-defined name.
- **Sensor:** The sensor table holds the sensors that gather telemetry data in the system. Each sensor is identified by its location, component, and serial number. The TEDS specification includes a 64-bit identifier within its content. The identifier elements, which are 64 bits in length, are detailed in 5.1. Users have the option to utilise a user-defined serial number or customise it.
- **Component Type:** Component Type is used as a reference to describe a system component. Given the wide breadth of potential systems and associated subsystems, the selection of the term is intended to support extensibility. For example, a component can describe a machine or part of

	Bit Length	Permitted Range
Manufacturer ID	14	17-16381
Model Number	15	0-32767
Version Letter	5	a-z
Version Number	6	0-63
Serial Number	24	0-16777215

Table **(5.1)** –Basic TEDS format

a machine or device, such as *gateway, Eon, industrial PC or laser printer.* The component type could also enable the underlying schema to be adopted in different applications. For example, in a home automation application, it could describe *cooker, fridge, freezer*

- **Component:** Each component type can contain any number of components, for example, in a gateway. We have shown components to depend on location, as we contend that a specific site element is contextual to a place's specifics. However, it is also equally valid that the component and location need not depend on each other.

- **Location** Location contains information about the specific location of a sensor gathering data. One consideration is to use the geo-coordinates of the location to describe the physical location; however, in many applications, more than one sensor could likely be at the exact location. We have elected to use the following format discussed in 5.2. We use the format of *PostCode.Enterprise.Site.Area.WorkCentre.WorkUnit* with the **.** denoting a hierarchy. The suggested approach could be extended to describe different businesses at a specific location, or users could use a subset of the data, depending on their needs. The name can be a business used to identify the specific location, which also should be changeable. For example, if the data

was related to a transient or short-lived manufacturing process, the name could be updated to a more helpful name.

- **Telemetery** The telemetry table contains the sensor data collected from components at a specific location, timestamped with the time the measurement was captured at a remote location. The table contains the timestamp of the data in which the device observed the observation in question. For example, if an energy sensor observes electrical data on a machine, the timestamp would represent the observation's time and local time. The date-time type used is *timestamp*, which can store 1 μs resolution.

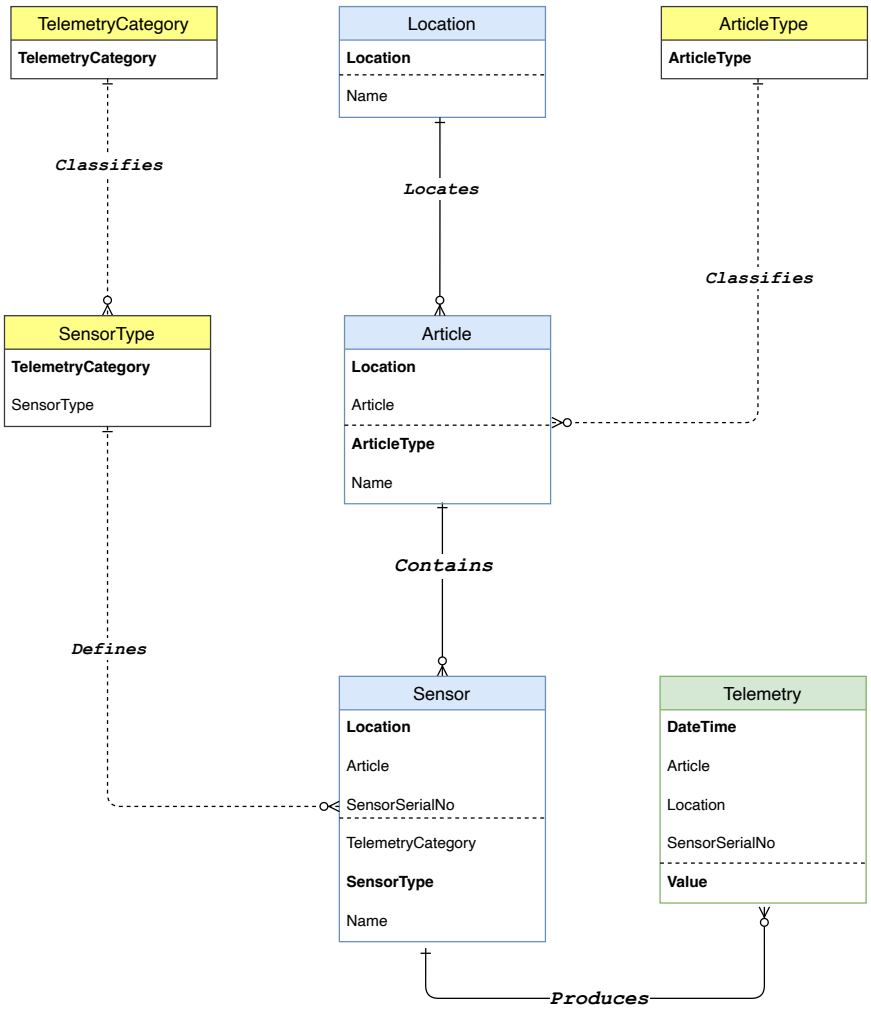


Figure **(5.11)** –Information model of system database

5.4.4 Data Definition Language

The data definition language for the database is presented in Appendix a. The data definition language included is compatible with PostgreSQL, version 15. We deliberately made a design decision to store almost all of the data in the $VARCHAR$ data type, which is a SQL standard supported by all SQL-compliant databases. Data types can be changed or altered to improve performance or save storage space.

The decision to avoid storing data in JSON format within the SparkPlug framework was driven by the need for a more adaptable and protocol-agnostic data model. This approach ensures flexibility for accommodating various communication protocols and future-proofing the system, while also leveraging the robust querying and analytical capabilities offered by relational databases. Consideration was given to storing the data in a NoSQL style database, which are incrasingly popular in IoT implmentations [370]. However, we elected to use a relational model as it providers structured data and a schemas, their pervasive and established use.

In Listing 4, we illustrate the Data Definition Language (DDL) code used to generate the component table.

The process of creating a hypertable is straightforward. Firstly, a standard PostgreSQL table is created, which stores the data required in time-series. In our case, this is the Telemetry table, illustrated in Listing 5

Next, we transform the PostgreSQL table into a TimescaleDB hypertable. For this, we need a column to store the time values. In our case, we use the DateTime

Listing 4 SQL command for Create Component Table

```
-- object: public."Component" | type: TABLE --
-- DROP TABLE IF EXISTS public."Component" CASCADE;
CREATE TABLE public."Component" (
"Location" varchar(255) NOT NULL,
"Component" varchar(255) NOT NULL,
"ComponentType" varchar(255),
"CName" varchar(255),
"ComponentType_ComponentType" varchar(255),
"Location_Location" varchar(255),
CONSTRAINT "Component_pk" PRIMARY KEY ("Location", "Component")
);
-- ddl-end --
```

Listing 5 SQL command for Create telemetry Table

```
-- DROP TABLE IF EXISTS public."Telemetry" CASCADE;
CREATE TABLE public."Telemetry" (
"DateTime" timestampz NOT NULL,
"Component" varchar(255) NOT NULL,
"Location" varchar(255) NOT NULL,
"SensorSerialNo" smallint NOT NULL,
"Value" varchar(255),
"Location_Sensor" varchar(255),
"Component_Sensor" varchar(255),
"SensorSerialNo_Sensor" varchar(255),
"Location_Component_Sensor" varchar(255),
"Component_Component_Sensor" varchar(255),
CONSTRAINT "Telemetry_pk" PRIMARY KEY ("DateTime","Component","Locat
);
-- ddl-end --
```

stored in the *timestampz* format. You can find the command for creating the hypertable in 6.

Listing 6 SQL command for Create Component Table

```
SELECT create_hypertable('Telemetry', 'datetime');
```

5.4.5 Protocol Mapping

Our messaging protocol utilises the SparkPlugB protocol that we have previously discussed. We have extended this protocol to create a messaging protocol compatible with the ISA-95 standard. Our structure is illustrated in Figure 5.13. By mapping the ISA-95 model structure to SparkPlugv1.0B, also known as the IEC/ISO 62264, our proposed messaging protocol provides a common taxonomy and definition of industrial functions. It simplifies integration with higher-level ERP and MES-type systems and improves interoperability between automation OEM equipment. Enterprise Resource Planning (ERP) manages business processes, logistics, and workflows, while Manufacturing Execution System (MES) monitors and manages production in real time. Both optimize industrial operations. With a standardised model and `pub/sub`Sub architecture, our messaging protocol extension structure provides a plug-and-play-like system. We provide more detail on our messaging protocol extension structure in figure 5.12.

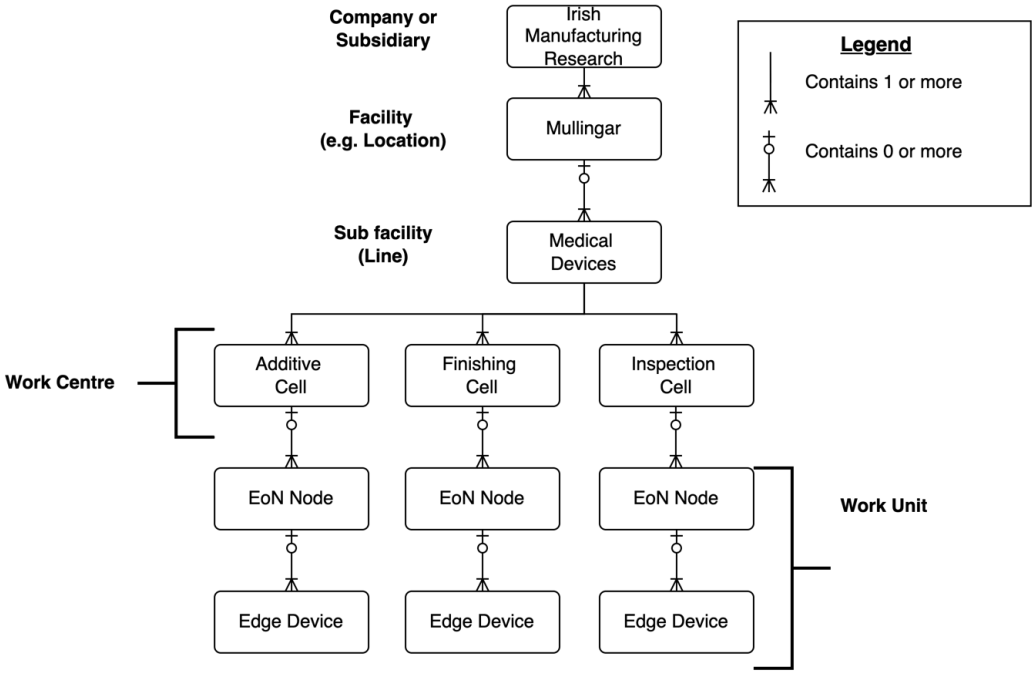


Figure **(5.12)** –ISA-IMRHierarchy Mapping

We have demonstrated our protocol mapping by using the ISA-95 hierarchy to map it to the Irish Manufacturing Researchs structure. The mapping definitions from Table 5.2 have been converted into the *SparkPlugB* format, as shown in Figure 5.13. The *group_id* for both the Enterprise and Site is mapped using a period or **.** separator. We have used a three-letter abbreviated notation to describe the site, with **imr** representing Irish Manufacturing Research and **mul** being short for their Mullingar facility. Similarly, we have followed the same area and line convention, mapped to **add** and **polish**, respectively. The cell has a cell mapped to a *device_id* and an Edge device. We have used an abbreviated form in the message structure to reduce its byte size. Though the structure could be further experimented with, our approach is reasonable while maintaining human readability.

Listing 7 Sparkplug namespace structure

```
namespace/group_id/message_type/edge_node_id/[device_id]
```

ISA-95 Defintion	IMR- Definition	Description
Enterprise	Irish Manufacturing Research	Name of the main entity in which the system is being deployed
Site	Mullingar	Location of the facility in which tests were conducted
Area	Medical Devices	Name of the area reserved for experimentation on medical device manufacturing
Work Centre	Additive Manufacturing	3d printing manufacturing work cell
Work Unit	Printer1	printer 1 of 1 in the work cell
Work Unit	Finishing1	Finishing substation, which is part of the manufacturing work cell
Work Unit	Inspection1	Inspection substation, which is part of the manufacturing work cell

Table **(5.2)** –ISA-95 to IMR mapping

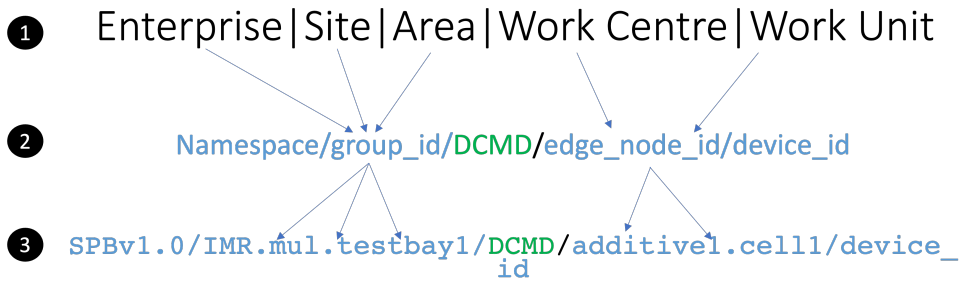


Figure **(5.13)** –ISA-95 and Sparkplug mapping

5.4.6 Messaging structure

In MQTT-based systems, a topic is used to identify the content of a message's payload and who has subscribed to it. The MQTT protocol allows for flexibility in creating the topic structure, making it suitable for many applications. However, in industrial settings, it is essential to have standardised naming conventions and defined structures to ensure consistency in messaging. Sparkplug provides a standardised namespace and structure to address these concerns and follows a specific convention, which is illustrated in Listing 7

The namespace defines the structure used for the remaining namespace elements and the encoding definition of the carried payload data. The Sparkplug B version of the specification uses a UTF-8 string constant:

spBv1.0/group_id/message type

The topic namespace has a group_id element that allows MQTT nodes to be organised into logical groups based on location or function. We recommend keeping the group_id small to save bandwidth, but with improved bandwidth, it is worth considering the trade-off between performance and readability. We use the group_id to indicate the physical or logical location of the system, following a shortened naming convention. For instance, we use IMR1 to describe the area we are monitoring in IMR, while other examples include foundary1 or plant1. Our name, *med-d*, represents an additive manufacturing line in IMR that produces medical device parts, hence the abbreviation for medical devices.

The "message_type" part of the Topic Namespace specifies what the message contains. How the message is encoded will depend on which Sparkplug implementation is used - in our case, it is Sparkplug B. A list of Message Types and their descriptions in Table 8.6, and several different types are available. The Work Center is linked to the three primary sections of the additive process line, namely printing, finishing, and inspection. We employ an edge of Network Node in each work centre as an aggregator to connect to edge devices. We utilise the structure below to define the 3 EoN nodes that constitute the cells in our system design.

Work units relate to the edge devices collecting data inside each work centre, and there can be a many-to-one mapping. The edge devices collect sensor telemetry

Listing 8 Sparkplug topic structure leveraging our proposed protocol

```
spBv1.0/IMR1.mul.med/message_type/fin1/{Payload}
spBv1.0/IMR1.mul.med/message_type/fin1/emm-sen/{Payload}
spBv1.0/IMR1.mul.med/message_type/fin1/ism-sen/{Payload}
```

from each work centre in our work. We use one device per work centre, but the numbers could be much higher in a practical implementation.

The finishing cell *(Work Centre)* illustrates and elaborates our messaging protocol. We assign an EoN for each cell and the cell as the central gateway or aggregator. Multiple options exist for configuring or using the EoN node; for example, the EoN could aggregate at the line level (sub-facility). However, deploying the EoN node at the work centre level supports extensibility and segmentation of the system aligned to logical groupings.

In our proposed solution, the finishing cell has cell devices connected, collecting sensing data from the work centre. Listing 8 illustrates in the following order. Data is collected from two different sensing modules *Edge Devices*, called *emm-sen* and *ism-sen*. Emm-sen refers to an electromagnetic sensing module (not part of the work). Ism-sen refers to the sensing module introduced in Section 5.3.

5.5 Conclusion

In this chapter, we presented a solution for wireless industrial networks that uses IoT technologies and open-source resources. Our design and architectural blueprint offer a flexible edge computing system that can be applied to various domains beyond industrial settings. Using primarily open-source components ensures that the construction and deployment of this solution is cost-effective.

The only exception is the IIoT host application based on commercial software. However, we anticipate that an open-source alternative will be introduced soon.

Our Edge node and sensor module make significant contributions by laying a robust foundation for future research to build upon and further synthetic sensing advancements initiated at CMU. We have also introduced a messaging protocol that enhances the MQTT-based Sparkplug protocol, facilitating a harmonized mapping to the SparkPlug namespace structure and the ISA-95 automation standard. This protocol can significantly contribute to Industrial Automation and Control Systems (IACS), Prognostics and Health Management (PHM), and digital twin applications.

IACS requires reliable wireless connectivity and fast decision-making capabilities. Such performance can be achieved by leveraging the benefits of 802.11ax (Wi-Fi 6E) technology, which provides faster and more robust wireless connectivity. Edge computing enables real-time data processing closer to where it is generated, reducing latency and improving responsiveness. The SparkPlugB protocol ensures standardized data communication, enhancing interoperability and simplifying data sharing between devices and systems.

PHM applications utilise enhanced connectivity and real-time data processing to monitor equipment health, facilitating predictive maintenance strategies that prevent unexpected breakdowns. PHM applications benefit from containerisation, which allows for deploying sophisticated data analysis tools and algorithms directly at the edge, making it efficient to analyze and interpret data. An open-source approach provides flexibility and scalability, ensuring the system can evolve and adapt to changing requirements and technologies.

Digital twin technology has various applications, with synchronization being a critical one. A reliable wireless connection guarantees that the digital twin remains synchronised with its physical counterpart, resulting in more accurate and reliable simulations and analyses. The SparkPlugB protocol enhances interoperability, enabling the digital twin to communicate effectively with other systems and devices for integrated functionalities. Additionally, modular deployment is possible using containers, allowing for independent management, updating, and scaling of different aspects of the digital twin.

An active community of developers continuously innovating and improving the system is a significant benefit of open-source. This ensures that the system can remain up-to-date with the latest technological advancements.

Chapter 6

Industrial wireless network: System test and evaluation

This chapter outlines the performance analysis and experimentation performed on the IEEE 802.11ax-based wireless industrial system outlined in Chapter 5. This chapter details the test criteria selection and discusses the justification of the system performance metrics. We outline the testing system architecture used to collect performance data from the system under test. We also analyse the performance data from experimentation conducted with the system, and contains the following contributions:

- **Design of a Novel Wi-Fi-based Test Methodology for Industrial Wireless Networks** We propose a novel testing methodology for Wi-Fi-based wireless industrial networks that incorporates end-to-end testing

procedures. Integrating network and application layer testing, the hybrid testing protocol extends state-of-the-art in wireless industrial networks. The testing framework is extensible for use outside industrial applications and in different radio frequency spectrum bands.

- **Analysis and Evaluation of Test Data for Different Application Classes** We present a comprehensive analysis and evaluation of the test data for different application classes based on leading global standards bodies. Our study provides a quantitative assessment of the suitability of Wi-Fi-based wireless industrial networks for various industrial applications. This contribution offers valuable insights into the design and implementation of wireless industrial networks that meet the specific requirements of different industrial applications.
- **Performance Evaluation of Wi-Fi 6E in Industrial Settings** We evaluated Wi-Fi 6e in a real-world test facility to extend state-of-the-art testing from laboratory to industrial settings. Our evaluation uses the emerging 6 GHz frequency spectrum, critical for high-performance, reliable wireless communications in industrial environments. This contribution offers valuable insights for deploying Wi-Fi 6e-based wireless industrial networks. It supports the development of future wireless industrial networks that meet the demanding requirements of industrial applications.

6.1 Introduction

With the increasing use of wireless networks in various applications, including industrial settings, it is crucial to also consider performance criteria beyond reliability, latency, and jitter. In industrial networks, supporting application-specific performance criteria, such as those outlined in the ISA classes, is essential to ensure optimal operation.

When it comes to Wi-Fi network designs, they are typically used to support a wide range of traffic and applications. However, industrial networks present very different challenges and have stringent performance requirements. Furthermore, machine-to-machine communications are also evolving to support higher bandwidth applications and services [371, 372].

Therefore, networks must accommodate various payload sizes from different devices, sensors, and systems. End-to-end cycle times are crucial for systems with feedback and control loops, like automated control systems or human-machine interfaces. These systems require a sustained update rate frequency ranging from 1 Hz to 1 kHz.

In industrial networks, optimal performance traditionally relies on deterministic networking. However, meeting operational requirements demands more than theoretical performance testing. Testing under representative modes of operation and actual operating conditions is crucial to assess the system's reliability and latency challenges accurately. Therefore, a comprehensive testing methodology that includes end-to-end testing of Wi-Fi-based industrial networks is vital.

We assess our system's suitability for various industrial applications, including performance criteria in the ISA class.

6.2 Test system and test criteria

We have leverage performance criteria for the system that extends the work outlined by NIST [373]. Figure 6.1 illustrates the scope of our testing. The dotted black line denotes the system's test boundary, while the dotted blue lines represent the components or subsystems of the overall design. The Edge Devices are separate entities, and the Edge Appliance is a single device.

We used an integrated switch for communication between an AP and MQTT Server on the same industrial system. Historian and IIoT services were Docker containers on the same system. Ethernet provided AP-PC connectivity, while wireless IEEE802.11ax connected the EoN node and AP. WiFi was on a separate subnet for better data processing. A Device Under Test (DUT) is connected via a 10Gbps wire.

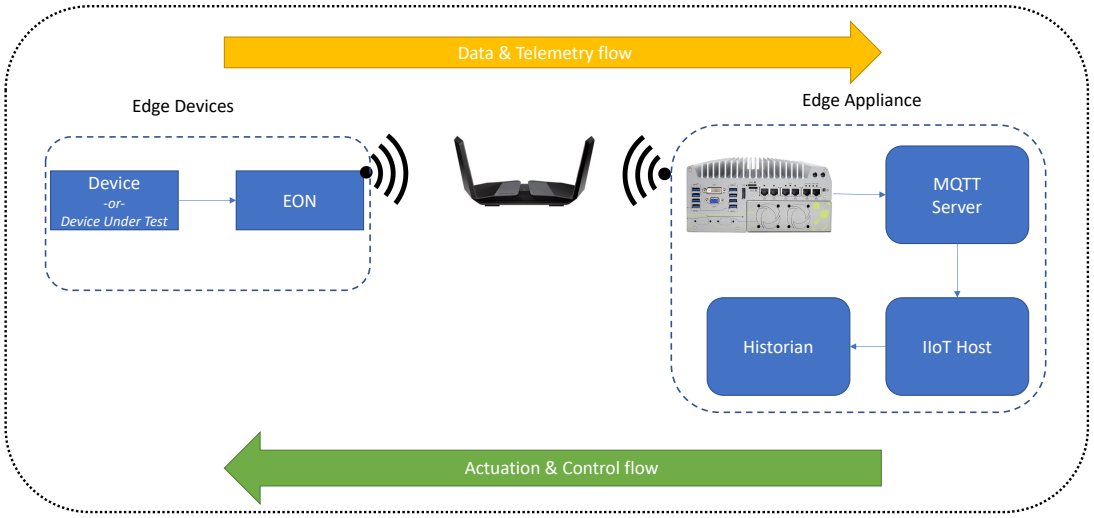


Figure **(6.1)** –System Test flows

Figure 6.3 illustrates our system and its components. Depending on the application class being tested, the system's design, configuration, and testing configuration may

vary. Nonetheless, the system's design can accommodate multiple configurations and performance test crtiteria. We will detail these on subsequent sections. We define the critical path within the system, which facilitates data and control flow.

```
Edge Device > Edge of Network Node > Event Broker > IIoT Host system
```

Figure 6.1 has two arrows: the top is for data flow, and the bottom is for control flow. Information flows from a sensor module to the EoN node and the IIoT Host system. The IIoT host system manages multiple devices and collects data for real-time monitoring and analysis of industrial operations. Historians are optional. The IIoT system sends commands and control data back to the end devices through the EoN node. The IIoT host system uses telemetry and performance data to control devices like actuators, warning lights, conveyors, or robotic arms.

For class 0-3 applications discussed in Chapter 2, latency is the roundtrip time for data to be sent from the device to the IIoT host and for a command to be returned to the device. For class 4-5 applications, latency is measured as the time it takes to complete an insert on the historian. In the following subsections, we will discuss the critical performance criteria for our testing.

- Reliability
- Latency
- Payload support
- Update Rate

6.2.1 Reliability

In industrial wireless networks, reliability means that the network can consistently and successfully perform its intended function without any issues. A reliable network is crucial for transmitting and receiving data accurately and promptly, which is necessary for real-time applications such as process control and monitoring to operate smoothly. Table 6.1 illustrates that reliability requirements vary from application to application. Combined with the guidance from NIST, there is a vast span of reliability requirements related to the application classes.

Application	Reliability Requirement	Reference
Smart Factory Systems	99.999%	[374]
Industrial Internet of Things (IIoT)	99.99%	[28]
Industrial drone control	99.9999%	[313]
Industrial AI	99.999%	[155]
Teleoperation in industry	99.9999%	[374]

Table (6.1) –Reliability requirements for various industrial applications

An industrial process requires a stable wireless network to operate safely and efficiently. It enables timely problem detection and resolution, preventing downtime and enhancing productivity. A dependable network also ensures accurate data transmission, minimising errors and inaccuracies. Conversely, an unreliable wireless industrial network can cause various problems that interrupt the process, such as:

- **Data loss:** Packets can be lost or delayed, resulting in stale or missing data.
- **Inaccurate data**: Packets can be corrupted or arrive out of order, leading to errors and inaccuracies.

- **Downtime:** Network failures can cause disruptions to the process, leading to downtime and lost productivity.
- **Safety issues:** An unreliable network can lead to unsafe conditions in critical applications, such as process control.

Industrial systems can require transmission rates up to 2000 Hz, that is to say the frequency at which messages are being transmitted in the system. Given this high-frequency data transmission, ensuring the reliability of message exchange within the system becomes critical.

Our approach to quantifying reliability includes an examination of sequence differences and temporal dynamics of message arrival. We denote the sequential identifier of each MQTT payload as p_s.

The sequence difference check evaluates the difference between sequential identifiers of consecutive messages $\Delta p_s = p_{s_{i+1}} - p_{s_i}$, where p_{s_i} is the sequential identifier of the i^{th} message. Valid messages increment the sequence number by one or experience a rollover to zero after reaching the maximum sequence number (255). Therefore, $\Delta p_s = 1$ or $\Delta p_s = -255$ are considered as reliable sequences.

We incorporate temporal dynamics into the reliability assessment and examine the time differences between consecutive messages. Given a set of timestamps t_{s_i} associated with each message, we calculate $\Delta t_s = t_{s_{i+1}} - t_{s_i}$. Then, over a rolling window of size N, we calculate the mean $\mu_{\Delta t}$ and standard deviation (measure of the variability in the time differences between consecutive message arrivals) $\sigma_{\Delta t}$ of Δt_s. Messages with $\Delta t_s \leq \mu_{\Delta t} + 3\sigma_{\Delta t}$ are marked as reliable regarding time difference.

We formulate the reliability as the ratio of 'reliable messages' ($M_{reliable}$) to 'valid messages' (M_{valid}):

$$Reliability = \frac{M_{reliable}}{M_{valid}}$$

A reliable message satisfies both sequence and time difference criteria. High-frequency transmission may cause rollovers, limiting sequence number to 255, thus affecting reliability. Incorporating the temporal aspect ensures comprehensive and accurate reliability metrics. MQTT protocol's inherent TCP/IP provides reliability via error-checking and retransmission mechanisms. Deploying the system on a Wi-Fi 6E network enhances wireless communication efficiency, reduces latency, and improves network performance in high-density areas, thus significantly contributing to message reliability.

6.2.2 Latency and Round Trip Time

Low latency is a critical factor in ensuring the safety, control, and optimal functioning of automation systems in industrial settings. Exceeding a certain latency threshold can result in severe repercussions. It is generally accepted in the industry that a latency below 10ms is required for real-time control and safety-critical applications, although the specific requirements can vary considerably depending on the application, as illustrated in Table 6.2.

In the evolving landscape of IIoT technology, M2M network traffic is adapting to accommodate more complex sensing needs, necessitating larger bandwidths. Consequently, payload selection for an application must be meticulously done,

considering the specific use case to maintain efficiency while meeting the increased data transmission demands.

Application	Latency Range	Reference
Industrial automation & control systems	<1 ms - 100 ms	[375]
Industrial safety systems	<10 ms	[376]
Industrial robotics & motion control	<1 ms - 10 ms	[377]
Remote monitoring & diagnostics	10 ms - 500 ms	[378]
Machine-to-machine (M2M) communication	<1 ms - 50 ms	[33]
Autonomous vehicles & real-time navigation	<1 ms - 20 ms	[379]
AR & VR applications in industry	<20 ms	[380]

Table (6.2) –Latency numbers for various industrial applications

A vital metric in edge-based IIoT systems is the round-trip time (RTT), which measures the duration a data packet takes to travel from the source to the destination and back, encompassing travel and processing times. RTT serves as a more precise performance gauge for real-time or near-real-time responses in complex networks.

In industrial environments, especially those utilizing SCADA systems, the necessity for acknowledgements or responses is paramount, making RTT a crucial performance indicator that encapsulates the total process time. The RTT can be calculated using the formula presented in Equation 6.1.

$$\text{RTT} = \frac{T_{total}}{W \times U} \tag{6.1}$$

where:

- RTT: is the average round-trip time for each update
- T_{total}: time taken to process all updates
- W: is the time window, the period in which updates are measured

- U: is the update rate, number of updates per unit of time

The performance benchmarks and requisite update rates are contingent upon the specific type of application. While class 0 applications adhere to NIST standards, classes 1-3 are guided by their operational demands in determining the update rate. It is essential to establish both "typical" and "minimum" latency requirements, which correspond to the end-to-end RTT, thereby ensuring the transmission and receipt of data within the stipulated window [50].

It is pivotal to distinguish between latency — the interval between the transmission and reception of a message — and RTT, which encompasses the time a message consumer takes to process or act upon the data within a cycle.

6.2.3 Payload Support

Our system design aims to facilitate handling a diverse range of application payloads characterized by varying types, frequencies, and bandwidth requirements. As sensor technologies advance, necessitating higher performance metrics, the network must remain robust and adaptable to meet evolving demands seamlessly.

A comprehensive approach to network performance evaluation goes beyond just focusing on the payload size; it also encompasses considerations for network and transport overheads. In our analysis, we adopt this holistic perspective, considering the different layers of network design to provide a more rounded insight into the network's performance.

A notable feature of the SparkplugB protocol is its efficiency in data conversion between formats such as JSON and Protobufs. Protobufs facilitate more compact

message structures, enhancing storage efficiency and transmission speed. This serialization process curtails latency and augments scalability through strong type-checking and schema evolution capabilities, allowing for a flexible data representation. Consequently, the conversion from JSON to Protobufs orchestrated by SparkplugB is pivotal in optimizing data communication in industrial IoT systems.

In the dynamic landscape of industrial wireless networks, there is a pressing need to support payloads with diverse attributes, including varying sizes and response times. This necessitates a system that can adeptly handle sensors transmitting data at disparate intervals, underscoring the importance of flexibility in network design. The industrial environment often demands low latency and the transmission of smaller packets at precise intervals. The categorization of payload types, in line with the criteria outlined in Table 6.3, considers the specifics of Wi-Fi packets and Sparkplug communications, offering a detailed breakdown of the payload and its constituent sizes. Figure 6.2 further details the details of the payload structure.

Application	**Payload**(B)	**Network**(B)	**Total**(B)
Class 0	6	30	36
Class 1-2	17	30	47
Class 3	33	30	63
Class 4	16	30	46

Table **(6.3)** –Payload sizes for application class in Bytes

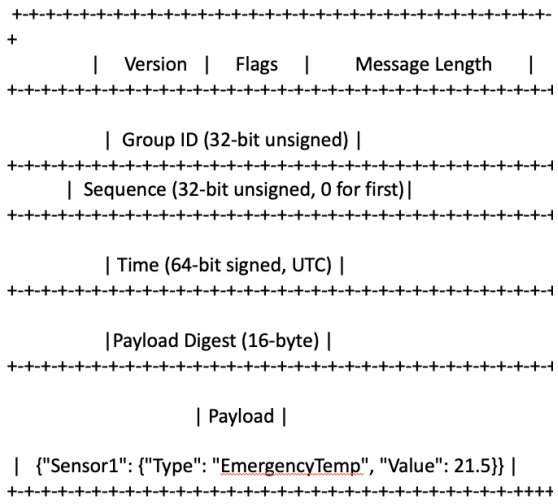


Figure **(6.2)** –Example payload format including network and SparkPlug data

6.2.4 Update rate

The update rate, expressed in updates per second (UPS) or hertz (Hz), delineates the frequency at which sensors and actuators relay data to a central controller or network. While a high update rate facilitates precise data collection, it potentially escalates the network load. Conversely, a reduced update rate might yield outdated data.

In the context of a wireless industrial system, it is imperative to accommodate the diverse update rates necessitated by various applications utilizing the system. The update rate spectrum spans from 1 kHz to 125 kHz, encompassing various applications from motor controller drives to alerts.

Established industrial wireless protocols such as WirelessHART and ISA100.11a stipulate the minimum and maximum update rates to foster effective communication between devices and networks. These guidelines, grounded in the specific demands of the application and the network's capacity, dictate the data trans-

mission frequency. For instance, while WirelessHART caps the update rate at 10 Hz, ISA100.11a sets the floor at 1 Hz, striking a harmonious balance between the urgency for current data and the network's constraints.

Manufacturing applications exhibit diverse requirements, with specific scenarios demanding high-frequency update rates. The efficacy of data processing is intrinsically tied to both the payload size and the frequency of updates. Montgomery et al. delve into the nuances of update rates pertinent to various ISA class types, offering a detailed exploration of this aspect [373].

6.2.5 Jitter

Jitter, characterized as the packet delay fluctuation, is pivotal in wireless industrial networks. It represents the deviation from the maximum permissible latency, causing packets to reach their destination in a disordered sequence and inducing delays between network packets. This phenomenon can significantly impair real-time applications such as process control and monitoring by fostering errors and inaccuracies due to the asynchronous arrival or delay of data. Jitter can be caused by a myriad of factors, including:

- Interference from neighbouring wireless devices or networks, leading to packet delays or losses.
- Restricted network bandwidth engendering congestion and subsequent delays.
- Limited processing prowess or memory in wireless devices, resulting in data transmission delays.

- Environmental determinants, such as distance, terrain, and physical barriers, can attenuate signal strength and induce delays.

Metrics such as mean packet delay variation (MPDV) or root mean square (RMS) jitter can be employed to measure jitter. Vigilant jitter monitoring is indispensable in wireless industrial networks to safeguard the efficiency of real-time applications and ensure the timely and accurate transmission of data.

Application	**Jitter Range (ms)**	**Reference**
Industrial automation & control systems	<1 - 10	[381]
Industrial safety systems	<5	[382]
Industrial robotics & motion control	<1 - 5	[53]
Remote monitoring & diagnostics	1 - 50	[383]
Machine-to-machine (M2M) communication	<1 - 20	[384]
Autonomous vehicles & real-time navigation	<1 - 10	[385]
AR & VR applications in industry	<10	[386]

Table (6.4) –Jitter specifications for various industrial applications (illustrative)

6.3 Experimental Approach and Configuration

In this study, we adhere to the ISA-TR100.00.03-2011 standard delineated by the International Society of Automation to classify and categorize the application types subjected to our system testing [387]. This standard segregates automation into six distinct classes based on their criticality level, with Class 0 denoting the highest criticality and Class 5 representing less critical applications. We excluded Class 5 applications from our testing scope, considering the sufficiency of existing wireless technologies in managing them. Our focal point was scrutinizing wireless systems for automation classes 0, 2, and 4. Given the practical constraints and to avoid a time-intensive process, we amalgamated classes 1-3, selecting class 2 as a representative category. This approach entailed testing each designated

category through our established test configuration, modulating parameters such as the update rate to ascertain the system's performance. This strategy yielded functional and representative results, aligning with our testing standards.

Our evaluation metric encompassed both *typical* and *strict* performance criteria pertinent to each class. The rationale behind adopting this dual-faceted approach is multi-fold, encompassing the following aspects:

- **Testing System Limits**: It is imperative to scrutinize systems under stringent conditions to delineate their maximal capabilities and anticipate their behaviour in worst-case scenarios. This is particularly salient in safety-critical applications where failures can engender severe repercussions.
- **Benchmarking**: Subjecting the system to strict conditions facilitates the establishment of a performance benchmark, thereby attesting to its quality and reliability. Concurrently, testing under typical conditions offers a realistic gauge of its routine performance, accommodating a benchmarking spectrum that caters to various application prerequisites.
- **Resilience**: Resilience is a system's ability to maintain consistent performance even under challenging circumstances. A resilient system can adapt without performance degradation, ensuring reliability and stability under increased load or faults. Testing under strict conditions can assess Resilience and ensure reliable performance in typical settings.
- **System Optimization**: The insights garnered from testing under both strict and typical conditions serve as a reservoir of data instrumental in system optimization. Identifying areas where the system excels or falls short

under varying conditions guides targeted improvements, from physical layout alterations to protocol optimizations.

Table 6.5 illustrates the performance requirements we utilized for testing, summarizing the criteria for various application types represented by different classes. Each column in the table represents an application class, accompanied by a typical application type. At the same time, the rows delineate the performance criteria along with the test values employed in our testing. Notably, the application classes exhibit similarities and differences in terms of these criteria.

For our tests, we focused on Class 0, Class 2, and Class 4 applications. We made a specific deviation from the table for the Class 0 tests, where we increased the update rate to 125 Hz to facilitate a more stringent testing environment. This adjustment explored the system's performance under higher update rates, providing a comprehensive view of its capabilities.

Application Type / **Performance Criteria**	Functional Safety: Class 0	Discreet Manufacturing: Class 1	Process Automation: Class 2	Operator Monitoring: Class 3	Condition monitoring: Class 4
Reliability	$10^{-}9$	$10^{-}7$	$10^{-}5$	$10^{-}4$	$10^{-}3$
Latency(ms)	10	12	50	15	100
Jitter	24	30	30	6	300
Payload Size(B)	24	64	64	64	33KB
Update Rate(Hz)	125	1000	125	1000	125
Range	10	10	10	10	10

Table (6.5) –Summary of performance requirements for Wireless Industrial Network

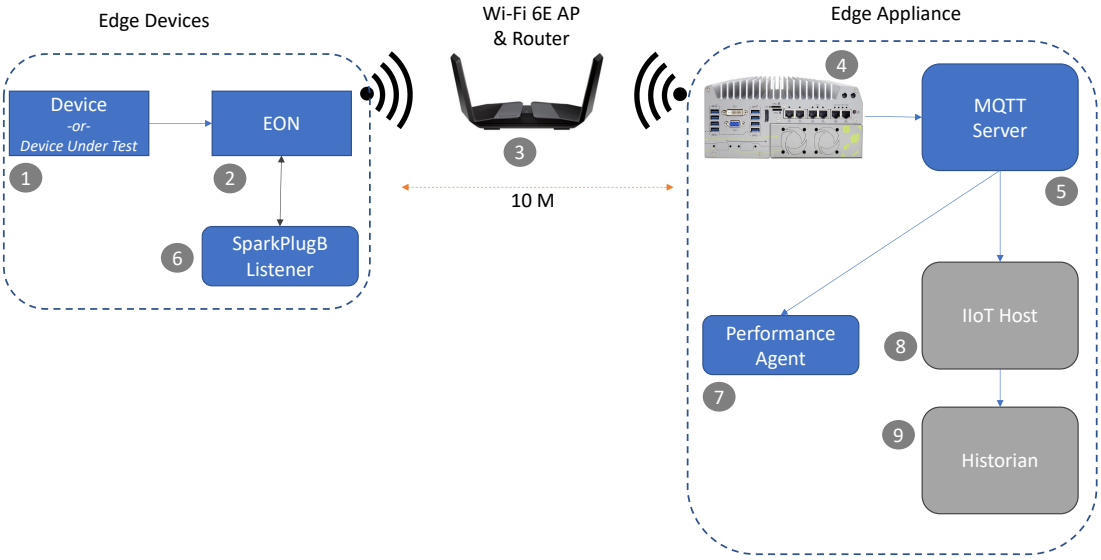


Figure **(6.3)** –Industrial Wireless System test configuration architecture

Primary Components of the test system

Component	Description
1. Sensor node	A physical unit interfaced with the EoN node, responsible for gathering telemetry data through sensors.
2. EoN Node	Serves as a gateway providing connectivity and protocol mapping functionality for associated devices.
3. Netgear NightHawk	802.11ax and Wi-Fi 6E Access point supporting 6GHz.
4. Industrial PC	Nuvo-900- Intel 13th Gen with 6 X 2.5Gb ethernet. Providing network management and hosting for subsystems.
5. MQTT Server	Facilitates message passing to the system through the support of SparkPlug and MQTT protocols.
6. SparkPlug Listener	A Python-based MQTT client, providing processing and timestamping for outbound and inbound SparkPlugBv1.0 messages and message monitoring
7. Performance Agent	Python-based agent provides application performance telemetry, offering metrics and reporting for application layer performance which produces.
8. IIoT host	An MQTT client, serving as the primary host node of the system. Its responsibilities include monitoring, controlling connected EoN nodes, and overseeing data acquisition within the system.
9. Historian	An ancillary application node connected to the primary node. It archives TimeSeries telemetry data transmitted from Devices and EoN nodes.

6.3.1 Testing Duration

We have used various sources to determine the performance criteria for Wi-Fi-based networks, including NIST and ETSI, TR-398 from the Broadband Forum

Class	Test Duration	Justification
Class 0 (Safety Systems)	2 hours test with high-frequency messaging	Critical systems necessitate testing under worst-case scenarios. Testing with high-frequency messages during a short, intensive period can effectively surface any issues.
Class 1-3 (Control systems)	Consistent performance testing under expected load 1 hour	These systems require steady performance. Testing under expected load continuously can identify trending performance issues or stability problems.
Class 4-5 (CBM, PHM Examples)	2 hours with frequency 'events' triggering maintenance or anomalies	These systems work over extended periods with less frequent messaging. Simulating triggering events can provide more informative insights than long-running tests.

Table **(6.6)** –Test runs for industrial application classes

and a report by UK telecommunications regulator Ofcom [388]. Although the application domains differ, both sources provide relevant and authoritative metrics for Wi-Fi-based networks. For instance, Ofcom recommends a testing duration of 120 seconds, excluding the initial and final periods, to ensure continuous data measurements. On the other hand, the Broadband Forum does not specify a testing duration, nor do NIST or ETSI reports. However, testing durations are critical in Industrial Wireless Networks, as more extended test periods allow dynamic or spontaneous events to occur.

Industrial environments are markedly different to residential settings. However, the network performance testing criteria are essentially the same. A *critical difference* is the performance levels required for industrial environments as outlined in Table 6.5. The other notable difference is the interference and obstructions. Our

approach to testing durations is to tie the testing duration to the application domain, that is, to align the testing cycle with the cycle time of the processes. We contribute the following test durations for each application class, with justification.

6.3.2 Data sampling approach

We utilised two data collection and analysis methods to evaluate network performance comprehensively: statistical sampling and active probing. This approach allows for a comprehensive system evaluation under controlled and real-world conditions.

We collected unbiased and representative data from the network by combining statistical sampling and active probing. Statistical sampling involves taking random or stratified samples to understand overall network performance in real-world scenarios, such as Irish Manufacturing Research (IMR). On the other hand, active probing involves injecting test packets into the network to measure performance under specific conditions. Our active probing included using payload data directly related to the application class type and the update rate of the data, ensuring that the packet data is as close to real-world application-level data as possible.

Our approach and methodology involved the following steps:

- **Defining Performance Objectives**: We established the performance requirements for Reliability, jitter, and latency based on the specific needs of the industrial application.

- **Identifying key system performance variables**: We determined the relevant systems variables.
- **Statistical sampling methodology**: We collected data based on the timing outlined in 6.3.1. The following formula was used to determine the samples, N, collected for testing:

$$N = \lambda * \tau * \sigma \tag{6.2}$$

where:

  - N = Number of samples collected
  - λ = frequency in Hz
  - τ = duration of test in minutes
  - σ = seconds in a minute

6.3.3 Frequency band selection

Testing Wi-Fi 6E in an industrial environment is essential to verify its durability, efficiency, and suitability for industrial applications. Unlike its predecessors, Wi-Fi 6E operates in the 6GHz frequency band, which provides additional spectrum that was not available before. Additionally, this frequency band is less crowded than the 2.4GHz and 5GHz bands, which results in fewer interferences from other devices, allowing for more reliable and faster connections. It is crucial to validate the performance at this frequency since it is the foundation of Wi-Fi 6E's improved capabilities.

Rigorous testing is required under realistic industrial conditions to ensure that the propagation characteristics and potential interference sources at 6GHz differ from those at 2.4GHz or 5GHz. In-situ testing is necessary to guarantee that the network can maintain its throughput, reliability, and latency performance, even in the complex and often challenging radio environments in industrial settings. This validation process is critical to optimize the full potential of Wi-Fi 6E and ensure that it meets the demanding requirements of industrial applications.

6.3.4 Timing and synchronisation

Accurate timing and reliable device communication are essential for the Network Time Protocol (NTP) and the Sparkplug B framework. These tools allow for stateful message exchange between devices and applications. However, discrepancies in timing can lead to incorrect operations, misinterpreted data, and system failures. NTP synchronises clocks, providing a consistent time reference and preventing inconsistencies in MQTT message order. Without NTP, clock drift could cause outdated information and incorrect actions. Therefore, NTP is crucial for maintaining data integrity, system performance, and correct operations.

Before implementing an NTP server into our test system, we noticed random and high volatility in our RTT and Jitter tests. For instance, we observed RTT ranges from a minimum of $4ms$ to a maximum of $233ms$ in various difficulties. After implementing NTP, we still observed high RTT and Jitter, but the variability was significantly reduced in the network.

6.3.5 Network and application testing

In industrial settings where real-time data acquisition is essential, reliability testing is critical for SparkPlug B and MQTT implementations. SparkPlug B, built on MQTT, is frequently used to monitor large-scale infrastructure and gather data from heavy machinery. In such situations, the integrity and timeliness of data are crucial, and any inaccuracies or untimely delivery can have severe operational and safety consequences.

To measure system reliability, it is necessary to conduct application-level reliability testing that analyses both network and MQTT metrics. While network-level parameters such as packet loss, latency, and jitter are essential factors, they alone cannot fully capture the complexities of MQTT or SparkPlug B implementation. Therefore, analysing both network and MQTT metrics is vital to fully understanding the system's performance.

6.3.6 Summary Statistics

Summary statistics facilitate comparative analysis between different groups or conditions in a study, making it easier for a broad audience to understand the results. Additionally, they provide foundational information for more advanced statistical analyses, like hypothesis testing and regression analysis.

When analyzing data, it's crucial to consider central tendency and dispersion. The median (50%) represents the central value of the dataset and is not affected by outliers, offering a more accurate representation of the dataset's central point.

The minimum and maximum values indicate the range within which all data points lie, helping to identify any outliers.

Quartiles (25% and 75%) aid in understanding data distribution by dividing the dataset into quarters. This provides a deeper understanding of the dataset's variability and distribution around the median. The median and quartiles are resistant to outliers, providing a more robust measure of central tendency and dispersion, ensuring the summary statistics represent most data points.

6.3.7 5GHz Testing

The decision to test the wireless industrial network at 5GHz before 6GHz was based on strategic considerations. The 5GHz frequency is widely adopted and provides a benchmark for comparisons. Testing at 5GHz allows for diagnosing fundamental system issues early and enhances the validity of test outcomes. By first testing the system at 5GHz, we were able to establish a baseline performance for the system. This provides a valuable reference point when we examine how the system performance adapts to the challenges associated with the 6GHz frequency. Therefore, this staged testing approach is both methodologically sound and practically advantageous.

Summary statistics from the testing at 5GHz are presented in Tables 6.7 and 6.9

	RTT *(ms)*	**Throughput** *(bps)*	**Jitter** *(ms)*	**Reliability** *(mls%)*
count	877 056	877 056	877 055	877 056
mean	6.47	85 998	0.87	$9.999\,977 \times 10^{1}$
std	1.43	14 611	0.94	$1.421\,086 \times 10^{-13}$
min	3.00	2564	0.00	$9.999\,977 \times 10^{1}$
25%	6.00	76 571	0.00	$9.999\,977 \times 10^{1}$
50%	6.00	89 333	1.00	$9.999\,977 \times 10^{1}$
75%	7.00	90 666	1.00	$9.999\,977 \times 10^{1}$
max	209.00	181 333	107.00	$9.999\,977 \times 10^{1}$

Table **(6.7)** –Class 0 5GHz Industrial System Test Data

	RTT *(ms)*	**Throughput** *(bps)*	**Jitter** *(ms)*	**Reliability** *(mls%)*
count	1 614 680	1 614 680	1 614 680	1 614 680
mean	8.63	365 792.50	2.69	$9.996\,742 \times 10^{1}$
std	9.35	257 134.27	2.49	$7.988\,954 \times 10^{-2}$
min	1.00	5309.42	0.00	$9.971\,608 \times 10^{1}$
25%	6.00	236 800.00	1.00	$9.999\,476 \times 10^{1}$
50%	8.00	297 000.00	2.00	$9.999\,597 \times 10^{1}$
75%	10.00	4 000 000.00	2.00	$9.999\,616 \times 10^{1}$
max	446.00	2 408 000.00	434.00	$9.999\,649 \times 10^{1}$

Table **(6.8)** –Class 2 5GHz Industrial System Test Data

	RTT *(ms)*	**Throughput** *(bps)*	**Jitter** *(ms)*	**Reliability** *(mls%)*
count	779 215	779 215	779 215	779 215
mean	6.93	352 767.99	0.83	$9.997\,098 \times 10^{1}$
std	7.50	86 877.25	2.00	0.001 689
min	2.0	3681.06	0.00	99.987 170
25%	5.00	280 000.00	0.00	99.998 432
50%	6.00	369 333.33	1.00	99.998 896
75%	8.00	440 000.00	1.00	99.999 069
max	602.00	1 128 000.00	595.00	99.999 272

Table **(6.9)** –Class 4 5GHz Industrial System Test Data

6.4 Class 0 system testing

Class 0 industrial applications are the most consequential, as they ensure the safety and protection of humans and equipment. These applications require high reliability and low latency, with an end-to-end latency of only $5ms$. Class 0 applications typically use smaller payload sizes to optimise network efficiency, sending only the necessary data to avoid transmission delays.

Class 0 systems require the highest levels of reliability; for example, IEC 61508 is an international functional safety standard providing a framework for the functional safety of electrical equipment used in industrial (and beyond) settings [389]. The standard uses Safety Integrity Levels (SIL) to allocate severity and frequency expectations that must be met to ensure safety [390]. In Europe, machine safety overseen by the EN-ISO 13849-1 and EN-IEC 62061 standards use

performance levels PLs. SIL and PL levels are designated in ascending order, with each increasing SIL level having a greater risk of value and stricter requirements.

6.4.1 Experimental setup and Configuration

The test environment configuration is detailed in 6.4. The payload used is an emergency temperature signal value. The total payload transmitted was 36 Bytes. The distance between the EoN and Edge appliance was 10m, with a mostly clear line of sight (LOS). This protocol describes the steps in transmitting sensor telemetry from an Edge Device to an Edge of Network (EoN) device and subsequently to the Industrial Internet of Things (IIoT) host.

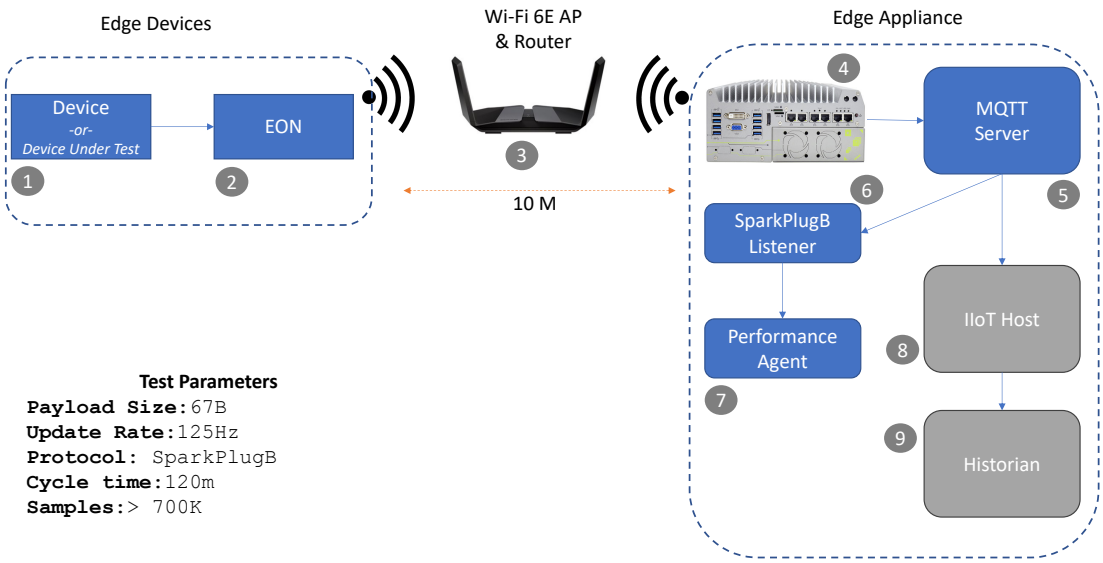


Figure **(6.4)** –Test configuration for Class 0 Applications

Testing Principal

1. Sensor telemetry send from Edge Device to EoN device.
2. EoN device transmits data wirelessly to Wi-Fi 6E AP.
3. AP transmits EON Data to Wi-Fi 6E industrial PC.
4. HiveMQ-based MQTT server collects SparkPlugBv1.0 messages.
5. SparkPlugBv1.0 Listener filters for DDATA messages, parses payload and timestamps data, captures payload and writes to memory.
6. Performance Agent processes data into performance metrics and telemetry, such as RTT and Jitter reliability data. Post processes summary statistics and plot
7. IIoT Host monitors all standard SparkplugBv1.0 data and writes messages to TimescaleDB.
8. TimescaleDB persists data to the database.

```
{
        "timestamp": 1620979200000,
        "metrics": [
        {
                "name": "alert",
                "alias": 0,
                "timestamp": 1620979200000,
                "dataType": "string",
                "value": "Temperature Threshold Exceeded",
                "properties": {
                        "alertType": {
                                "type": "string",
                                "value": "Temperature"
                        },
                        "alertLevel": {
                                "type": "string",
                                "value": "Critical"
                        }
                }
        }
        ] }
```


Figure **(6.5)** –Basic Alert Message (ISA-5.00.01 Class 0)

6.4.2 Results

Table 6.10 contains the results of Class 0 application testing. Results which meet the application class test criteria are coloured blue and bolded, whereas results which do not meet the application test criteria are coloured in red and italicised.

	RTT *(ms)*	**Throughput** *(bps)*	**Jitter** *(ms)*	**Reliability** *(mls)*
count	900 000	900 000	899 999	900 000
mean	9.29	65 174.71	0.47	99.999 131
std	2.92	26 598.91	0.77	0.000 586
min	0.91	6359.00	0.00	99.996 000
25%	6.58	47 481.76	0.13	99.999 194
50%	9.72	55 575.95	0.32	99.999 345
75%	11.37	82 008.74	0.65	99.999 399
max	84.29	600 437.62	77.22	99.999 568

Table **(6.10)** –Class 0 6GHz Industrial System Test Data

6.4.2.1 Reliability Analysis

The reliability analysis indicates a consistent and stable network and network connectivity. The mean reliability is 99.999 131 %, with a standard deviation of 0.000 586 %. The minimum and maximum reliability values are 99.996 000 % and 99.999 568 %, respectively. The 25th, 50th (median), and 75th percentiles are 99.999 194 %, 99.999 345 %, and 99.999 399 %, respectively.

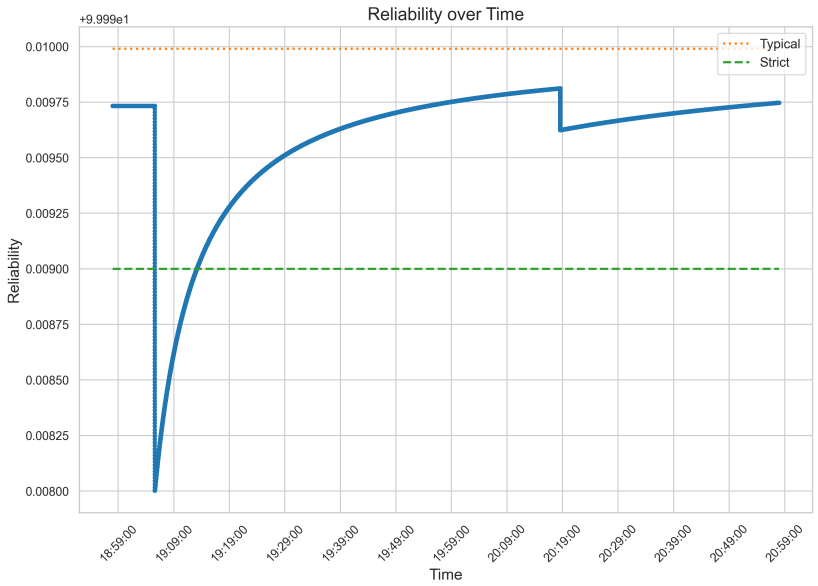


Figure **(6.6)** –Class 0 Reliability time series

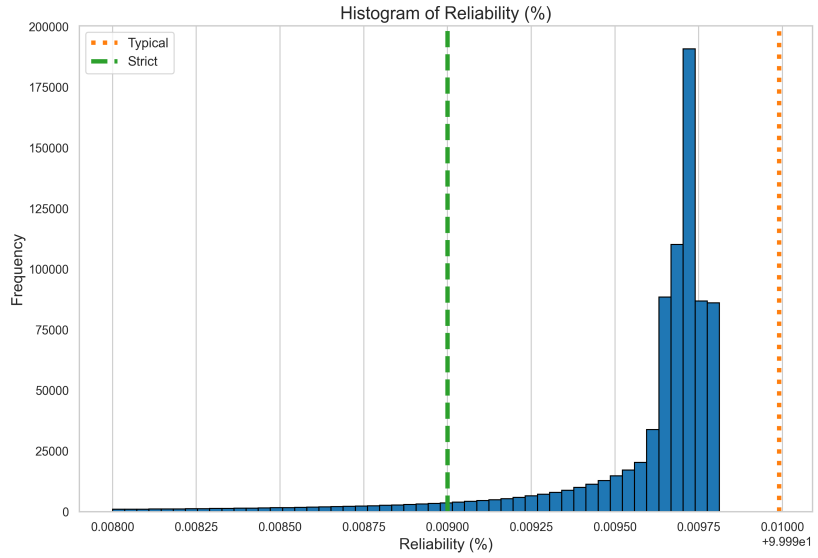


Figure **(6.7)** –Class 0 Reliability Histogram

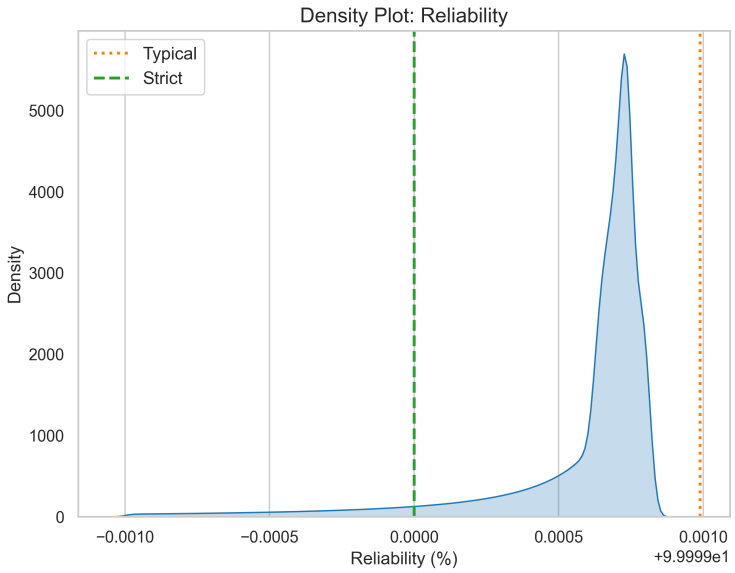


Figure **(6.8)** –Class 0 Reliability density diagram

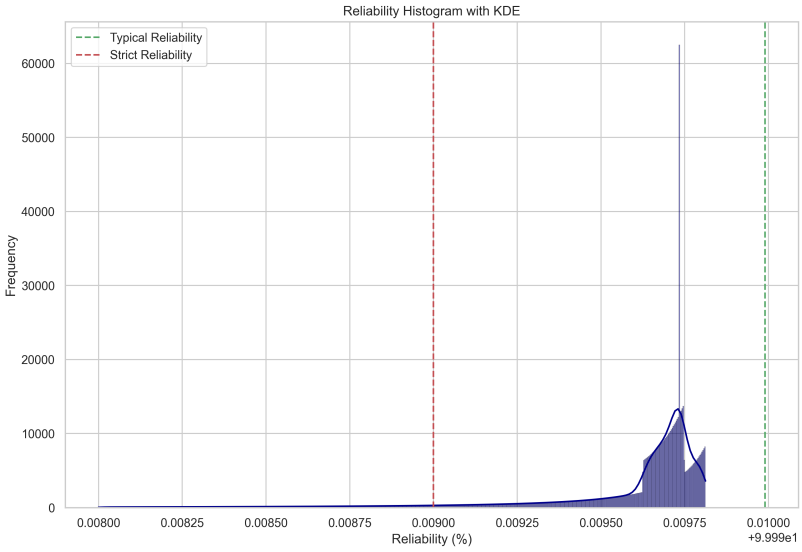


Figure **(6.9)** –Class 0 Reliability histogram with KDE

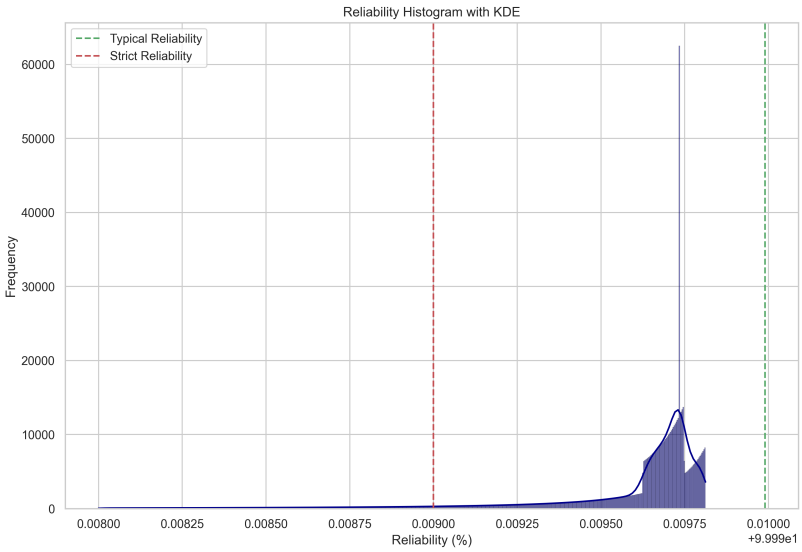


Figure **(6.10)** –Class 0 Violin plot

6.4.2.2 Round Trip Time Analysis

The Round-Trip Time (RTT) is a crucial metric that measures the time a packet travels from the sender to the receiver and back 6.11. The average RTT for the Wi-Fi 6E-based industrial network is approximately 9.29 ms. The standard deviation of 2.92 ms indicates the variability in RTT measurements. The minimum RTT observed is 0.91 ms, while the maximum reaches 84.29 ms. The 25th, 50th (median), and 75th percentiles are 6.58 ms, 9.72 ms, and 11.37 ms, respectively.

A low RTT is desirable in industrial networks, ensuring prompt communication between devices. The relatively low mean RTT suggests efficient round-trip data transmission in the network. However, a relatively large standard deviation and higher maximum RTT indicate occasional delays and potential performance variability.

It is worth noting that in the experimental setup we adopted, we did not use any of the QoS features of the SparkplugBv1.0 protocol. The reason was to observe the system's performance without additional techniques for optimising the application infrastructure.

These techniques remain viable options for future testing and system development.

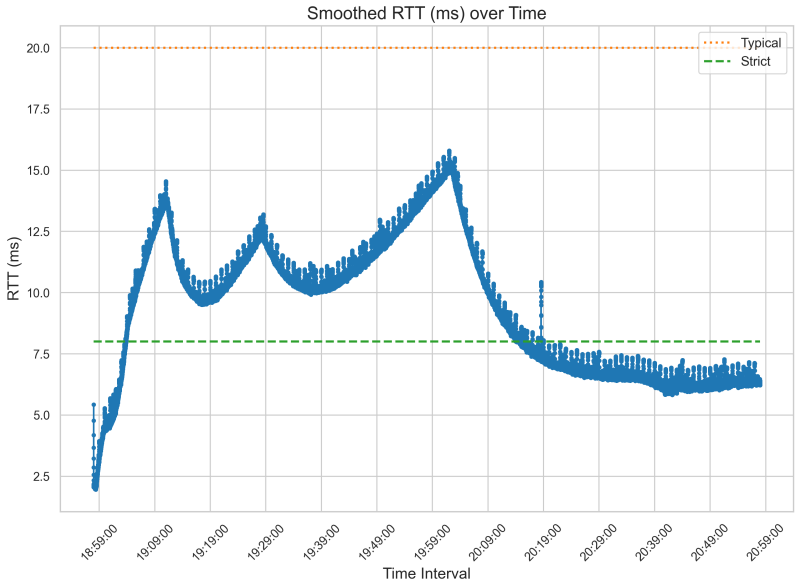


Figure **(6.11)** –Class 0 Round Trip Time smoothed over samples collected

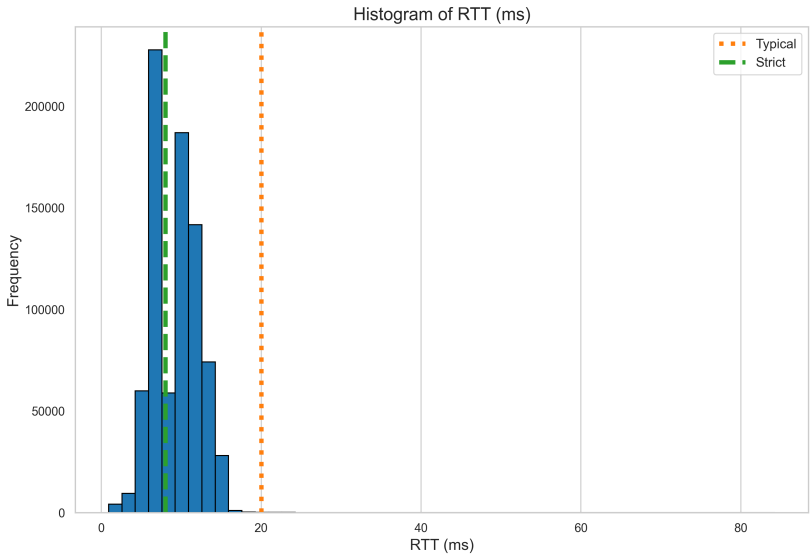


Figure **(6.12)** –Class 0 round trip time histogram

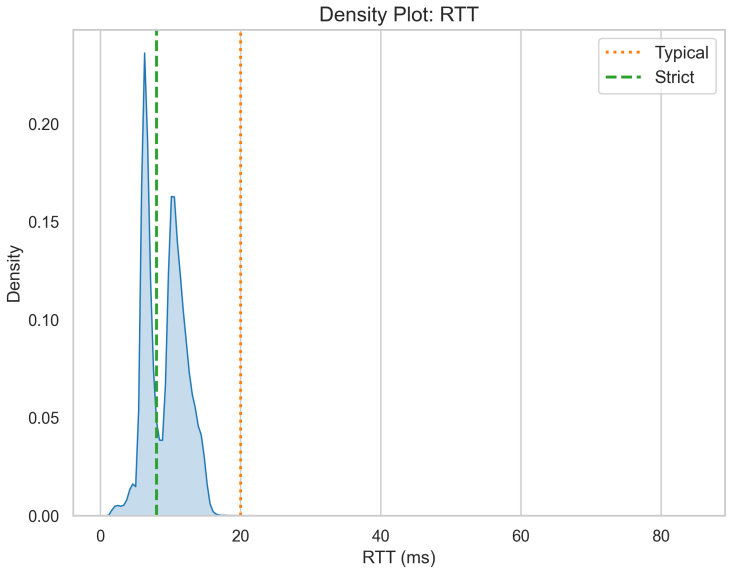


Figure **(6.13)** –Class 0 round trip time density

6.4.2.3 Throughput

The average throughput of the Wi-Fi 6E-based industrial network is approximately 65 174.71 Mbit s^{-1}. The standard deviation of 26 598.91 Mbit s^{-1} indicates considerable variation in throughput measurements. The minimum observed throughput is 6359.00 Mbit s^{-1}, while the maximum reaches 600 437.62 Mbit s^{-1}. The 25th, 50th (median), and 75th percentiles are 47 481.76 Mbit s^{-1}, 55 575.95 Mbit s^{-1}, and 82 008.74 Mbit s^{-1}, respectively.

There are several potential explanations for the above throughput variations. Firstly, as SparkPlugBv1.0 uses TCP as its transport layer, packet retries. In our testing, we elected to transmit data at the upper end of the payload, with update rates of 125 hertz. In practical applications, a safety system would likely not send that volume of data.

The provided mean throughput suggests the network can handle a substantial amount of data. However, the relatively large standard deviation and high maximum throughput indicate possible congestion and variability in network performance.

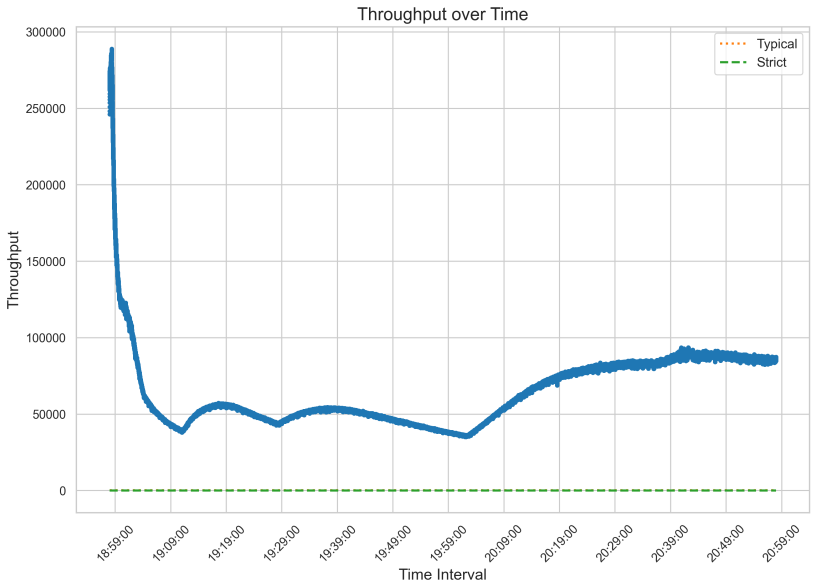


Figure **(6.14)** –Class 0 Throughput

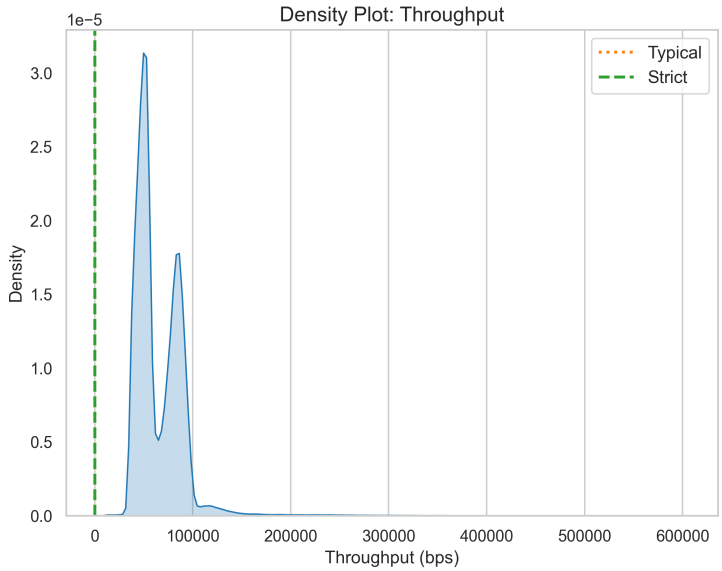


Figure **(6.15)** –Class 0 Throughput density plot

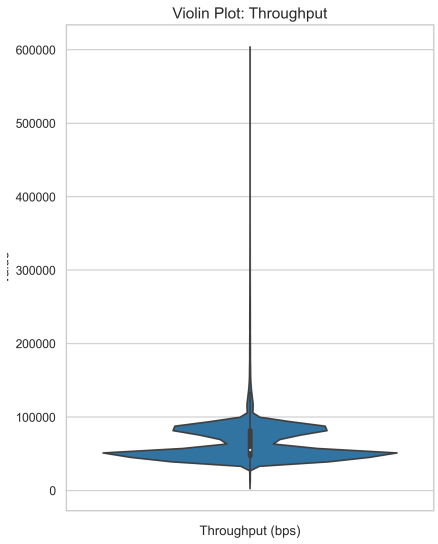


Figure **(6.16)** –Class 0 Throughput Violin plot

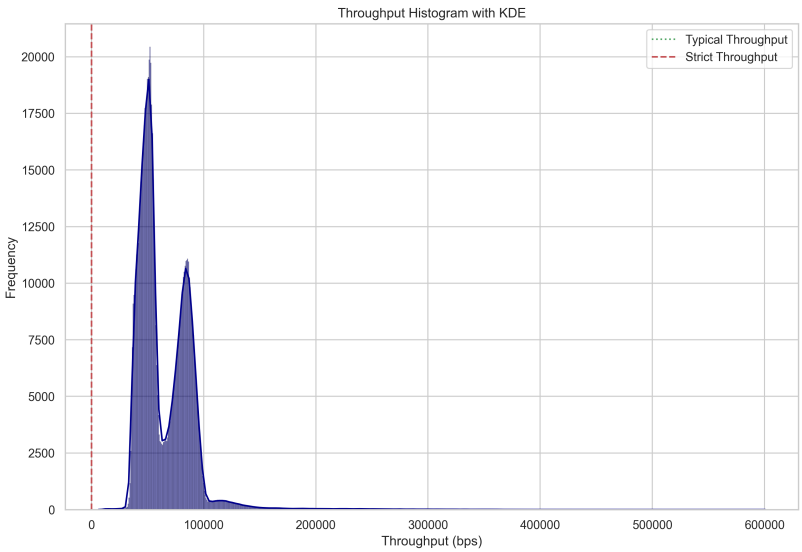


Figure **(6.17)** –Class 0 Throughput Historgram with KDE

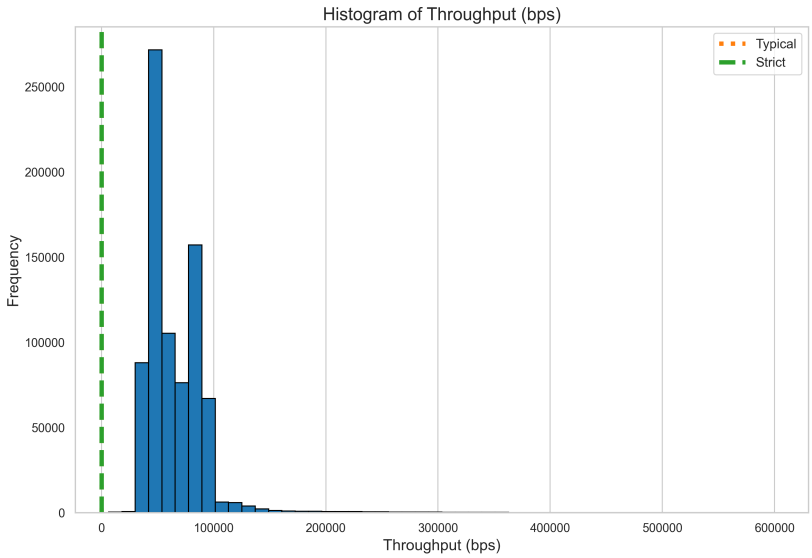


Figure **(6.18)** –Class 0 Histogram Histogram

6.4.2.4 Jitter Analysis

The mean jitter for our network is 0.47 ms. The standard deviation of 0.77 ms indicates variability in jitter measurements. The minimum jitter observed is 0.00 ms, while the maximum reaches 77.22 ms. The 25th, 50th (median), and 75th percentiles are 0.13 ms, 0.32 ms, and 0.65 ms, respectively.

The relatively low mean jitter suggests good network stability and minimal variation in packet delivery times. However, a more significant standard deviation and higher maximum jitter imply occasional delays and potential performance fluctuations. During our testing, we observed occasional increases in jitter, which did not seem to be network related. During the testing, we did not capture any network-specific issues. However, jitter appeared related to some limitations of using general-purpose computing.

We deliberately tried not to implement many optimisations during our testing, so these techniques could be included as future or further improvements after we established a performance baseline for the system.

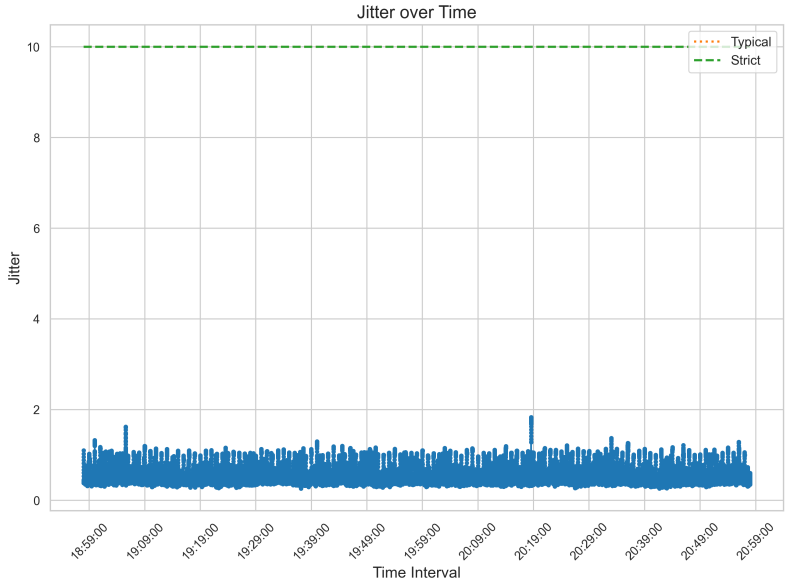


Figure **(6.19)** –Class 0 Jitter smoothed over samples collected

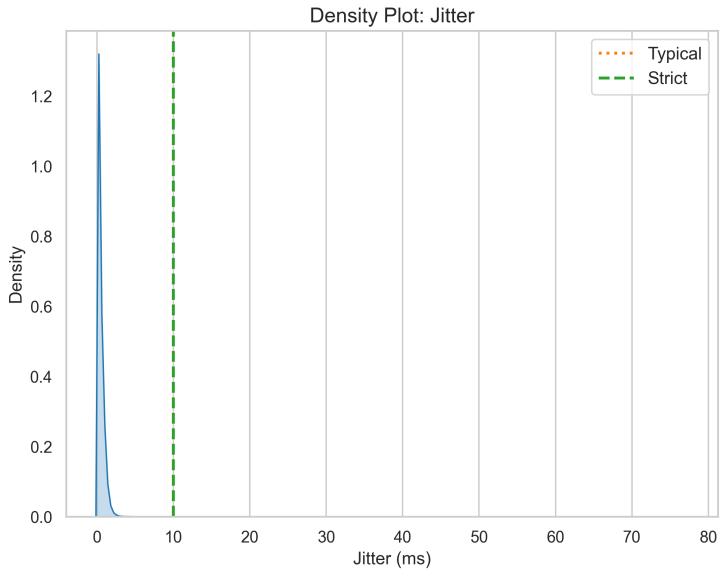


Figure **(6.20)** –Class 0 Jitter density

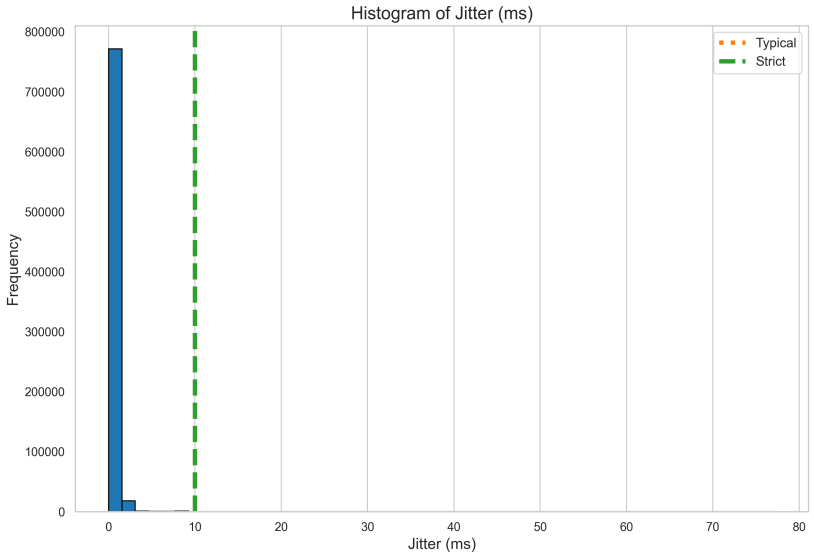


Figure **(6.21)** –Class 0 Jitter Histogram

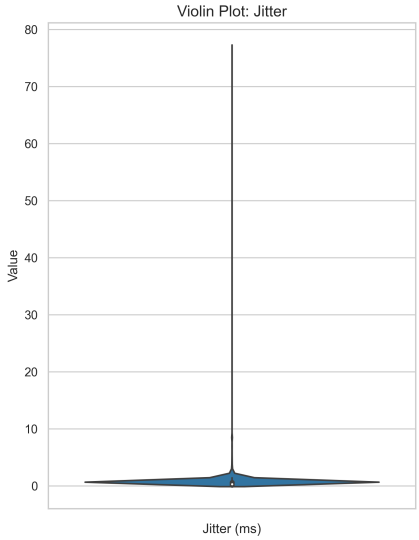


Figure **(6.22)** –Class 0 Jitter Violin plot

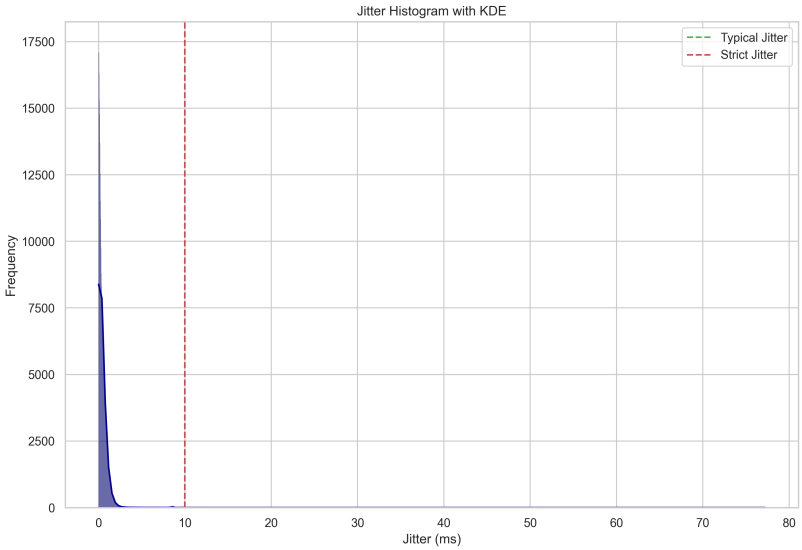


Figure **(6.23)** –Class 0 Hi

6.5 Class 2 system testing

Class *1*, *2*, and *3* applications belong to different industrial system categories but share specific requirements. We elected to test class 2 systems in our experiments. Let us briefly recap these application classes.

- In *Class 1*, the focus is on closed-loop regulatory systems that involve critical control functions demanding rapid response times and unwavering reliability. Examples of such systems include motors, compressors, and bio-reactors, where actuators are responsible for controlling process variables without human intervention. These systems operate based on feedback from sensors, controllers, and actuators. The closed-loop nature entails measuring, monitoring, and controlling the process by comparing actual outputs with desired values.

- *Class 2* encompasses loop supervisory control systems commonly employed in SCADA-type (Supervisory Control and Data Acquisition) systems for sequential or batch control. Although these systems have slightly less stringent latency requirements than Class 1, they play a crucial role in industrial operations and still have pretty stringent requirements.

  Class 3 applications typically involve human interaction within the control loop. This class includes scenarios where humans control specific aspects of the system, such as moving equipment through a control system. Latency requirements in Class 3 can be similar to those in Class 1. Examples of Class 3 applications encompass systems utilising robotics or hydraulics, where users interact with the system via button controls, switches, or joysticks.

The system's reliability remains high at 10^{-5}. We use the same range consistent with the measured ranges for IMR. Generally speaking the requirement across all three classes 10^{-7}, important in closed-loop control systems [391, 48]. however, as we were implementing our testing without any reliability techniques except for those present in the underlying TCP protocol, we wanted to ascertain performance without these techniques present, such as the QoS features of MQTT.

For typical and strict performance, we set the RTT at $20ms$ and $8ms$, respectively. To cover the manufacturing cell in IMR, we use a range of $10m$. The payload was set at $270B$ to test the system at high values. We set the update rate at $1000Hz$ in line with our testing strategy, but based on other testing, it could be as low as $25Hz$ [392].

6.5.1 Experimental setup and configuration

The configuration for the test environment is described in 6.24. We used this configuration to monitor a process control system for additive manufacturing. Specifically, we monitored a 3-D printing process and collected telemetry related to that process. Filament-based printing requires careful monitoring of parameters like temperature, speed, and diameter. Other parameters like print speed, infill density, layer height, and support structures also impact quality. A sample of the class 2 payload is illustrated in 6.25. The SparkPlugB payload tool optimizes the process by transmitting relevant data in real-time, allowing for adjustment of parameters and troubleshooting

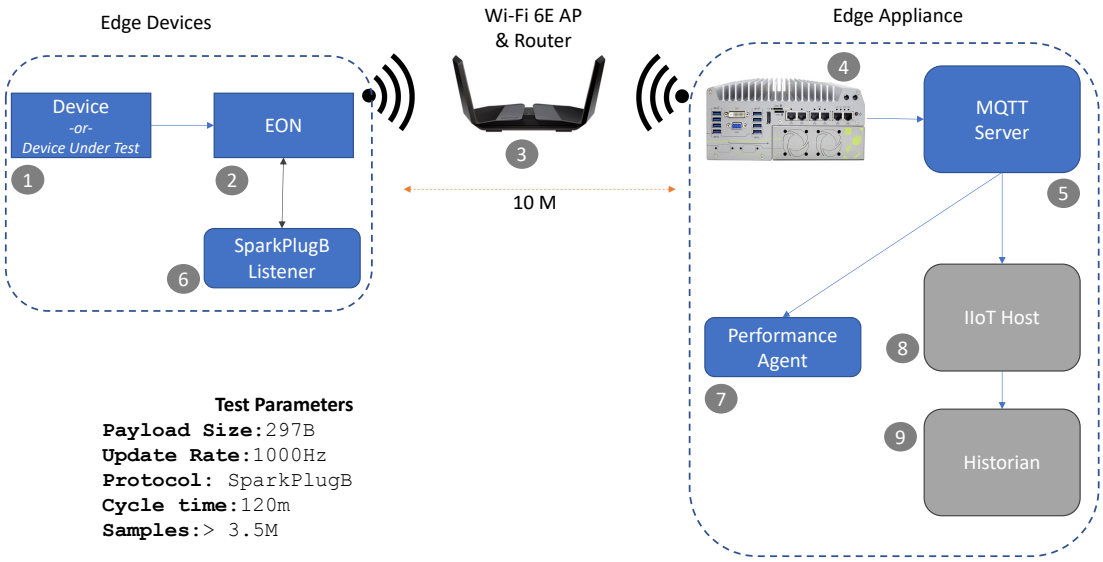


Figure **(6.24)** –Test configuration for Class 2 Applicatons

Testing Principal

1. Sensor telemetry send from Edge Device to EoN device.
2. EoN device transmits data wirelessly to Edge Appliance.
3. Signal is up-converted for processing.
4. CMW500 acts as Wireless Access Point.
5. AP sends data over a wired connection to SparkPlug-compliant MQTT Server.
6. MQTT Server sends data via RPC to IIoT Host.
7. IIoT Host sends a command signal as a response.
8. MQTT Server sends command signal back to AP.
9. AP sends response wirelessly to EoN Node.
10. Performance Monitor captures application performance metrics.
11. System telemetry data captured from Edge Appliance.

```
# Example parameters for resin-based 3D printing
parameters = {
        "process": "resin-based 3D printing",
        "temperature": 30.5,
        "humidity": 55.2,
        "printStatus": "inProgress",
        "layerNumber": 12,
        "buildPlateHeight": 15.3,
        "estimatedCompletionTime": "2023-06-15T12:00:00Z",
        "resinType": "Photopolymer",
        "resinColor": "Clear",
        "resinViscosity": 150,
        "exposureTime": 10.5,
        "printResolution": "50 microns",
        "supportStructure": "Enabled",
        "printingSpeed": "Medium",
        "powerConsumption": 120.5
}
```

Figure **(6.25)** –Class 2 example machine data

	RTT *(ms)*	**Throughput** *(bps)*	**Jitter** *(ms)*	**Reliability** *(mls)*
count	3 685 910	351 240.52	3 685 910	3 685 910
mean	9.41	228 119.50	2.73	$9.999\,258 \times 10^{1}$
std	45.73	718.91	2.99	$1.571\,153 \times 10^{-2}$
min	1	10 995.07	0.00	$9.986\,174 \times 10^{1}$
25%	6.00	236 800.00	2.00	$9.999\,485 \times 10^{1}$
50%	6.00	297 000.00	2.00	$9.999\,511 \times 10^{1}$
75%	10.00	397 333.33	2.00	$9.999\,544 \times 10^{1}$
max	3308.00	2 408 000.00	3259	$9.999\,606 \times 10^{1}$

Table **(6.11)** –Class 2 6GHz Industrial System Test Data

6.5.2 Results

Table 6.11 contains the results of Class 2 application testing.

6.5.2.1 Reliability Analysis

Reliability is a critical metric for continuous industrial processes as it consistently measures the network's ability to deliver data without errors or disruptions. The mean reliability value of 99.99258% indicates a high level of reliability. The standard deviation of 0.01571% suggests minor network reliability variations. The minimum reliability value is 99.86174%, and the maximum is 99.99606%. The median and *25th* and *75th* percentiles are above 99.995%, demonstrating the network's consistent performance. The high reliability is encouraging, indicating that the network can maintain its operational integrity during continuous industrial processes. However, even minor variations in reliability can have significant consequences in critical applications. Monitoring and optimising network parameters is essential to ensure continuous and reliable performance.

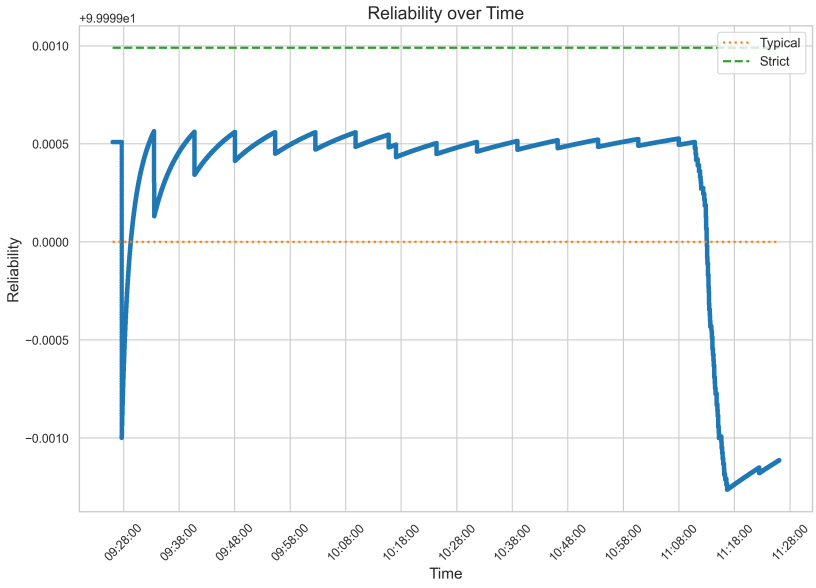


Figure **(6.26)** –Class 2 Reliability time series

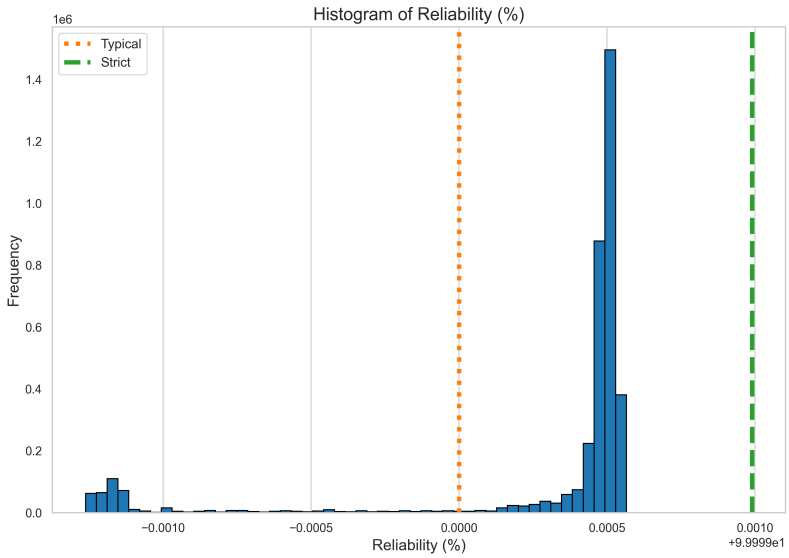


Figure **(6.27)** –Class 2 Reliability Histogram

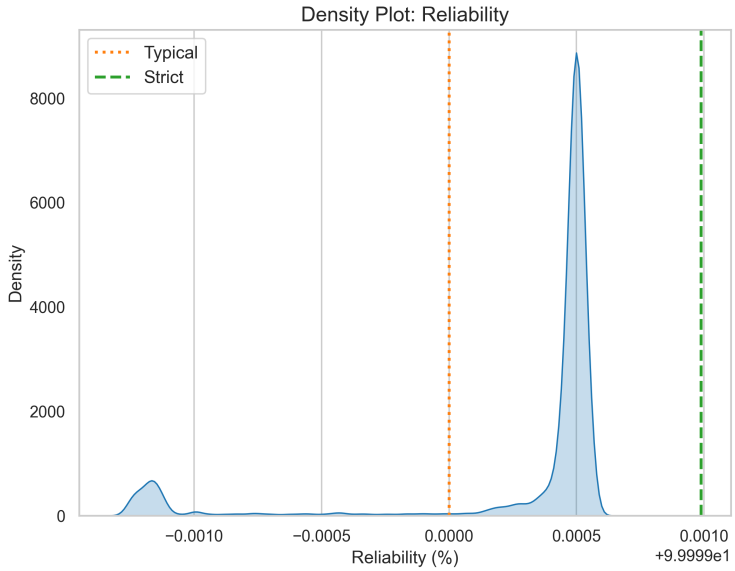


Figure **(6.28)** –Class 2 Reliability density diagram

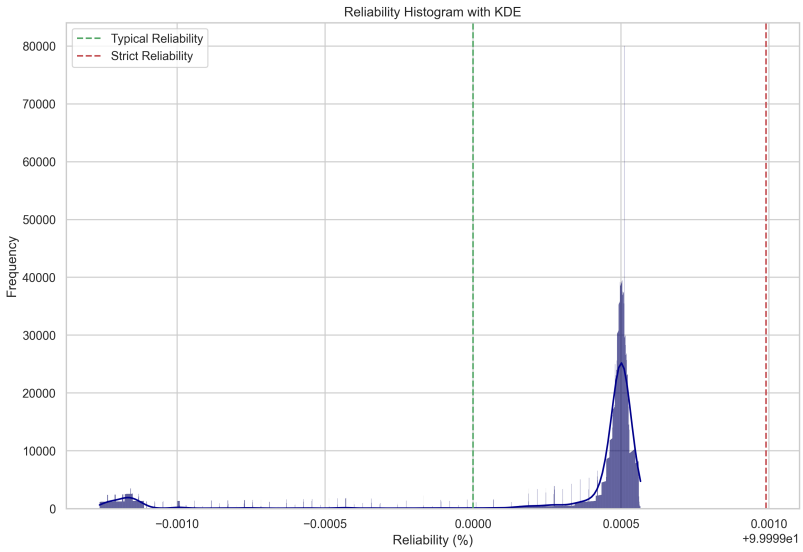


Figure **(6.29)** –Class 2 Reliability histogram with KDE

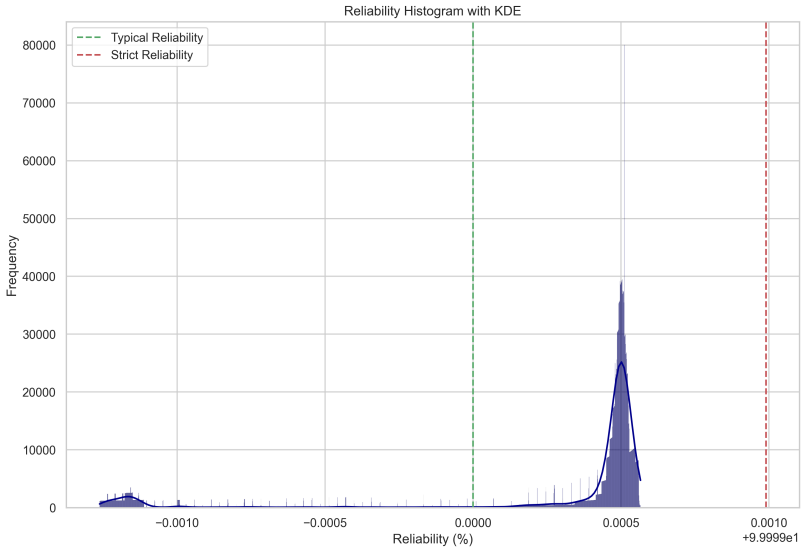


Figure **(6.30)** –Class 2 Violin plot

6.5.2.2 Round-Trip Time (RTT)

In class 1 or class 2 continuous process applications, where real-time data is paramount, Round-Trip Time (RTT) assumes significant importance. Our results exhibit a mean RTT of 8.90ms, a standard deviation of 3.76ms, and a noticeable disparity between the 75th percentile (10.89ms) and the maximum RTT (119.50ms) as seen in Fig. 6.31. These findings indicate potential latency spikes that could disrupt real-time data acquisition and control.

The causes of these spikes were initially attributed to Wi-Fi 6E signal interference from physical obstacles. Despite Wi-Fi 6E's significant latency advancements over its predecessors, it remains susceptible to these factors. However, upon deeper analysis, it was determined that the spikes were not a result of network congestion but possibly attributable to the inherent constraints of using general-purpose computing infrastructure and operating systems. Although versatile, these systems occasionally struggle with deterministic behaviour and real-time requirements due to non-deterministic scheduling, interrupt latency, shared resources, and cache effects, causing minor data processing delays. Nevertheless, our observations demonstrated an exact message reception with a timestamp resolution in the ns range, underscoring the system's overall efficacy.

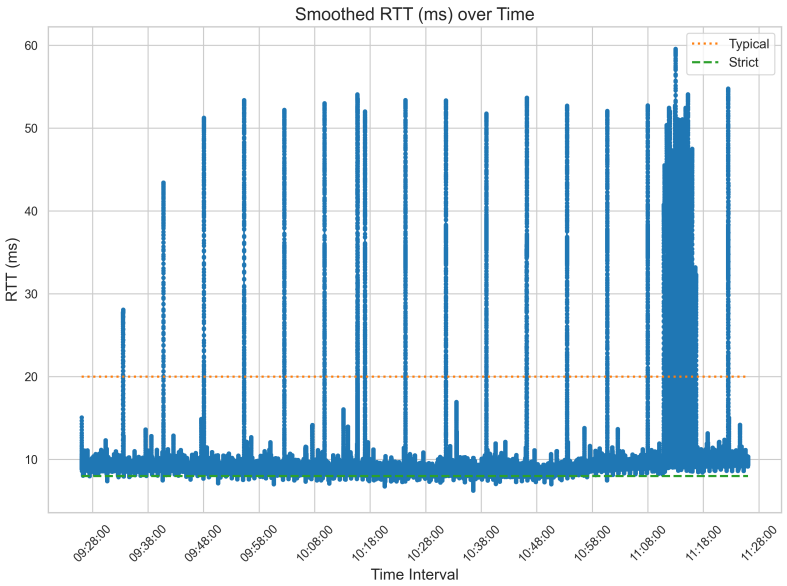


Figure **(6.31)** –Class 2 Round Trip Time smoothed over samples collected

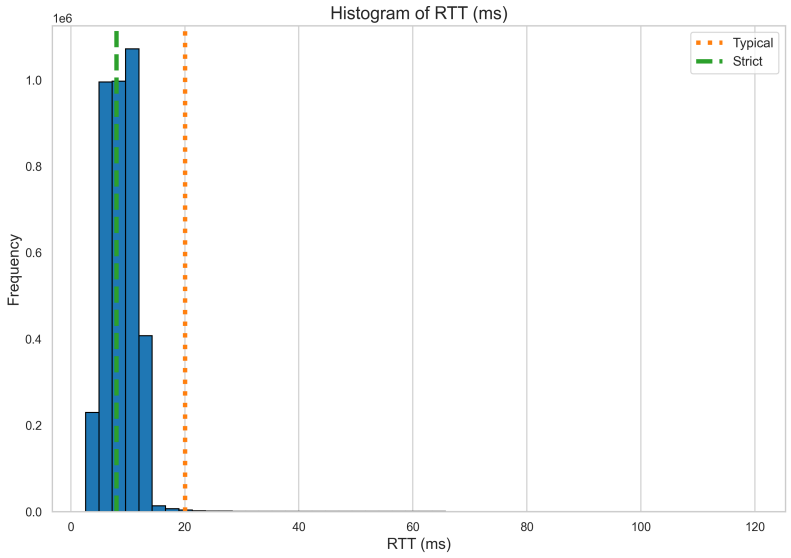


Figure **(6.32)** –Class 2 round trip time histogram

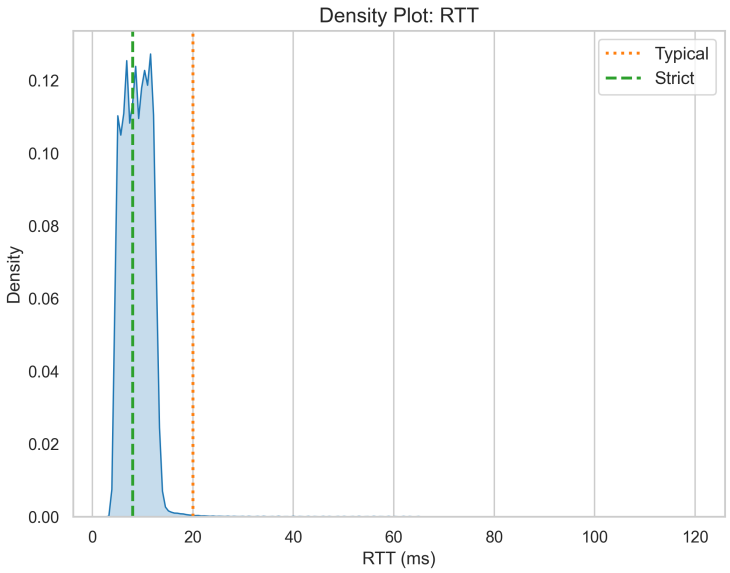


Figure **(6.33)** –Class 2 round trip time density

6.5.2.3 Throughput Analysis

Throughput, measured here in Mbps, indicates the capacity of the network, i.e., how much data it can handle within a given time frame. The system transmission data at 1000hertz

The mean throughput in our network is approximately 298474.46 Mbps, illustrating its capacity to manage high-capacity network payload. The minimum value (675.74 Mbps) and the 25th percentile (218989.13 Mbps) indicate that the network rarely, if ever, falls below a high level of throughput. This robustness is primarily due to Wi-Fi 6E's utilisation of the underutilised 6GHz band, providing improved spectral efficiency and capacity. Nevertheless, the broad standard deviation (99436.55 Mbps) indicates variance in throughput, which could affect the consistent

delivery of high-volume data essential for SCADA applications or other industrial automation-type applications.

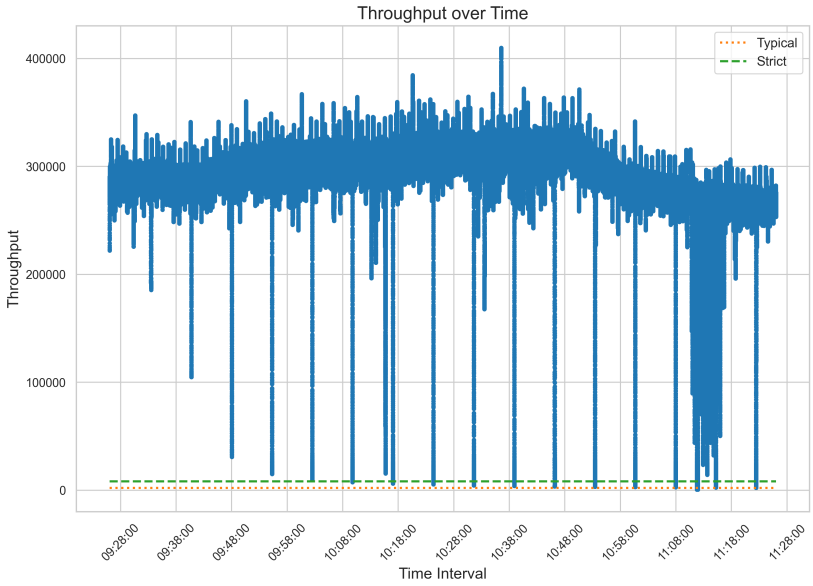


Figure **(6.34)** –Class 2 Throughput

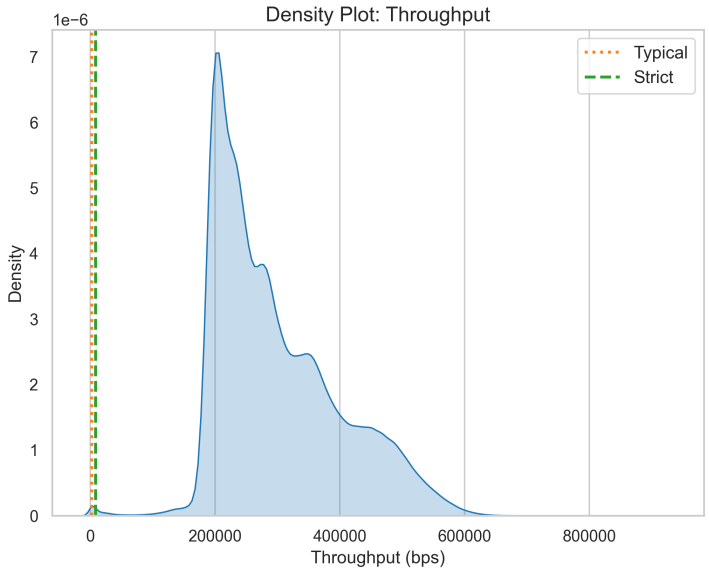


Figure **(6.35)** –Class 2 Throughput density plot

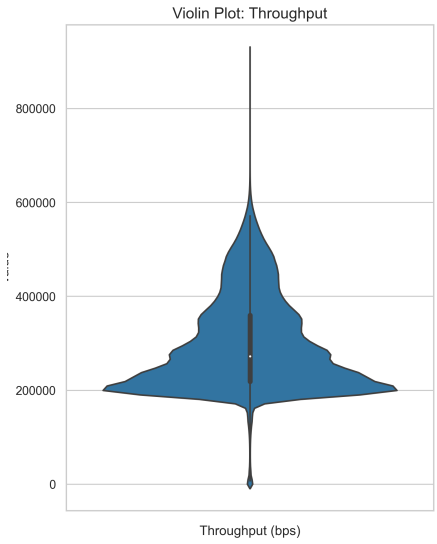


Figure **(6.36)** –Class 2 Throughput Violin plot

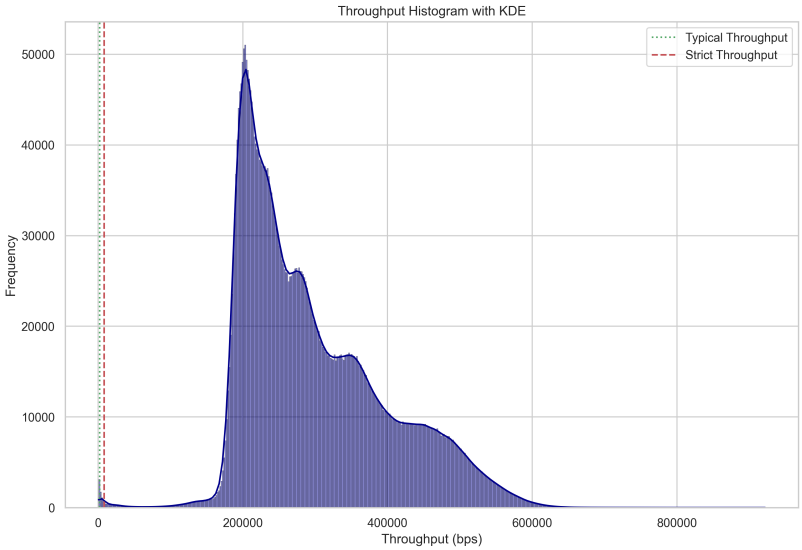


Figure **(6.37)** –Class 2 Throughput Historgram with KDE

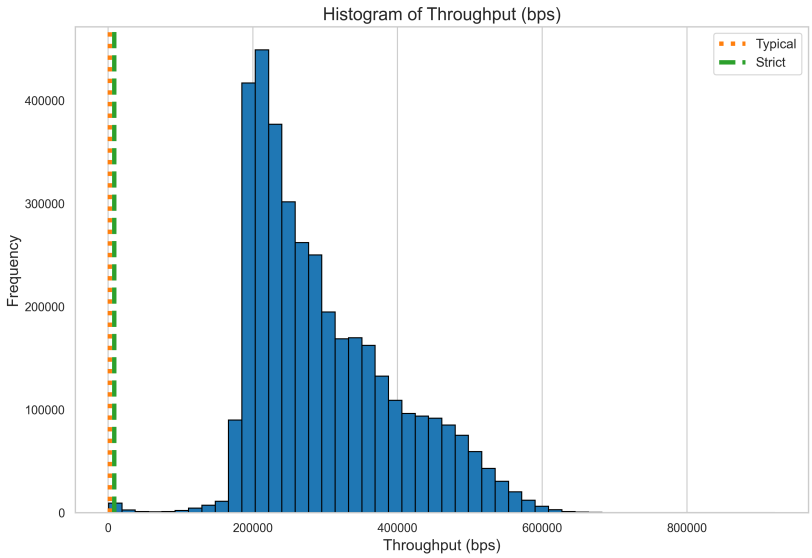


Figure **(6.38)** –Class 2 Histogram Histogram

6.5.2.4 Jitter Analysis

The dataset presents a mean jitter of 2.68ms, with a relatively low standard deviation (2.12ms), which signifies a generally consistent packet delivery time. Nonetheless, the maximum value (101.61ms) suggests occasional substantial jitter spikes. These jitter variations can impact the timeliness and order of packet delivery, possibly causing problems in SCADA systems where control signals are time-sensitive.

However, given that no significant optimisation or improvement techniques were adopted, there are opportunities to improve both the RTT and subsequent jitter within the network.

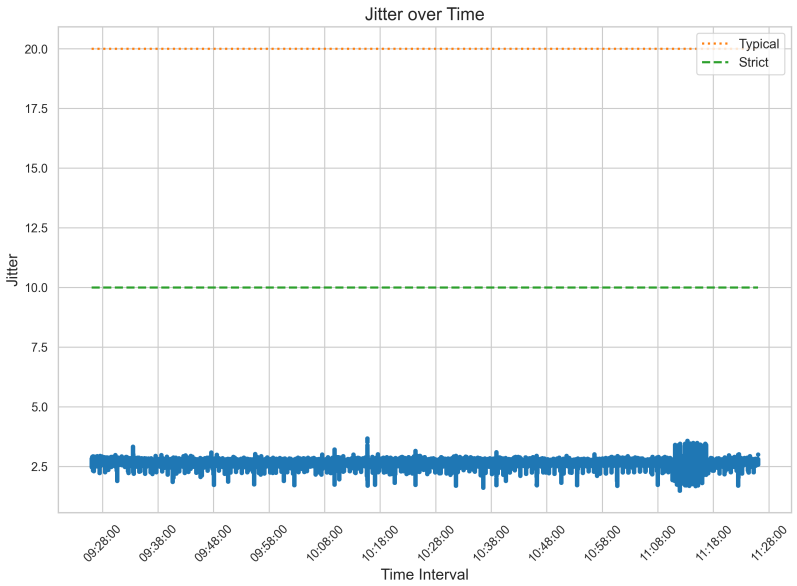


Figure **(6.39)** –Class 2 Jitter smoothed over samples collected

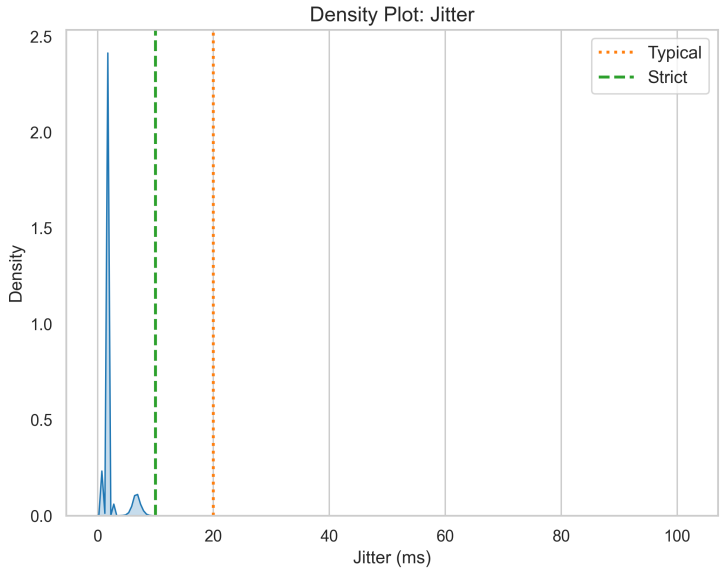


Figure **(6.40)** –Class 2 Jitter density

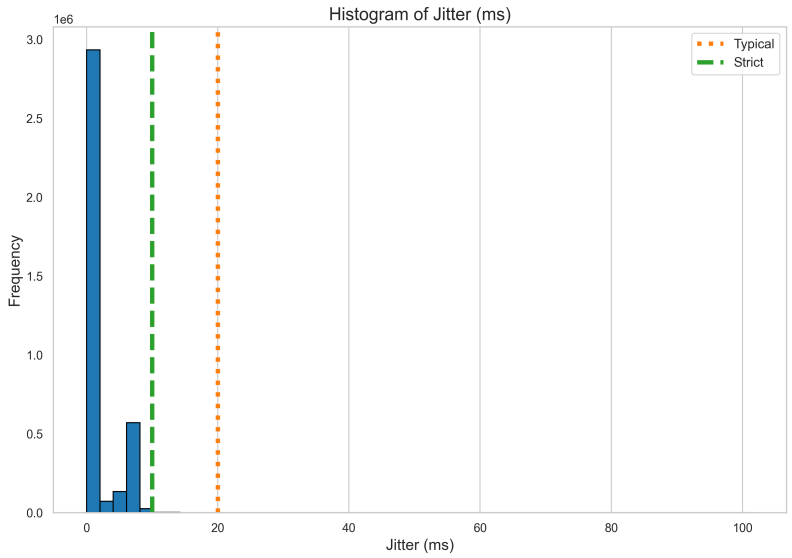


Figure **(6.41)** –Class 2 Jitter Histogram

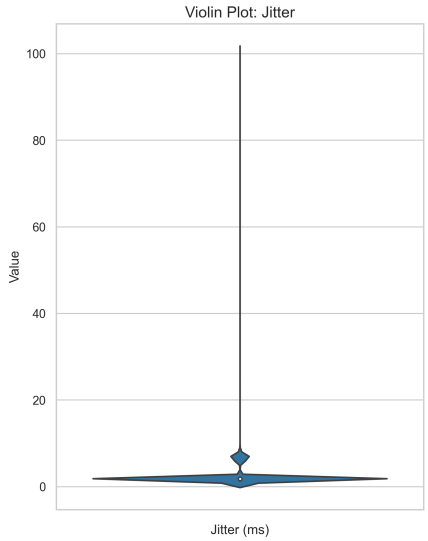


Figure **(6.42)** –Class 2 Jitter Violin plot

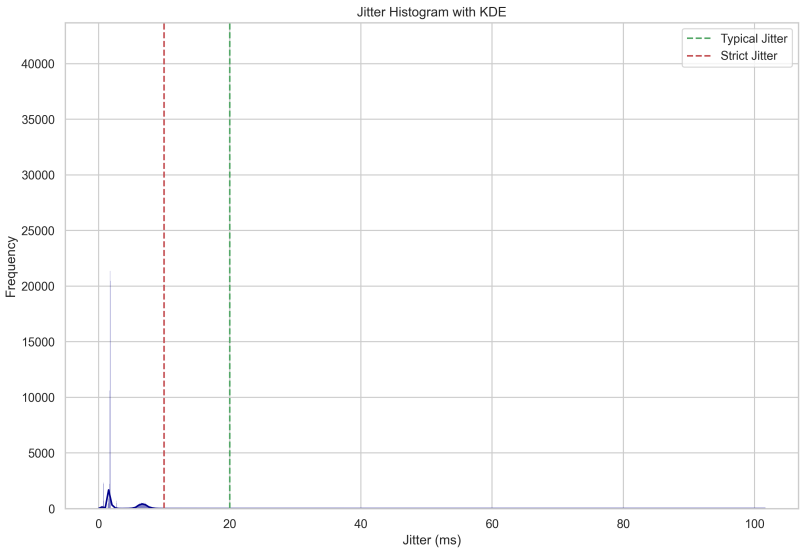


Figure **(6.43)** –Class 2 Histogram with KDE

- Class 0: We select a testing duration of $60s$. In an emergency such as an e-stop trigger, it is doubtful that an e-stop event would take that long. While the number is somewhat arbitrary, it provides ample coverage for such an event
- Class 1: For class 1 closed-loop control system elected to set the time at $30m$
- Class 3: We used a time of 180 seconds for class 3 applications. The basis of this selection was observing user interactions with the HMI interface for manual controls of some of the toolsets. We observed the use of the operator, which typically took 120 seconds. We added 60 as an upper limit of performance.

6.6 Class 4 system testing

The ISA defines Class 4 as suitable for condition monitoring and preventative maintenance applications. In these applications, devices send readings to a central system for offline analysis. Such applications have different latency and reliability requirements than the previous classes of industrial applications. For example, monitoring and diagnostics applications can have latencies between 20ms and 100ms and reliability between 10^{-4} and 10^{-5}. Class 4 applications can support latencies of $100ms$, similar to ETSI's recommendations. NIST recommends RTTs of $8 - 100ms$ and reliability of 10^{-6} and 10^{-7}. These numbers are not as strictly time-dependent as the other application classes, and reliability techniques can be adopted to achieve these numbers. Raptis et al. provide a comprehensive survey outlining the breadth of volume and variety of traffic in this space [393]. The authors broadly categorise three classes of data volume, from small to large inclusive. We have elected to base our testing on a medium size payload of *280B*, representing large payload sizes more likely encountered with data-rich sensor-based systems, which would be higher resolution and comprehensive.

We assume high sensor update rates and continuous sampling at a high frequency. While these applications do not provide regulatory control, stricter requirements can bridge the gaps between functionality and capabilities of different application classes, given the growing popularity of digital twin and advanced maintenance technologies [394]. We set the update rate at $125Hz$

Our testing focuses on wireless networks supporting complex data types and modalities, extending NIST's recommendations. This considers the evolution

of traditional monitoring apps towards emerging trends such as Digital Twin tech and condition-based monitoring systems, which are more time-sensitive and bandwidth-intensive [395].

6.6.1 Expermental setup and Configuration

Th experimental setup follows the same appoach as the previous experimentation with changes to the values in-line with the application class, although we do use numbers on the high performance range of expected value, which are included in 6.44

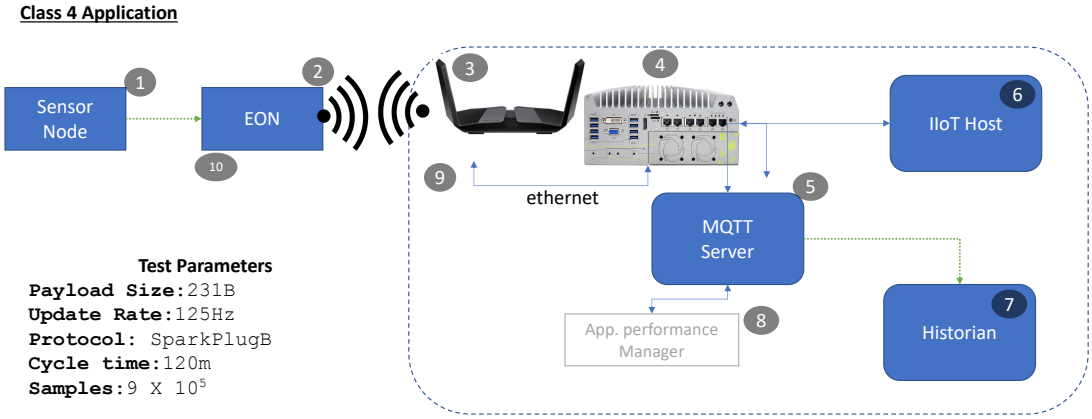


Figure **(6.44)** –System Test Configuration for class 4 and 5 applications

Figure 6.44 details the test architecture and design used for testing. In this configuration, we assume that sensor data collected from edge devices are being collected and stored in a time series database. The critical data path is unidirectional, from the edge device to the historian. Dietrich et al. outline performance criteria for condition-based monitoring applications with data sizes ranging from 30-1500 Bytes [396]. NIST's recommendations range from $12B$ and $33kB$.

Given the popularity and interest in emerging monitoring and diagnostics trends such as those discussed in Chapter 2 Digital Twin technologies and Augmented Reality systems and their high requirement for larger data sizes, we run our test across three ranges. They are 2^5, 2^7 and 2^{13} Bytes.

Testing Principal

1. Sensor telemetry send from Edge Device to EoN device.
2. EoN device transmits data wirelessly to Edge Appliance.
3. Signal is up-converted for processing.
4. CMW500 acts as Wireless Access Point.
5. AP sends data over a wired connection to SparkPlug-compliant MQTT Server.
6. MQTT Server sends data via RPC to IIoT Host.
7. IIoT Host sends a command signal as a response.
8. MQTT Server sends command signal back to AP.
9. AP sends response wirelessly to EoN Node.
10. Performance Monitor captures application performance metrics.
11. System telemetry data captured from Edge Appliance.

6.6.2 Results

The Test results are tabulated in Table 6.12. We compare the typical and strict values against the minimum, max and median values. As you can see from the

```
{
        "metrics": [
        // ... previous metrics omitted for brevity
        {
                "name": "PrintingSpeed",
                "datatype": "FLOAT",
                "floatValue": 75.0
        },
        {
                "name": "PowerConsumption",
                "datatype": "FLOAT",
                "floatValue": 120.5
        },
        {
                "name": "VibrationAcceleration",
                "datatype": "FLOAT",
                "floatValue": 0.05
        },
        {
                "name": "VibrationDisplacement",
                "datatype": "FLOAT",
                "floatValue": 0.02
        },
        // More metrics continue here...
        ]
}
```

Figure **(6.45)** –Class 4 sample machine data (excerpt)

6.6.2.1 Reliability Analysis

With a mean close to 100% (99.999345%), the network demonstrates excellent reliability, integral for continuous, uninterrupted monitoring and control operations in industrial settings. The minuscule standard deviation (0.000230) reinforces the network's consistent reliability. The performance numbers illustrate reliability performance well within the application and application classes' requirements.

	RTT (ms)	Throughput (bps)	Jitter (ms)	Reliability (%)
count	3 685 910.00	3 685 910.00	3 685 910.00	$3.685\,910 \times 10^{6}$
mean	8.18	351 240.52	2.73	$9.999\,234 \times 10^{1}$
std	3.16	228 119.50	2.99	$1.570\,861 \times 10^{-2}$
min	1.00	718.91	0.00	$9.986\,159 \times 10^{1}$
25%	6.00	236 800.00	2.00	$9.999\,467 \times 10^{1}$
50%	8.00	297 000.00	2.00	$9.999\,490 \times 10^{1}$
75%	10.00	397 333.33	2.00	$9.999\,519 \times 10^{1}$
max	122.00	2 408 000.00	3259.00	$9.999\,567 \times 10^{1}$

Table **(6.12)** –Class 4 6GHz Industrial System Test Data

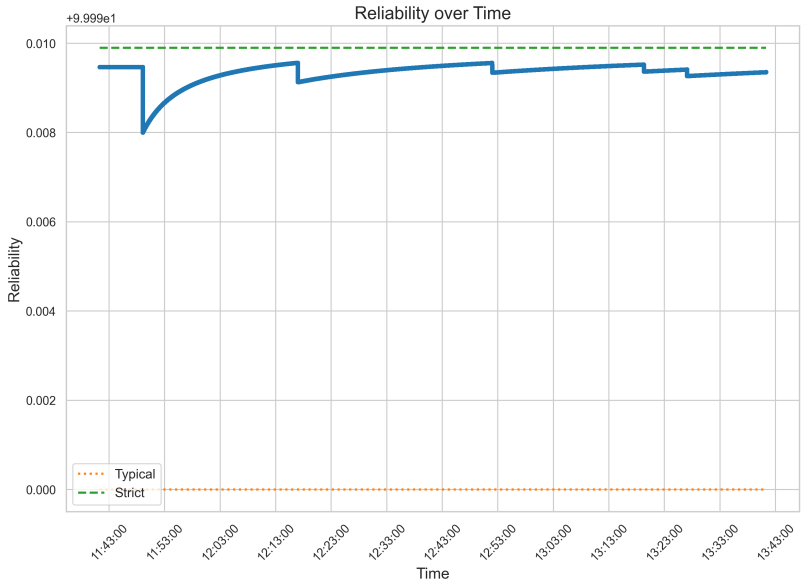


Figure **(6.46)** –Class 4 Reliability time series

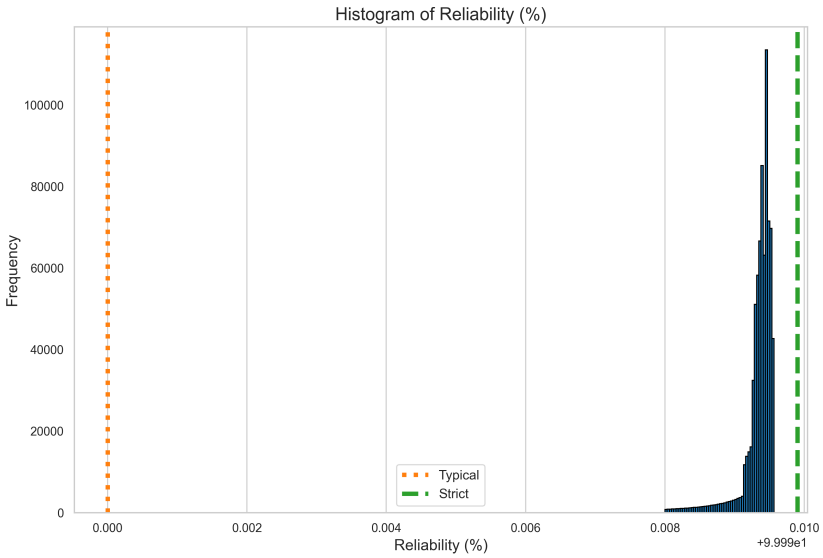


Figure **(6.47)** –Class 4 Reliability Histogram

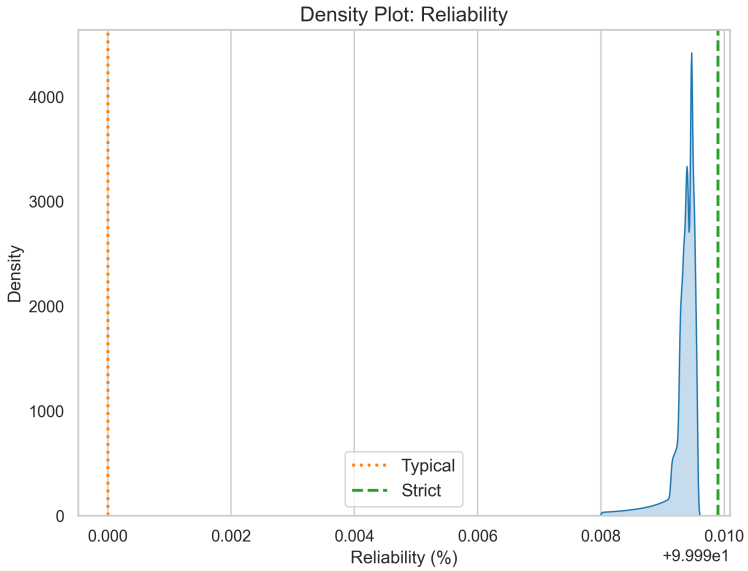


Figure **(6.48)** –Class 4 Reliability density diagram

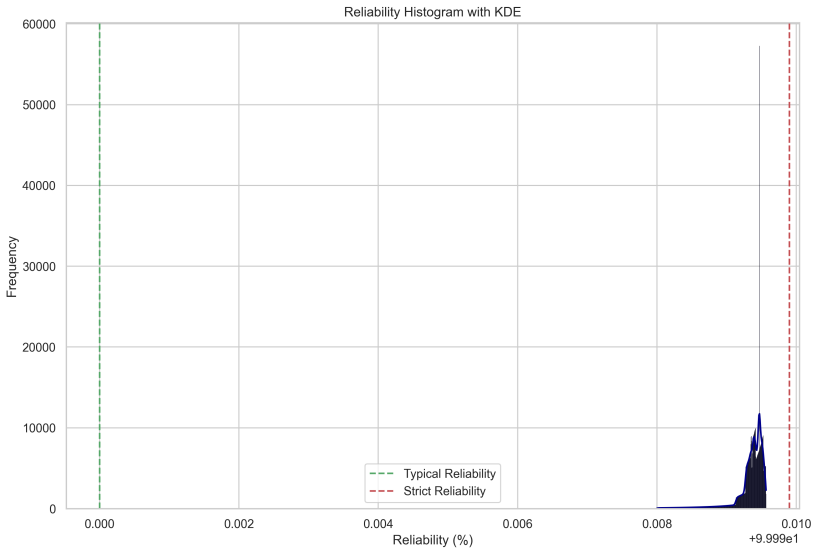


Figure **(6.49)** –Class 4 Reliability histogram with KDE

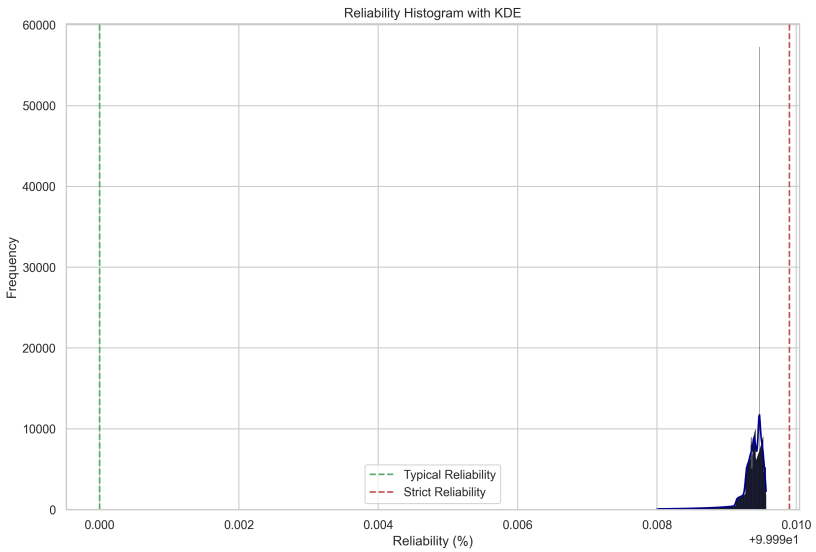


Figure **(6.50)** –Class 4 Violin plot

6.6.2.2 RTT Analysis

The network's RTT statistics illustrate a mean value of $4.14ms$ with a standard deviation of $1.54ms$. Despite this low average latency, which is beneficial for real-time PHM and digital twin updates, the maximum value reaches 114.17ms, suggesting occasional latency spikes, which we have observed in class 0 and class 2 applications. These latencies could delay processing vital predictive maintenance and condition monitoring information, potentially leading to slower response times in critical situations. However, the criticality in these instances is most likely less severe.

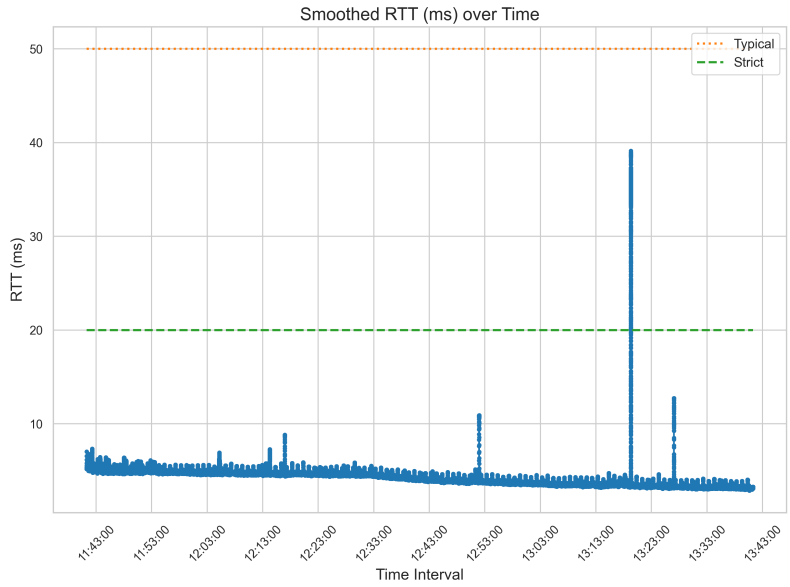


Figure **(6.51)** –Class 4 Round Trip Time smoothed over samples collected

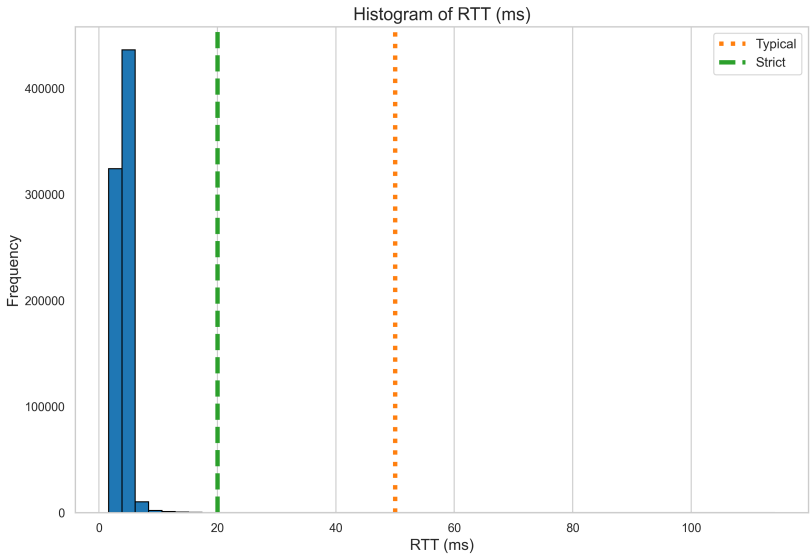


Figure **(6.52)** –Class 4 round trip time histogram

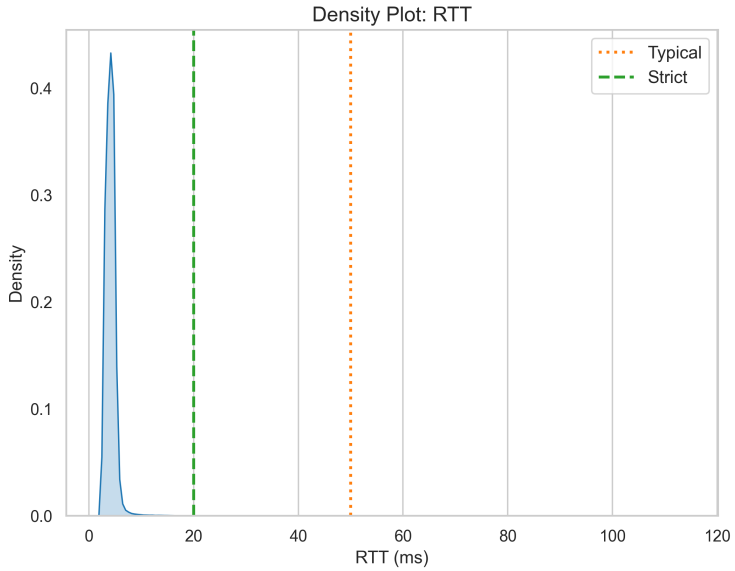


Figure **(6.53)** –Class 4 round trip time density

6.6.2.3 Throughput Analysis

Again, we can observe high average throughput (570327.78 Mbps), which further signifies the network's capability to handle substantial data volumes, an essential aspect for digital twin applications that require real-time data synchronisation and efficient condition monitoring. However, the relatively high standard deviation (122828.15 Mbps) may imply occasional variations in data rate, which influence real-time performance. Consistent with the other applications, the likelihood of this issue being related to Wi-Fi-specific limitations is low, given the accuracy and consistency of the inbound payload timestamp and sequence numbers being in the expected order.

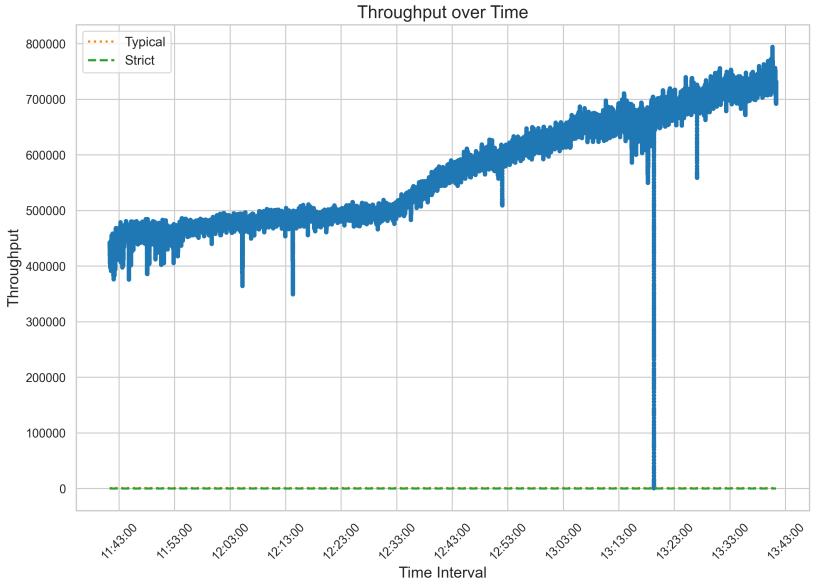


Figure **(6.54)** –Class 4 Throughput

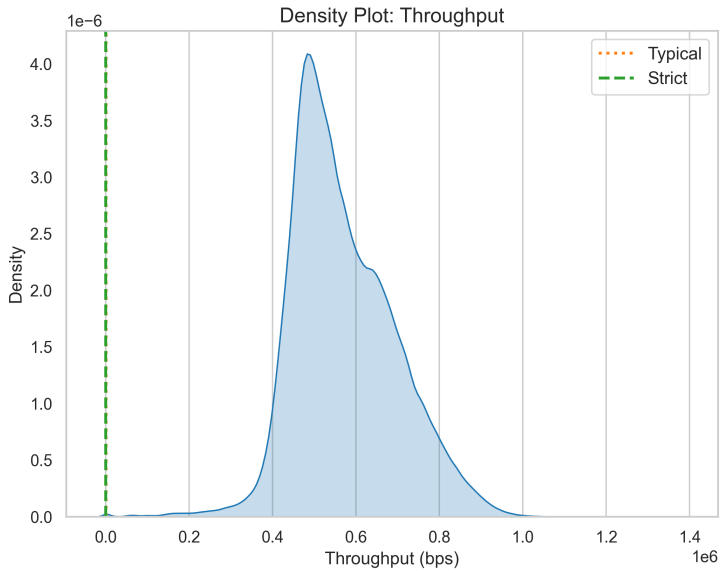


Figure **(6.55)** –Class 4 Throughput density plot

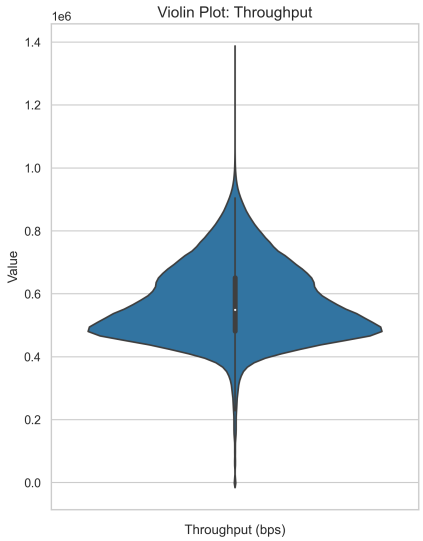


Figure **(6.56)** –Class 4 Throughput Violin plot

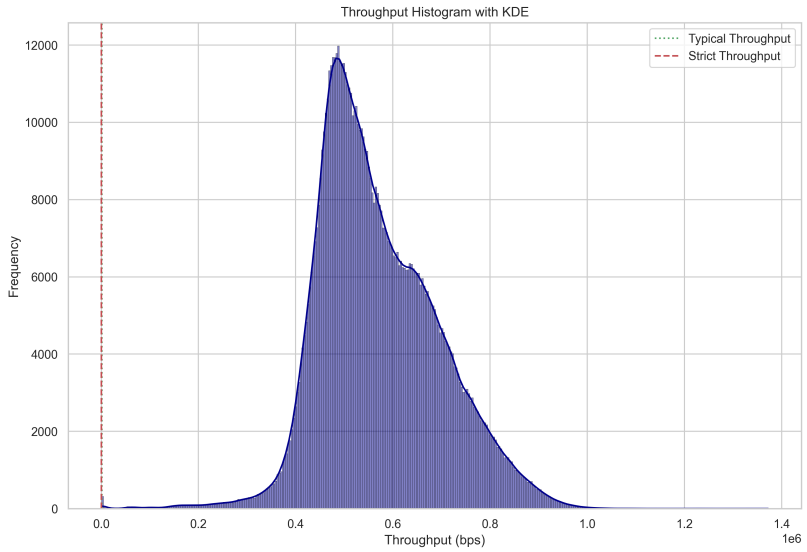


Figure **(6.57)** –Class 4 Throughput Historgram with KDE

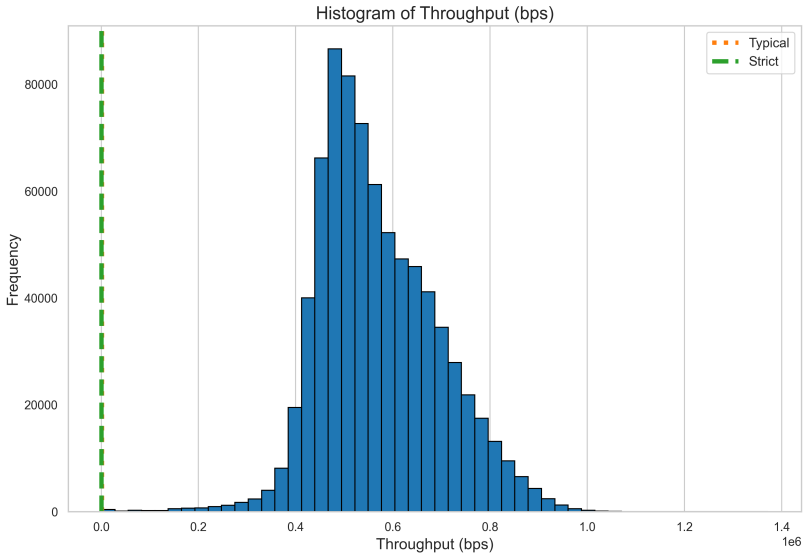


Figure **(6.58)** –Class 4 Histogram Histogram

6.6.2.4 Jitter Analysis

Jitter refers to the variation in packet arrival times at the destination. A low jitter value indicates consistent packet arrival times, while a high one suggests inconsistent or irregular packet delivery. In our analysis, the mean jitter is 2.73 ms, with a standard deviation of 2.99 ms. The minimum jitter observed is 0.00 ms, while the maximum is 3259.00 ms. The low mean and standard deviation indicate stable packet delivery with minimal variations in arrival times. However, some high jitter values indicate occasional packet delivery delays or disruptions.

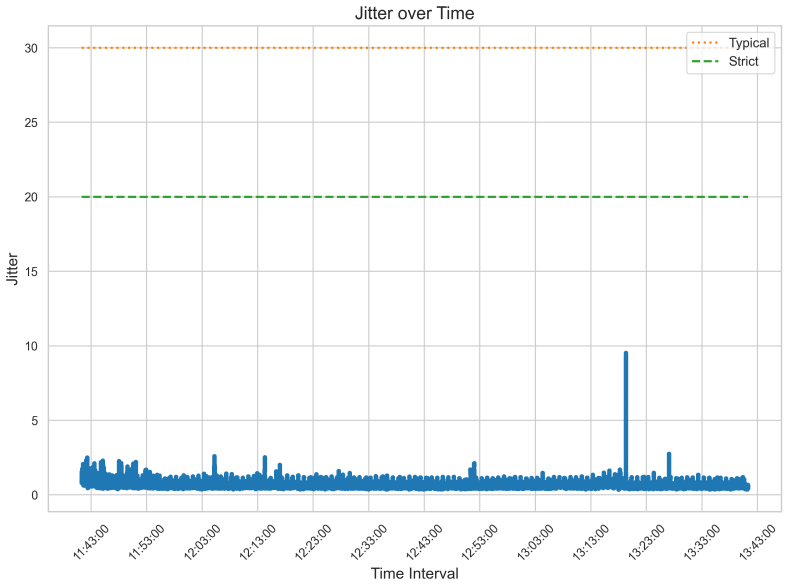


Figure **(6.59)** –Class 4 Jitter smoothed over samples collected

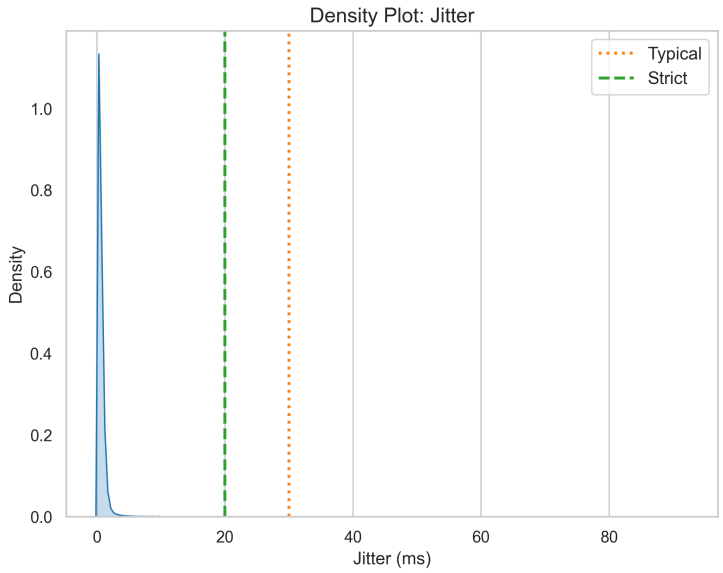


Figure **(6.60)** –Class 4 Jitter density

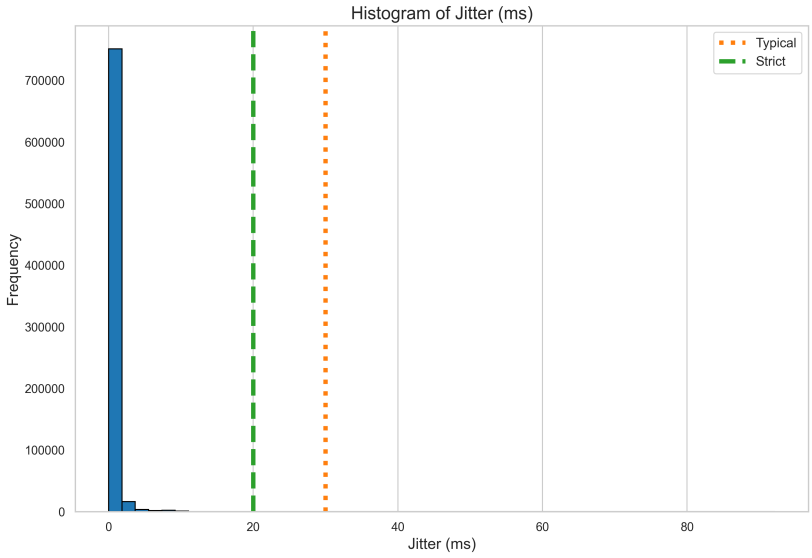


Figure **(6.61)** –Class 4 Jitter Histogram

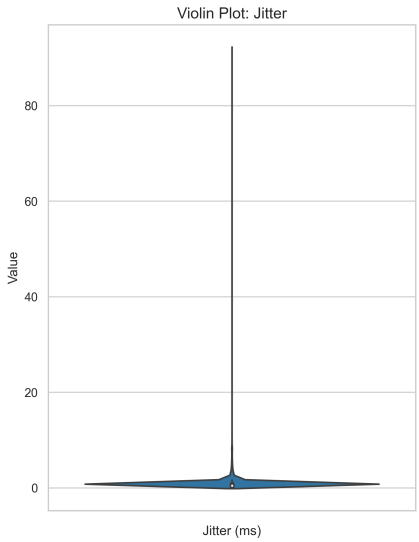


Figure **(6.62)** –Class 4 Jitter Violin plot

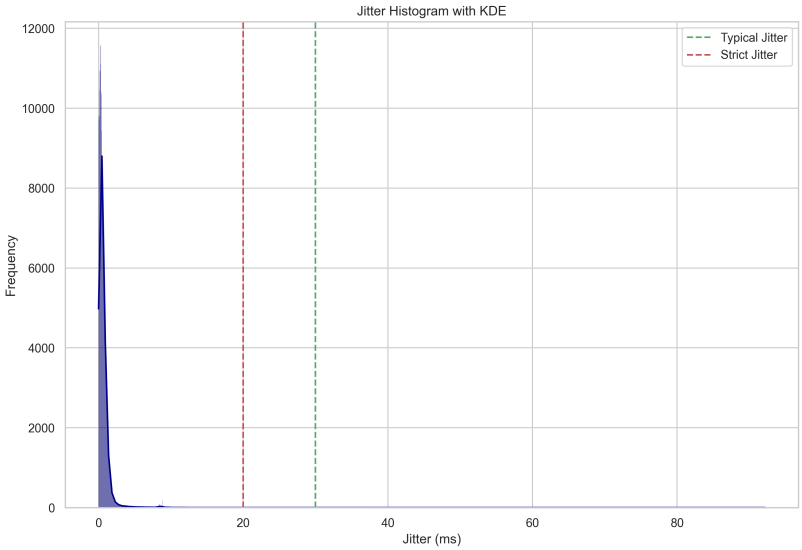


Figure **(6.63)** –Class 4 Hist-KDE

6.7 Conclusion

The Industrial Internet of Things (IIoT) is constantly changing, and Wi-Fi 6E-enabled industrial networks supported by SparkplugBv1 protocol offer a robust wireless solution for industrial networks. The evaluation of this technology across various industrial application categories confirms its versatility, making it a potential universal networking technology that can serve a wide range of industrial applications.

6.7.1 Performance Assessment and Network Dynamics

We focused on essential systems performance metrics like round trip time (RTT), throughput, jitter, and reliability. Our findings revealed that even with the update rate increased from 125Hz to 1000Hz, there was not a significant decline in the network's performance. This emphasises the robustness and resilience of the Wi-Fi 6E-based network, allowing it to handle heavy data traffic.

We also analysed the performance of the application layer, which provides a more comprehensive view of the system's overall performance. This multi-layer approach gives us a more detailed and realistic understanding of how the network behaves, which is often overlooked in other studies.

We did observe occasional latency spikes during our testing, which could impact the responsiveness of applications. While these were inconsistent and intermittent, they must be taken into account. Additionally, we noticed that the system behaved differently during its initial "warm-up" phase, generating data that may not accurately represent the system's steady-state behaviour. Although it is

typical to exclude this transient data, we included it for completeness and further exploration of these specific dynamics.

6.7.2 Key Observations and Optimisation Strategies

During our testing, we observed a significant drift in time synchronisation across network devices, known as clock drift. This deviation can impact latency and data consistency, affecting real-time responsiveness and overall network performance. Therefore, it is necessary to perform frequent synchronisation checks and adjustments to maintain temporal coherence across the network and optimise performance.

Our wideband sweep of the wireless channel, known as spectral scanning, revealed no interfering signals in the 6GHz frequency band. This supports our supposition that the observed performance spikes were due to computational limitations, not network interference.

The strategic placement of Wi-Fi access points, antennas, and industrial devices is crucial in optimising network performance. Our experiment highlighted the apparent influence of equipment placement on performance. Therefore, conducting a comprehensive wireless site survey is essential to ensure optimal device placement and signal coverage.

6.7.3 Future Optimisation Strategies

- **Firmware and Software Updates:** Regularly updating firmware and software can substantially improve network reliability and efficiency. This

process often includes essential bug fixes, performance enhancements, and protocol optimisations.

- **Performance Monitoring and Analysis:** A proactive approach to network health, involving real-time monitoring and analysis, allows for the early detection and resolution of performance degradation, ensuring optimal network operation. Future exploration into more dynamic management of Wi-Fi networks can pave the way for increased autonomous control of network infrastructure.
- **Synchronisation in Industrial Networks:** Incorporating Precision Time Protocol (PTP) or Network Time Protocol (NTP) is essential for maintaining synchronisation within an industrial network. Regular synchronisation checks are pivotal, particularly for the SparkplugBv1 protocol, which relies on precise time-stamping for efficient real-time data distribution.

Our study indicates that utilising the SparkplugBv1 protocol on Wi-Fi 6E-based industrial networks shows promising performance for various industrial applications. However, it is crucial to continuously monitor and optimise the network infrastructure to maintain a reliable and efficient wireless network ecosystem.

We can enhance the system's performance, scalability, and interoperability by utilising Wi-Fi 6E technology, precise time synchronisation, and meticulous network configuration. This creates a strong foundation for the future of IIoT.

Chapter 7

Conclusion

7.1 Concluding thoughts

This work introduces a new wireless solution for industrial settings utilising IEEE 802.11ax Wi-Fi 6E-based technologies. Wi-Fi is chosen for its availability, affordability, and easy integration. Wi-Fi has evolved to meet changing user needs and is the most widely used wireless technology. The digital transformation of the industry has made technology more open and interoperable. The IoT has matured into a connectivity fabric for devices and assets. Second-generation applications focus on making data actionable. The Industrial IoT is entering a second wave as physical processes transform into fully digital operations through technologies like digital twins.

The solution presented here combines various technologies to address the challenges of diverse industrial applications. It synthesises a range of technologies to cater to different industrial applications classes and answer the question.

Can Wi-Fi 6 based support high reliability wireless industrial networks

From the research conducted, the answer is yes. We also addressed many research questions, which informed the design of the system and its experimental evaluation. We will briefly reflect on those questions.

- **[R1] What is the current state of emerging applications in the industry?** Trends like Industry 4.0 and its associated technologies are starting to impact manufacturing and industrial environments. However, the rate at which these technologies will replace legacy systems will not be in the same vein of technology upgrades typically seen in enterprise IT-type applications. The cost, complexity, and effort required will likely mean a longer tail of adoption.

  The system's design was affected by the reality of the long tail of adoption time, which prompted the need for technology solutions that were backward and forward-compatible, allowing for operation in various environments. Another design consideration was the multivariate and evolving nature of M2M data, which required a communications protocol capable of supporting different bandwidths and update frequencies.

- **[R2] What is the current state of industrial wireless networks?** It is noticeable that wired technologies are still widely utilised in the industry and will continue to be a part of the communication system in industrial applications. Nevertheless, wireless communication has shown significant performance improvements, making it a practical choice and likely to increase in installations in the future. The question of what wireless technology will

win out needs to be clarified. 3GPP technologies and their advancement are gaining traction but remain costly to install and operate.

Wi-Fi continues its advance in both technological and scale trajectories. It is already the wireless communication choice of most enterprises, and it seems reasonable that the IT/OT convergence will propel Wi-Fi forward. Wireless time-sensitive networking also looks promising as having the potential to provide performance and reliability requirements to match wired-based systems. The motivation for selecting Wi-Fi was to advance our understanding of the potential of IEEE 802.11ax to address the most demanding communication challenges. In that regard, it is clear that the direction of travel of the standard holds significant promise. The following standard release based on IEEE802.11be will further move the Wi-Fi capability.

- **[R3] What are the radio propagation phenomena in modern industrial facilities?** As NIST correctly calls out, understanding the radio propagation environment is critical to ensuring successful communication systems deployments. Given the heterogeneity of different backgrounds, the radio propagation test plays a vital role in specific deployment success and broadens our understanding of different scenarios. Limited information about 802.11ax-based systems, specifically in industrial environments, was another critical factor in the work presented, and research on Wi-Fi in the 6GHz band, especially in industrial settings, was limited.
- **[R4] Can we design an IEE802.11ax Wi-Fi 6 industrial wireless system for modern industrial applications?** Industry standards and current trends in wireless industrial networks influenced the system's design.

Open-source technologies, including containers, provided flexibility for updates to different subsystems, ensuring the system's modularity. Containers also allow for interoperability and sharing physical hardware with other service providers, allowing operators to replace subsystems as needed. For instance, the historian container allows for the use of different databases or upgrades to the historian when required. Another crucial design choice was to leverage the publishsubscribe pattern for data sharing. This messaging pattern enables modularity and supports different subsystems to share data of different types and frequencies. Migrating from the pollresponse model appears to be a broader industry trend, with OPC-UA now supporting publishsubscribe.

The trade-off between OPC-UA and MQTT was another critical consideration. Our initial design incorporated OPC-UA, given its use in industry. The broad popularity of MQTT technology and enhancements such as the SparkPlug definition pushed the choice toward SparkPlug. SparkPlug is open-source and keeps up with the ethos of the design. Also, the ease of programming and development is more straightforward with MQTT, compared to OPC-UA, which lowers the barrier to adoption.

[R5]. Can we improve interoperability between legacy industrial standards and modern IoT protocols?. We demonstrated the ability of SparkPlug to map to the popular ISA95 framework, which enables mapping to other information models such as OPC-UA and IEC61850.

- **[R6]** Can our candidate design meet the communication requirements of wired counterparts? Chapter 6 illustrates the system's performance capa-

bilities. A Wi-Fi-based system can meet the needs of Class 3 and Class 4 applications, but meeting the requirements of Class 0 is problematic.

7.2 Contributions

- We present a comprehensive exploration and generalisation of emerging technologies in the context of Industry 4.0 and the broader industrial domain, contributing to understanding the current technological landscape.
- We delve into the current state of industrial wireless technologies, focusing on the latest advancements in the IEEE 802.11ax and Wi-Fi 6 standards. We provide a detailed overview of the contemporary wireless technologies pertinent to industrial applications.
- We propose a design for an edge-based system leveraging the IEEE 802.11ax (Wi-Fi 6) standard for deployment in industrial environments, offering a practical blueprint for developing future Wi-Fi 6-based industrial systems.
- We conduct extensive radio propagation testing within an industrial facility and generate an empirical model based on the results. This contribution enriches the existing knowledge on industrial wireless networks, specifically focusing on IEEE 802.11ax (Wi-Fi) based networks.
- We propose a messaging protocol utilising the SparkPlug framework to foster interoperability between legacy industrial systems, IoT applications, and our Wi-Fi 6-based candidate communication network for multimodal sensing in industrial or harsh environments.

- We evaluate the performance of our proposed approach against industry application class performance criteria and design and implement a Wi-Fi 6-based sensor node for multimodal sensing, thereby providing a practical demonstration of the system's capabilities.
- We provide a comprehensive analysis of the potential of Wi-Fi to meet the communication requirements of all industrial applications, offering valuable insights into the viability of Wi-Fi as a solution for industrial communication needs.

7.3 Implications

The work presented here has several implications for industrial wireless networks.

- It demonstrates the potential of Wi-Fi 6 as a viable wireless communication technology for industrial applications. The system's performance in meeting the communication requirements of different industrial applications suggests that Wi-Fi 6 can be a cost-effective and efficient alternative to wired networks and other wireless technologies in industrial settings.
- The use of open-source technologies and standards in the system design promotes flexibility and interoperability, which are crucial for integrating the system into existing industrial environments. The system's ability to interoperate with legacy industrial standards and modern IoT protocols can facilitate the transition of industrial systems towards more open and flexible architectures.

- The system's design and implementation provide a practical reference for designing and deploying Wi-Fi 6-based industrial wireless networks. The lessons learned from the system design and testing can inform future efforts in designing and implementing similar systems.
- The work contributes to knowledge in industrial wireless networks, particularly in Wi-Fi 6-based networks. The results from the radio propagation testing and system performance evaluation provide valuable insights into the behaviour and performance of Wi-Fi 6 in industrial settings.

7.4 Limitations

Although our work has made notable progress in exploring the potential of Wi-Fi 6 in industrial applications, we must acknowledge some limitations. Firstly, testing was conducted in a controlled environment, which may only partially reflect the complexities of a real-world industrial setting. Factors like interference from other wireless devices, physical obstacles, and variable environmental conditions can significantly affect the performance of wireless networks in industrial environments.

Secondly, the system was designed and tested with a specific set of industrial applications in mind. While the system showed promising results for these applications, its performance and suitability for other industrial applications remain to be tested.

Thirdly, the performance of the system was tested without adopting QoS features available, there would be a trade off between against latency performance. This is an area where we beleive would benefit from further investifation and analysis.

Finally, while the system leverages open-source technologies and standards, the integration and interoperability of the system with existing industrial systems and protocols may pose challenges. The system's ability to interoperate with other systems and protocols is crucial for its adoption in industrial settings, where legacy systems and protocols are prevalent.

7.5 Future Work

802.11ax (Wi-Fi 6E) has significantly improved performance, reliability, and security. However, with the growing demands of industrial applications, there is a need for new wireless standards that can support a higher density of devices, provide faster and more reliable communication, and ensure data security and privacy. The upcoming standards, 802.11be and Wi-Fi 7, will build on the progress of 802.11ax and significantly improve wireless communication.

The recent allocation of the 6GHz frequency band by regulatory bodies has opened up new opportunities for Wi-Fi networks. The wider bandwidths in this frequency range enable higher data rates and lower latency, making it ideal for applications requiring fast and reliable connectivity. Using 6 GHz frequencies in industrial settings would allow for more efficient use of the available spectrum, resulting in less interference and increased reliability [397].

Managed spectrum technology could significantly improve Wi-Fi reliability in industrial applications. Spectrum management techniques such as Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) can help minimise interference and improve network performance [398]. DFS allows Wi-Fi networks

to dynamically select channels free from interference, while TPC helps optimise transmit power levels to reduce interference with neighbouring networks. In addition to improving reliability, the managed spectrum can also help ensure compliance with regulatory requirements for wireless devices. By avoiding interference with other wireless services, industrial Wi-Fi networks can maintain performance and prevent costly downtime due to regulatory violations. One challenge with implementing managed spectrum in industrial settings is the need for coordination among multiple Wi-Fi networks. Industrial Wi-Fi networks are often deployed in environments with many access points, each using different channels and differing transmit power levels. Advanced spectrum management techniques such as Cooperative Spectrum Sensing (CSS) and Spectrum Resource Management (SRM) can coordinate and optimise spectrum usage across multiple networks to address this [399, 400].

The adoption of 6GHz frequencies and managed spectrum has the potential to improve Wi-Fi reliability in industrial applications significantly. By leveraging wider bandwidths and spectrum management techniques, industrial Wi-Fi networks can achieve higher data rates, lower latency, and improved reliability [401]. As industrial applications rely more on wireless connectivity, these technologies will become increasingly important for ensuring optimal network performance and reducing downtime.

7.5.1 Strategies to Improve Performance

Based on the analysis and understanding of the factors influencing network performance, we propose the following strategies to improve the Wi-Fi 6E-based industrial network utilising the SparkplugBv1 protocol:

- **Wireless Site Survey:** Conduct a comprehensive wireless site survey to identify areas with weak signal strength, potential interference sources, and areas prone to congestion. This survey will guide the placement of access points, antennas, and industrial devices to optimise signal coverage and minimise interference.
- **Channel Optimisation:** Analyse the neighbouring Wi-Fi networks and select optimal 6 GHz frequency band channels with minimal interference. Leveraging features such as Dynamic Frequency Selection (DFS) to automatically switch to less congested channels can help mitigate interference issues.
- **QoS Implementation**: Implement Quality of Service (QoS) mechanisms to prioritise critical industrial data traffic over non-critical traffic. This ensures that time-sensitive data, such as control signals, receive higher priority and is transmitted with lower latency, improving overall network performance.

Chapter 8

Appendix A

8.1 Wi-Fi data formats

Element	Size(Bytes)	Description
Frame Control	2	describes the frame type, version and subtype metadata
Duration	2	defines length of the frame
Address 1	6	Destination address
Address 2	6	Source address of the sending device
Address 3	6	Network BSSID
Sequence Control	2	Ensure the correct ordering of fragmented data streams
address 4	6	
Frame Body	0-2113	Payload to be carried from upper layer
CRC		Cyclic redundancy check provides redundancy to protect data from interference

Table **(8.1)** –802.11 frame structure

Subfield	Size	Description
Trigger Type	4	is of type: Basic,Beamforming Report Poll, MU-Bar, MU-RTS....
Length	12	L-SIG Length value of
Cascade	1	indicator for subsequent trigger frames
Required CS	1	bit of signal to STAs indicate they must sense the channel before sending
BW	2	sets the bandwidth in the HE-SIG-A of the triggered uplink frame
GI-LTF Type	2	set the guard interval and long training field
MU-MIMO LTF Mode	1	0 indicates single stream pilots
HE-LTF Symbols	3	is the number of
STBC	1	is used to enable the space-time block coding on the triggered frame
LDPC Extra	1	enables Low-Density Parity-Check code extra symbol segment
AP TX Power	6	the combined average power settings of 20MHz bandwidth of transmitting antennas
Packet Extension	3	bits used to set the duration of the packet extension of the triggered frame
Spatial Reuse	16	sets the value for Spatial reuse in the SIG-A field in the triggered frame
Doppler	1	indicator for transmission using high-doppler mode
HE-SIG-A Reserved	9	reserved bits in the He-SIg-A field are set
Reserved	1	Missing Row Value

Table **(8.2)** –802.11 Common information field subfield

Frame Type	Description
PS-Poll	Power Save poll is used by an STA when it is waiting for additional data
Block-ACK	Block is used to acknowledge a set of data with output the need for sending individual blocks per data frame. This improvement can save time
BAR	STA can issue a Block ACK Request; then it wants to verify the receiver can send Block ACKs

Table **(8.3)** –802.11 Control frames description

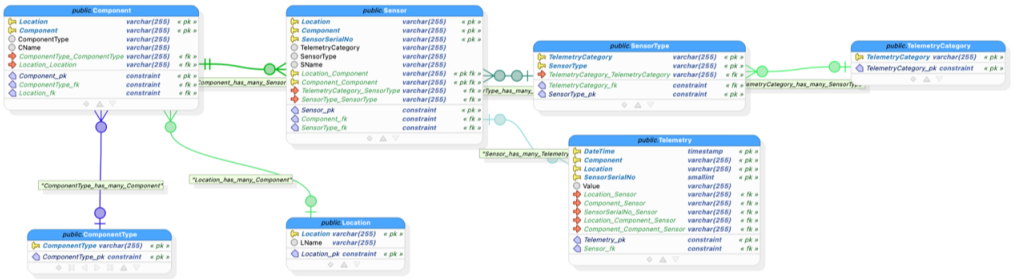


Figure **(8.1)** –Database schema for Edge based Telemetry Database

Table **(8.4)** –802.11 management Subtypes

Description	Subtype bits
Association Request	0000
Association Response	0001
Reassociation Response	0010
Probe Request	0011
Probe Response	0100
Beacon	0101
Announcement Traffic indication message	1000
Disassociation	1010
Authentication	1011
Deauthentication	1100
Action	1101

Table **(8.5)** –802.11 management frame structure

Element	**Size(Bytes)**	**Description**
Frame Control	2	describes the frame type, version and subtype metadata
Duration	2	defines length of the frame
Destination Address	6	Destination address
Source Address	6	Source address of the sending device
BSSID	6	Network BSSID
Sequence Control	2	Ensure the correct ordering of fragmented data streams
Frame Body	0-2113	Payload to be carried from upper layer
CRC		Cyclic redundancy check provides redundancy to protect data from interference

Message Type	Description
NBIRTH	State management is a critical feature of Sparkplug. For real-time SCADA applications, the host must know the state of the network and connected device. The NBIRTH message acts as a birth certificate and is the first message that an EoN node publishes when a session with a broker is established. The NBIRTH messages are comprised of the metadata and metrics definitions which the sending device will send
NDEATH	Another essential aspect of state management is managing the state of devices which go offline—leveraging the notion of last will from MQTT. When an EoN sends an NDEATH message, all MQTT client subscriptions will set their metrics to STALE and have an associated timestamp noting the NDEATH event.
DBIRTH	Birth certificates from Devices are often sent via an EoN node which acts as a gateway for connected devices connecting to a Sparkplug network. When an EoN is
DDEATH	The EoN node publishes a DDEATH message when a connected device becomes unavailable. Clients who are subscribed to the device should then set their metrics to STALE from the device and store the timestamp of when the DEATH message was received
NDATA	Node data message is sent after the NBIRTH and the EoN node are connected. Either time-based or reporting can send NDATA by exception. It will begin publishing data either in a report or by exception. The typical payload can be made up of any metrics or all metrics collected by the EoN node
DDATA	Device data message is the message type used for devices to send data topics Once the EoN node and the devices are online, the
NCMD	Node command message is used to send commands to any connected EoN nodes, such as control messages
DCMD	Device command message is used to send commands to any device connected to the system, such as control messages
STATE	The state is an application state message, and environments are designed for redundancy or scalability. EoN nodes must be aware of the state of the SCADA/IIOT host. The host publishes birth and death certificates when a new connection is established. When a BIRTH message is sent, the payload is ONLINE; when a DEATH message is sent, the payload is to, while the last will payload to OFFLINE.

Table **(8.6)** –Sparkplug version B message types

Message Type	SparkPlug code

NBIRTH	spBv1.0/IMR1.mul.med-d/NBIRTH/finish1/{mm-senss {
	"timestamp": <timestamp>,
	"metrics": [{
	"name": <metric_name>,
	"alias": <alias>,
	"timestamp": <timestamp>,
	"dataType": <datatype>,
	"value": <value>
	}],
	"seq": <sequence_number>
	}

NDEATH	spBv1.0/IMR1.mul.med-d/NBIRTH/finish1/{"timestamp": <timestamp>,"seq": <1234>}
DBIRTH	spBv1.0/IMR1.mul.med-d/DBIRTH/finish1/mmp
DDEATH	spBv1.0/IMR1.mul.med-d/NDEATH/finish1/{mm-senss {"timestamp": <timestamp>,"seq": <1234>
NDATA	spBv1.0/IMR1.mul.med-d/NDATA/finish1/mmp
DDATA	spBv1.0/IMR1.mul.med-d/DDATA/finish1/{mm-senss {"timestamp": <timestamp>,"seq": <1234>
NCMD	//send a command to reboot a device spBv1.0/IMR1.mul.med-d/NDEATH/finish1/'Reboot':BOOL:True
DCMD	*//Send a command to turn the GREEN LED On* spBv1.0/IMR1.mul.med-d/DDATA/finish1/{mm-senss['Outputs/LEDs/green':BOOL:true] }
STATE	'State/Ignition-MQTT, ONLINE

Table **(8.7)** –Sparkplug version B message types for finishing machine

Bibliography

[1] T.Snyder and G.Byrd. The internet of everything. *Computer*, 50:8–9, 2017. doi:10.1109/MC.2017.179.

[2] S. Gusmeroli, H. Sundmaeker, and A. Bassi. Internet of things strategic research roadmap. *2016 11th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 9–52, 2016.

[3] L. Benini, E. Farella, and C. Guiducci. Wireless sensor networks: Enabling technology for ambient intelligence. *Microelectronics Journal*, 37:1639–1649, 12 2006. doi:10.1016/j.mejo.2006.04.021.

[4] ITU. The internet of things. Technical report, International Telecommunications Union, 2005. doi:10.1109/IEEESTD.2007.373646.

[5] W. E. Forum. What is the internet of things - an explainer | world economic forum. URL `https://www.weforum.org/agenda/2021/03/what-is-the-internet-of-things/`.

[6] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy. Smart objects as building blocks for the internet of things. *IEEE Internet Computing*, 14:44–51, 2009. doi:10.1109/MIC.2009.143.

[7] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin. Iot gateway: Bridgingwireless sensor networks into internet of things. *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pages 347–352, 2010. doi:10.1109/EUC.2010.58.

[8] P. Prakash, K. G. Darshaun, P. Yaazhlene, M. V. Ganesh, and B. Vasudha. Fog computing: Issues, challenges and future directions. *International Journal of Electrical and Computer Engineering*, 7:3669–3673, 12 2017. doi:10.11591/ijece.v7i6.pp3669-3673.

[9] K.-D. Chang, J.-L. Chen, C.-Y. Chen, and H.-C. Chao. Iot operations management and traffic analysis for future internet. In *Computing, Communications and Applications Conference*, pages 138–142. IEEE, 1 2012. doi:10.1109/ComComAp.2012.6154018.

[10] IDC. Idc's worldwide iot platforms and analytics taxonomy, 2020. Technical report, International Data Corporation, 2020. URL `https://www.idc.com/getdoc.jsp?containerId=US45860020`.

[11] F. Magazine. 10 charts that will challenge your perspective of iot's growth. URL `https://www.forbes.com/sites/louiscolumbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/?sh=1af769e73ecc`.

[12] NewsWire. Agriculture iot market worth $32.75 billion by 2027 market, 2021. URL https://tinyurl.com/39mymrff.

[13] M. T. Hoske. Industrial internet of things, industry 4.0. *Control Engineering*, 62:26–35, 2015. URL http://www.scopus.com/inward/record.url?eid=2-s2.0-84938283377&partnerID=tZOtx3y1.

[14] H. Lasi, P. Fettke, H.-G. G. Kemper, T. Feld, M. Hoffmann, A. Gilchrist, H. Lasi, P. Fettke, H.-G. G. Kemper, T. Feld, and M. Hoffmann. Industry 4.0. Technical report, European Commission, 2014. doi:10.1007/s12599-014-0334-4.

[15] D. Ivanov, A. Dolgui, B. Sokolov, F. Werner, and M. Ivanova. A dynamic model and an algorithm for short-term supply chain scheduling in the smart factory industry 4.0. *Journal of Production Research*, 54:386–402, 2016. doi:10.1080/00207543.2014.999958.

[16] B. Vavra. A hands-on approach for manufacturing. *Plant Engineering*, 69:26–27, 29, 33, 36, 2015. URL http://search.proquest.com/docview/1711005457?accountid=13031%5Cnhttp://sfx.nelliportaali.fi/nelli28b?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=unknown&sid=ProQ:ProQ%3Aabiglobal&atitle=A+hands-on+approach+for+manufacturing&title=P.

[17] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen. A survey on internet of things from industrial market perspective. *IEEE Access*, 2:1660–1679, 2014. doi:10.1109/ACCESS.2015.2389854.

[18] A. P. Castellani, N. Buit, P. Casari, M. Rossi, Z. Shelby, and M. Zorzi. Architecture and protocols for the internet of things: A case study. *. . .), 2010 8th IEEE . . .*, pages 678–683, 2010. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5470520.

[19] J. Theunissen, H. Xu, R. Y. Zhong, and X. Xu. Smart agv system for manufacturing shopfloor in the context of industry 4.0. In *2018 25th International Conference on Mechatronics and Machine Vision in Practice (M2VIP)*, 2018. doi:10.1109/M2VIP.2018.8600887.

[20] R. Davies. Industry 4.0. digitalisation for productivity and growth. Technical report, European Parliment, 2015.

[21] M. Brettel. How virtualization , decentralization and network building change the manufacturing landscape :. *international journal of mechanical, aerospace, Industrial,mechatronic and manufacturing engineering*, 8:37–44, 2014.

[22] A. Hahn. Operational technology and information technology in industrial control systems. In *Advances in Information Security*, volume 66, pages 51–68, 2016. doi:10.1007/978-3-319-32125-7_4.

[23] ETSI. Network functions virtualisation (nfv); resiliency requirements. Technical report, ETSI, 2015. doi:DGS/NFV-0011.

[24] T. Cruz, P. Simões, and E. Monteiro. Virtualizing programmable logic controllers: Toward a convergent approach. *IEEE Embedded Systems Letters*, 8:69–72, 2016. doi:10.1109/LES.2016.2608418.

[25] M. Alam, J. Rufino, J. Ferreira, S. H. Ahmed, N. Shah, and Y. Chen. Orchestration of microservices for iot using docker and edge computing. *IEEE Communications Magazine*, 56:118–123, 2018. doi:10.1109/mcom.2018.1701233.

[26] D. F. Merchan, J. A. Peralta, A. Vazquez-Rodas, L. I. Minchala, and D. Astudillo-Salinas. Open source scada system for advanced monitoring of industrial processes. In *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, 2017. doi:10.1109/inciscos.2017.9.

[27] N. Finn. Introduction to time-sensitive networking. *IEEE Communications Standards Magazine*, 2:22–28, 2018. doi:10.1109/mcomstd.2018.1700076.

[28] F. Foukalas, P. Pop, F. Theoleyre, C. A. Boano, and C. Buratti. Dependable wireless industrial iot networks: Recent advances and open challenges. In *2019 IEEE European Test Symposium (ETS)*, volume 2019-May, 2019. doi:10.1109/ETS.2019.8791551.

[29] R. Sousa, P. Pedreiras, and P. Gon??alves. Enabling iiot ip backbones with real-time guarantees. In *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, volume 2015-Octob, 2015. doi:10.1109/ETFA.2015.7301497.

[30] M. Patel, J. Shangkuan, and C. Thomas. What's new with the internet of things? *McKinsey Quarterly*, 2017, 2017.

[31] J. Ren, Y. He, G. Huang, G. Yu, Y. Cai, and Z. Zhang. An edge-computing based architecture for mobile augmented reality. *IEEE Network*, 33:162–169, 7 2019. doi:10.1109/MNET.2018.1800132.

[32] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang, and W. Shi. Edge computing for autonomous driving: Opportunities and challenges. *Proceedings of the IEEE*, 57, 2019. doi:10.1109/JPROC.2019.2915983.

[33] P. Ferrari, E. Sisinni, D. Brandao, and M. Rocha. Evaluation of communication latency in industrial iot applications. In *2017 IEEE International Workshop on Measurement and Networking (M and N)*, pages 1–6. IEEE, 9 2017. doi:10.1109/IWMN.2017.8078359.

[34] O. Salman, I. Elhajj, A. Kayssi, and A. Chehab. Edge computing enabling the internet of things. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 603–608. IEEE, 12 2015. doi:10.1109/WF-IoT.2015.7389122.

[35] K. Yelamarthi, M. S. Aman, and A. Abdelgawad. An application-driven modular iot architecture. *Wireless Communications and Mobile Computing*, 2017, 2017. doi:10.1155/2017/1350929.

[36] P. J. Escamilla-Ambrosio, A. Rodríguez-Mota, E. Aguirre-Anaya, R. Acosta-Bermejo, and M. Salinas-Rosales. Distributing computing in the internet of things: Cloud, fog and edge computing overview. In *NEO 2016. Studies in Computational Intelligence*, pages 87–115. Springer International Publishing, 2016. doi:10.1007/978-3-319-64063-1_4.

[37] P. Skarin, W. Tarneberg, K.-E. Arzen, and M. Kihl. Towards mission-critical control at the edge and over 5g. In *2018 IEEE International Conference on Edge Computing*, 2018. doi:10.1109/edge.2018.00014.

[38] S. Naveen and M. R. Kounte. Key technologies and challenges in iot edge computing. In *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pages 61–65. IEEE, 12 2019. doi:10.1109/I-SMAC47947.2019.9032541.

[39] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. Fog computing and its role in the internet of things. In *MCC 2012: Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, page 13, 2012. doi:10.1145/2342509.2342513.

[40] J. Gedeon, F. Brandherm, R. Egert, T. Grube, and M. Mühlhäuser. What the fog? edge computing revisited: Promises, applications and future challenges. In *IEEE Access*, volume 7. IEEE, 2019. doi:10.1109/ACCESS.2019.2948399.

[41] N. Ahmed, H. Rahman, and M. I. Hussain. A comparison of 802.11ah and 802.15.4 for iot. *ICT Express*, 2, 2016. doi:10.1016/j.icte.2016.07.003.

[42] K. Dolui and S. K. Datta. Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. In *GIoTS 2017 - Global Internet of Things Summit, Proceedings*, 2017. doi:10.1109/GIOTS.2017.8016213.

[43] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue. All one needs to know about fog computing and related edge computing paradigms: A complete survey. In *Journal of Systems Architecture Journal of Systems Architecture*, volume 98, 2019. doi:10.1016/j.sysarc.2019.02.009.

[44] M. Satyanarayanan. The emergence of edge computing. *Computer*, 50:30–39, 1 2017. doi:10.1109/MC.2017.9.

[45] Cisco. Cisco annual internet report (2018–2023). *Cisco*, 2020.

[46] K.Cao, Y.Liu, G.Meng, and Q.Sun. An overview on edge computing research. *IEEE Access*, 8:85714–85728, 2020. doi:10.1109/ACCESS.2020.2991734.

[47] S. Parikli, D. Dave, R. Patel, and N. Doshi. Security and privacy issues in cloud, fog and edge computing. In *Procedia Computer Science*, volume 160, 2019. doi:10.1016/j.procs.2019.11.018.

[48] A. Frotzscher, U. Wetzker, M. Bauer, M. Rentschler, M. Beyer, S. Elspass, and H. Klessig. Requirements and current solutions of wireless communication in industrial automation. In *2014 IEEE International Conference on Communications Workshops, ICC 2014 2014 IEEE International Conference on Communications Workshops, ICC 2014*, pages 67–72, 2014. doi:10.1109/ICCW.2014.6881174.

[49] R. Candell, M. Hany, K. B. Lee, Y. Liu, J. Quimby, and K. Remley. Guide to industrial wireless systems deployments. Technical report, National Institute of Standards and Technology, 4 2018. doi:10.6028/NIST.AMS.300-4.

[50] R. Candell and M. Kashef. Industrial wireless: Problem space, success considerations, technologies, and future direction. Technical report, NIST, 9 2017. doi:10.1109/RWEEK.2017.8088661.

[51] X. Vilajosana, C. Cano, B. Martinez, P. Tuset, J. Melià, and F. Adelantado. The wireless technology landscape in the manufacturing industry: A reality check. *arXiv*, 2018.

[52] C. Schellenberger, M. Zimmermann, and H. D. Schotten. Wireless communication for modular production facilities. *VDE ITG Conference on Mobile Communication*, 4 2018.

[53] R. Zurawski. *Industrial Communication Technology Handbook*. Taylor and Francis Group, 2017.

[54] P. A. M. Devan, F. A. Hussin, R. Ibrahim, K. Bingi, and F. A. Khanday. A survey on the application of wirelesshart for industrial process monitoring and control. In *Sensors*, volume 21, 2021. doi:10.3390/s21154951.

[55] K. Pahlavan and P. Krishnamurthy. Evolution and impact of wi-fi technology and applications: A historical perspective. In *International Journal of Wireless Information Networks*, volume 28, 2021. doi:10.1007/s10776-020-00501-8.

[56] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and zigbee standards. In *Computer Communications*, volume 30. Elsevier, 2007. doi:10.1016/j.comcom.2006.12.020.

[57] K. E. Nolan, M. Y. Kelly, M. Nolan, J. Brady, and W. Guibene. Techniques for resilient real-world iot. In *2016 International Wireless Communications and Mobile Computing Conference, IWCMC 2016*, 2016. doi:10.1109/IWCMC.2016.7577061.

[58] R. Candell, K. A. Remley, J. T. Quimby, D. Novotny, A. Curtin, P. B. Papazian, M. Kashef, and J. Diener. Industrial wireless systems radio propagation measurements. Technical report, NIST, 2017. doi:10.6028/NIST.TN.1951.

[59] A. Willig. Recent and emerging topics in wireless industrial communications: A selection. *IEEE Transactions on Industrial Informatics*, 4:102–122, 2008. doi:10.1109/TII.2008.923194.

[60] S. Savazzi, S. Guardiano, and U. Spagnolini. Wireless sensor network modeling and deployment challenges in oil and gas refinery plants. *International Journal of Distributed Sensor Networks*, 2013, 2013. doi:10.1155/2013/383168.

[61] G. Anastasi, M. Conti, and M. D. Francesco. A comprehensive analysis of the mac unreliability problem in ieee 802.15.4 wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 7, 2011. doi:10.1109/TII.2010.2085440.

[62] S. Wang, J. Ouyang, D. Li, and C. Liu. An integrated industrial ethernet solution for the implementation of smart factory. *IEEE Access*, 5, 2017. doi:10.1109/ACCESS.2017.2770180.

[63] D. Cavalcanti, J. Perez-Ramirez, M. M. Rashid, J. Fang, M. Galeev, and K. B. Stanton. Extending accurate time distribution and timeliness capabilities over the air to enable future wireless industrial automation systems. *Proceedings of the IEEE*, 107:1132–1152, 2019. doi:10.1109/jproc.2019.2903414.

[64] A. Rostami. Private 5g networks for vertical industries: Deployment and operation models. In *2019 IEEE 2nd 5G World Forum (5GWF)*, pages 433–439. IEEE, 9 2019. doi:10.1109/5GWF.2019.8911687.

[65] A. Aijaz. High-performance industrial wireless: Achieving reliable and deterministic connectivity over ieee 802.11 wlans. *IEEE Open Journal of the Industrial Electronics Society*, 1, 2020. doi:10.1109/ojies.2020.2983259.

[66] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz. A survey on 5g networks for the internet of things: Communication technologies and challenges. *IEEE Access*, 6:3619–3647, 2018. doi:10.1109/ACCESS.2017.2779844.

[67] F. M. for Economic Affairs and Energy. Plattform industrie 4.0. *Plattform Industrie 4.0*, 2019.

[68] W. wahlster. (noindustrie 4.0: Mit dem internet der dinge auf dem weg zur 4. industriellen revolution title). *VDI nachrichten*, 2011. URL `http://www.wolfgang-wahlster.de/wordpress/wp-content/uploads/Industrie_4_0_Mit_dem_Internet_der_Dinge_auf_dem_Weg_zur_vierten_industriellen_Revolution_2.pdf`.

[69] IIC. Industrial internet consortium. URL `https://www.iiconsortium.org/`.

[70] G. Sziebig and P. Korondi. Effect of robot revolution initiative in europe - cooperation possibilities for japan and europe. In *IFAC-PapersOnLine*, volume 48, 2015. doi:10.1016/j.ifacol.2015.12.027.

[71] K. Fukuda. Science, technology and innovation ecosystem transformation toward society 5.0. *International Journal of Production Economics*, 220, 2020. doi:10.1016/j.ijpe.2019.07.033.

[72] A. C. Pereira and F. Romero. A review of the meanings and the implications of the industry 4.0 concept. *Procedia Manufacturing*, 13, 2017. doi:10.1016/j.promfg.2017.09.032.

[73] S. Vaidya, P. Ambad, and S. Bhosle. Industry 4.0 – a glimpse. *Procedia Manufacturing*, 20:233–238, 2018. doi:10.1016/j.promfg.2018.02.034.

[74] C. L. Garay-Rondero, J. L. Martinez-Flores, N. R. Smith, S. O. C. Morales, and A. Aldrette-Malacara. Digital supply chain model in industry 4.0. *Journal of Manufacturing Technology Management*, 31, 2020. doi:10.1108/JMTM-08-2018-0280.

[75] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman. Intelligent manufacturing in the context of industry 4.0: A review. *Engineering*, 3:616–630, 10 2017. doi:10.1016/J.ENG.2017.05.015.

[76] I. Seoane-Viaño, S. J. Trenfield, A. W. Basit, and A. Goyanes. Translating 3d printed pharmaceuticals: From hype to real-world clinical applications. *Advanced Drug Delivery Reviews*, 174:553–575, 7 2021. doi:10.1016/j.addr.2021.05.003.

[77] M. Elbadawi, L. E. McCoubrey, F. K. H. Gavins, J. J. Ong, A. Goyanes, S. Gaisford, and A. W. Basit. Harnessing artificial intelligence for the next generation of 3d printed medicines. *Advanced Drug Delivery Reviews*, 175:113805, 8 2021. doi:10.1016/j.addr.2021.05.015.

[78] M. K.Bahrin and M.Fauzi. Industry 4.0: A review on industrial automation and robotic. In *Jurnal Teknologi*, volume 78. Penerbit UTM Press, jun 2016. doi:10.11113/jt.v78.9285.

[79] L. U. Ha, F. Ferreira, and A. Marques. Digitisation and industry 4.0 in the portuguese textile and clothing sector. *Industria Textila*, 70, 2019. doi:10.35530/IT.070.04.1612.

[80] O. Senvar and E. Akkartal. an overview to industry 4.0. *International Journal of Information, Business and Management*, 10, 2018.

[81] E. Y. Nakagawa, P. O. Antonino, F. Schnicke, R. Capilla, T. Kuhn, and P. Liggesmeyer. Industry 4.0 reference architectures: State of the art and future trends. *Computers and Industrial Engineering*, 156:107241, 6 2021. doi:10.1016/j.cie.2021.107241.

[82] P. Kostal and K. Velisek. Flexible manufacturing system. *World Academy of Science, Engineering and Technology*, 77, 2011. doi:10.4324/9781482278392-20.

[83] M. Munsamy and A. Telukdarie. Application of industry 4.0 towards achieving business sustainability. In *IEEE International Conference on Industrial Engineering and Engineering Management*, volume 2019-Decem, 2019. doi:10.1109/IEEM.2018.8607566.

[84] I. Heritage. Protecting industry 4.0: challenges and solutions as it, ot and ip converge. *Network Security*, 2019:6–9, 10 2019. doi:10.1016/S1353-4858(19)30120-5.

[85] I.-S. from EU. Business guide to industrial iot (industrial internet of things). URL `https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/`.

[86] Frost and Sullivan. Application of edge computing in industrial internet of things. URL `https://ww2.frost.com/frost-perspectives/application-of-edge-computing-in-industrial-internet-of-things/`.

[87] M. Hermann, T. Pentek, and B. Otto. Design principles for industrie 4.0 scenarios. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, volume 2016-March, 2016. doi:10.1109/HICSS.2016.488.

[88] A. G. Frank, L. S. Dalenogare, and N. F. Ayala. Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics*, 210, 2019. doi:10.1016/j.ijpe.2019.01.004.

[89] Top 10 iot applications in 2020 - which are the hottest areas right now? URL `https://iot-analytics.com/top-10-iot-applications-in-2020/`.

[90] A. J. Biron. The state of industrial internet of things 2019: Spotlight on operational effectiveness. *PTC International*, 2019.

[91] PTC. The state of the industrial internet of things 2017. Technical report, PTC technologies, 2017. URL `https://www.abiresearch.com/press/professional-services-driving-iot-`.

[92] M.Schallehn, C.Schorling, P.Bowen, and O.Straehle. Beyond proofs of concept: Scaling the industrial iot. Technical report, Bain and Company, 2019.

[93] B. Galloway and G. P. Hancke. Introduction to industrial control networks. *IEEE COMMUNICATIONS SURVEYS AND TUTORIALS*, 15:860–880, 2013. doi:10.1109/surv.2012.071812.00124.

[94] M. Crnjac, I. Veža, and N. Banduka. From concept to the introduction of industry 4.0. *International Journal of Industrial Engineering and Management*, 8, 2017.

[95] R. Titmarsh, F. Assad, and R. Harrison. Contributions of lean six sigma to sustainable manufacturing requirements: An industry 4.0 perspective. In *Procedia CIRP*, volume 90, 2020. doi:10.1016/j.procir.2020.02.044.

[96] J. Fortuny-Santos, P. R. de Arbulo López, I. Luján-Blanco, and P. K. Chen. Assessing the synergies between lean manufacturing and industry 4.0. *Direccion y Organizacion*, 2020. doi:10.37610/dyo.v0i71.579.

[97] M. S. Bali, K. Gupta, K. K. Bali, and P. K. Singh. Towards energy efficient nb-iot: A survey on evaluating its suitability for smart applications. *Materials Today: Proceedings*, 235, 2021. doi:10.1016/j.matpr.2020.11.1027.

[98] A. Schütze, N. Helwig, and T. Schneider. Sensors 4.0 - smart sensors and measurement technology enable industry 4.0. *Journal of Sensors and Sensor Systems*, 7, 2018. doi:10.5194/jsss-7-359-2018.

[99] K. Campell. A broader view of manufacturing | automation world, 2018. URL `https://www.automationworld.com/home/blog/13310069/a-broader-view-of-manufacturing`.

[100] P. Dalwalla, E. Delahostria, D. Noller, L. Childress, A. Boyd, B. Scholten, M. Schneider, J. Vieille, and C. Pipero. *The Hitchhiker's Guide to Manufacturing Operations Management*. ISA, 2007.

[101] M. Åkerman. *Implementing Shop Floor IT for Industry 4.0*. PhD thesis, Department of Industrial and Materials Science CHALMERS UNIVERSITY OF TECHNOLOGY, 6 2018.

[102] N. Agarwal and A. Brem. Strategic business transformation through technology convergence: implications from general electric's industrial internet initiative. *International Journal of Technology Management*, 67:196, 2015. doi:10.1504/IJTM.2015.068224.

[103] Y. L. The and A. G. Kuusk. Aligning iiot and isa-95 to improve asset management in process industries. In *World Congress on Engineering Asset Management*, 2021. doi:10.1007/978-3-030-64228-0_14.

[104] D. C. Castillón, J. C. Martín, D. P.-M. Suarez, Á. R. Martínez, and V. L. Álvarez. Automation trends in industrial networks and iiot. In *Automation Trends in Industrial Networks and IIoT*, pages 161–187. Springer International Publishing, 2020. doi:10.1007/978-3-030-42500-5_4.

[105] R. Kazala and P. Straczynski. The most important open technologies for design of cost efficient automation systems. *IFAC-PapersOnLine*, 52:391–396, 2019. doi:10.1016/j.ifacol.2019.12.567.

[106] K. Stouffer, J. Falco, and K. Scarfone. Guide to industrial control systems (ics) security recommendations of the national institute of standards and technology. *NIST Special Publication*, 2007.

[107] H. H. Cheng, F. Proctor, J. L. Michaloski, , and W. P. Shackleford. Real-time computing in open systems for manufacturing. *Journal of Computing and Information Science in Engineering*, 1:92–99, 3 2001. doi:10.1115/1.1351819.

[108] S. Mackay, E. Wright, D. Reynders, and J. Park. Modbus overview, 2004. doi:10.1016/b978-075065807-2/50031-5.

[109] B. G. Houk, D. L. DeBari, S. Bitar, D. Bartusiak, and K. Ribe. Open process automation for distributed control systems. *Chemical Engineering Progress*, 116, 2020.

[110] Microsoft : Autonomous systems. URL `https://autonomoussystems.microsoft.com/welcome/`.

[111] K. Ahmed, J. O. Blech, M. A. Gregory, and H. W. Schmidt. Software defined networks in industrial automation. *Journal of Sensor and Actuator Networks*, 7, 2018. doi:10.3390/jsan7030033.

[112] V. Bourne. After the fall. Technical report, Vanson Bourne, 2019.

[113] D. S. Thomas and B. A. Weiss. Economics of manufacturing machinery maintenance a survey and analysis of u.s. costs and benefits nist advanced manufacturing series 100-34. *NIST Special Publication*, 2016. doi:10.6028/NIST.AMS.100-34.

[114] J. Lee, F. Wu, W. Zhao, M. Ghaffari, L. Liao, and D. Siegel. Prognostics and health management design for rotary machinery systems - reviews, methodology and applications. *Mechanical Systems and Signal Processing*, 42, 2014. doi:10.1016/j.ymssp.2013.06.004.

[115] G. W. Vogl, B. A. Weiss, and M. Helu. A review of diagnostic and prognostic capabilities and best practices for manufacturing. *Journal of Intelligent Manufacturing*, 30, 2019. doi:10.1007/s10845-016-1228-8.

[116] D. Thomas and B. Weiss. Maintenance costs and advanced maintenance techniques in manufacturing machinery: Survey and analysis. *International Journal of Prognostics and Health Management*, 12, 2021. doi:10.36001/IJPHM.2021.V12I1.2883.

[117] X. Jin, D. Siegel, B. A. Weiss, E. Gamel, W. Wang, J. Lee, and J. Ni. The present status and future growth of maintenance in us manufacturing: Results from a pilot survey. In *Manufacturing Review*, volume 3, 2016. doi:10.1051/mfreview/2016005.

[118] G. P. Sullivan, R. Pugh, A. P. Melendez, and W. D. Hunt. Operations and maintenance best practices a guide to achieving operational efficiency. Technical report, the international society for optics and photonics, 2010.

[119] J. H. Shin and H. B. Jun. On condition based maintenance policy. *Journal of Computational Design and Engineering*, 2, 2015. doi:10.1016/j.jcde.2014.12.006.

[120] M. G. Pecht. *Prognostics and Health Management of Electronics*. John Wiley and Sons, 2008. doi:10.1002/9780470385845.

[121] W. Tiddens, J. Braaksma, and T. Tinga. Exploring predictive maintenance applications in industry. *Journal of Quality in Maintenance Engineering*, 2020. doi:10.1108/JQME-05-2020-0029.

[122] M. G. Martín, A. P. Álvarez, J. Ordieres-Meré, J. Villalba-Díez, and G. Morales-Alonso. New business models from prescriptive maintenance strategies aligned with sustainable development goals. *Sustainability 2021*, 13, 2021. doi:10.3390/su13010216.

[123] J. Mattioli, P. Perico, and P. O. Robic. Improve total production maintenance with artificial intelligence. In *2020 Third International Conference on Artificial Intelligence for Industries (AI4I)*, 2020. doi:10.1109/AI4I49448.2020.00019.

[124] H. Nordal and I. El-Thalji. Lifetime benefit analysis of intelligent maintenance: simulation modeling approach and industrial case study. *Applied Sciences (Switzerland)*, 11, 2021. doi:10.3390/app11083487.

[125] S. Mullick. A novel approach to distributed field-based gas lift facilities. In *SPE Liquids-Rich Basins Conference*, 2017. doi:10.2118/187490-ms.

[126] J. Z. Sikorska, M. Hodkiewicz, and L. Ma. Prognostic modelling options for remaining useful life estimation by industry. *Mechanical Systems and Signal Processing*, 25, 2011. doi:10.1016/j.ymssp.2010.11.018.

[127] X.-S. Si, W. Wang, C.-H. Hu, and D.-H. Zhou. Remaining useful life estimation – a review on the statistical data driven approaches. *European Journal of Operational Research*, 213:1–14, 8 2011. doi:10.1016/j.ejor.2010.11.018.

[128] N. Li, Y. Lei, L. Guo, T. Yan, and J. Lin. Remaining useful life prediction based on a general expression of stochastic process models. *IEEE Transactions on Industrial Electronics*, 64, 2017. doi:10.1109/TIE.2017.2677334.

[129] W. Huang, H. Khorasgani, C. Gupta, A. Farahat, and S. Zheng. Remaining useful life estimation for systems with abrupt failures. *Annual Conference of the PHM Society*, 10, 9 2018. doi:10.36001/phmconf.2018.v10i1.590.

[130] R. Glawar, F. Ansari, C. Kardos, K. Matyas, and W. Sihn. Conceptual design of an integrated autonomous production control model in association with a prescriptive maintenance model (prima). *Procedia CIRP*, 80:482–487, 2019. doi:10.1016/j.procir.2019.01.047.

[131] W. Polini and A. Corrado. Digital twin of composite assembly manufacturing process. *International Journal of Production Research*, 58, 2020. doi:10.1080/00207543.2020.1714091.

[132] P. van Schalkwyk Shi-Wan Lin Somayeh Malakuti. A short introduction to digital twins | machine design, 2020. URL https://www.machinedesign.com/automation-iiot/article/21122237/a-short-introduction-to-digital-twins.

[133] J. Trauer, S. Schweigert-Recksiek, C. Engel, K. Spreitzer, and M. Zimmermann. What is a digital twin? – definitions and insights from an industrial case study in technical product development. *Proceedings of the Design Society: DESIGN Conference*, 1, 2020. doi:10.1017/dsd.2020.15.

[134] M. R. Enders and N. Hoßbach. Dimensions of digital twin applications - a literature review. In *25th Americas Conference on Information Systems, AMCIS 2019*, 2019.

[135] Dr. michael grieves discusses the future of the digital twin. - asme. URL https://www.asme.org/topics-resources/content/6-question-with-michael-grieves-on-the-future-of-digital-twins.

[136] S. Meng, Y. Ye, Q. Yang, Z. Huang, and W. Xie. Digital twin and its aerospace applications. In *Acta Aeronautica et Astronautica Sinica*, volume 41. Hangkong Xuebao, 2020. doi:10.7527/S1000-6893.2020.23615.

[137] F. Biesinger and M. Weyrich. The facets of digital twins in production and the automotive industry. In *2019 23rd International Conference on Mechatronics Technology (ICMT)*, pages 1–6. IEEE, 10 2019. doi:10.1109/ICMECT.2019.8932101.

[138] M. Chetan, S. Yao, and D. T. Griffith. Multi-fidelity digital twin structural model for a sub-scale downwind wind turbine rotor blade. *Wind Energy*, 2021. doi:10.1002/we.2636.

[139] M. J. Kaur, V. P. Mishra, and P. Maheshwari. *The Convergence of Digital Twin, IoT, and Machine Learning: Transforming Data into Action*, pages 3–17. Springer, 2020. doi:10.1007/978-3-030-18732-3_1.

[140] S. Malakuti and S. Grüner. Architectural aspects of digital twins in iiot systems. In *ECSA 2018: Proceedings of the 12th European Conference on Software Architecture:*. ACM, 2018. doi:10.1145/3241403.3241417.

[141] B. Korth, C. Schwede, and M. Zajac. Simulation-ready digital twin for realtime management of logistics systems. In *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018. doi:10.1109/bigdata.2018.8622160.

[142] N. Mohammadi and J. E. Taylor. Smart city digital twins. In *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, volume 2018-Janua, pages 1–5. IEEE, 11 2017. doi:10.1109/SSCI.2017.8285439.

[143] G. White, A. Zink, L. Codecá, and S. Clarke. A digital twin smart city for citizen feedback. *Cities*, 110:103064, 3 2021. doi:10.1016/j.cities.2020.103064.

[144] A. Fuller, Z. Fan, C. Day, and C. Barlow. Digital twin: Enabling technologies, challenges and open research. *IEEE Access*, 8:108952–108971, 2020. doi:10.1109/ACCESS.2020.2998358.

[145] K. Bruynseels, F. S. de Sio, and J. van den Hoven. Digital twins in health care: Ethical implications of an emerging engineering paradigm. *Frontiers in Genetics*, 9, 2 2018. doi:10.3389/fgene.2018.00031.

[146] F. Tao, W. Liu, J. Liu, X. Liu, Q. Liu, T. Qu, T. Hu, Z. Zhang, F. Xiang, W. Xu, J. Wang, Y. Zhang, Z. Liu, H. Li, J. Cheng, Q. Qi, M. Zhang, H. Zhang, F. Sui, L. He, W. Yi, and H. Cheng. Digital twin and its potential application exploration. *Jisuanji Jicheng Zhizao Xitong/Computer Integrated Manufacturing Systems, CIMS*, 24, 2018. doi:10.13196/j.cims.2018.01.001.

[147] Q. Qi and F. Tao. Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison. *IEEE Access*, 6:3585–3593, 2018. doi:10.1109/ACCESS.2018.2793265.

[148] W. Kritzinger, M. Karner, G. Traar, J. Henjes, and W. Sihn. Digital twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine*, 51:1016–1022, 2018. doi:10.1016/j.ifacol.2018.08.474.

[149] E. Glaessgen and D. Stargel. The digital twin paradigm for future nasa and u.s. air force vehicles. Technical report, NASA, 4 2012. doi:10.2514/6.2012-1818.

[150] T. Peters. Data-driven science and engineering: machine learning, dynamical systems, and control. *Contemporary Physics*, 60, 2019. doi:10.1080/00107514.2019.1665103.

[151] H. Zhang, Q. Liu, X. Chen, D. Zhang, and J. Leng. A digital twin-based approach for designing and multi-objective optimization of hollow glass production line. *IEEE Access*, 5, 2017. doi:10.1109/ACCESS.2017.2766453.

[152] M. Helu, T. Hedberg, and A. B. Feeney. Reference architecture to integrate heterogeneous manufacturing systems for the digital thread. *CIRP Journal of Manufacturing Science and Technology*, 19:191–195, 11 2017. doi:10.1016/j.cirpj.2017.04.002.

[153] T. Y. Pang, J. D. P. Restrepo, C.-T. Cheng, A. Yasin, H. Lim, and M. Miletic. Developing a digital twin and digital thread framework for an 'industry 4.0' shipyard. *Applied Sciences*, 11:1097, 1 2021. doi:10.3390/app11031097.

[154] A. B. A. Alaasam, G. Radchenko, and A. Tchernykh. Stateful stream processing for digital twins: Microservice-based kafka stream dsl. In *2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, pages 804–809. IEEE, 2019. doi:10.1109/SIBIRCON48586.2019.8958367.

[155] L. Zhang and H. Lu. Discussing digital twin from of modeling and simulation. In *Journal of System Simulation*, volume 33, 2021. doi:10.16182/j.issn1004731x.joss.21-0262.

[156] S. Reed, M. Löfstrand, and J. Andrews. Modelling cycle for simulation digital twins. *Manufacturing Letters*, 28:54–58, 4 2021. doi:10.1016/j.mfglet.2021.04.004.

[157] M. Fera, A. Greco, M. Caterino, S. Gerbino, F. Caputo, R. Macchiaroli, and E. D'Amato. Towards digital twin implementation for assessing production line performance and balancing. *Sensors*, 20:97, 12 2019. doi:10.3390/s20010097.

[158] J. L. Kang, C. C. Wang, D. S. H. Wong, S. S. Jang, and C. H. Wang. Digital twin model and dynamic operation for a plant-scale solid oxide fuel cell system. *Journal of the Taiwan Institute of Chemical Engineers*, 118, 2021. doi:10.1016/j.jtice.2021.01.001.

[159] M. Schluse, L. Atorf, and J. Rossmann. Experimentable digital twins for model-based systems engineering and simulation-based development. In *2017 Annual IEEE International Systems Conference (SysCon)*, pages 1–8. IEEE, 4 2017. doi:10.1109/SYSCON.2017.7934796.

[160] Q. Lu, X. Xie, A. K. Parlikad, and J. M. Schooling. Digital twin-enabled anomaly detection for built asset monitoring in operation and maintenance. *Automation in Construction*, 118:103277, 10 2020. doi:10.1016/j.autcon.2020.103277.

[161] F. Tao, F. Sui, A. Liu, Q. Qi, M. Zhang, B. Song, Z. Guo, S. C. Lu, and A. Y. Nee. Digital twin-driven product design framework. *International Journal of Production Research*, 57, 2019. doi:10.1080/00207543.2018.1443229.

[162] M. Macchi, I. Roda, E. Negri, and L. Fumagalli. Exploring the role of digital twin for asset lifecycle management. *IFAC-PapersOnLine*, 51:790–795, 2018. doi:10.1016/j.ifacol.2018.08.415.

[163] C. Cimino, E. Negri, and L. Fumagalli. Review of digital twin applications in manufacturing. *Computers in Industry*, 113, 2019. doi:10.1016/j.compind.2019.103130.

[164] Catapult. Feasibility of an immersive digital twin. Technical report, UK Catapult Centre, 2018. URL `https://www.amrc.co.uk/files/document/219/1536919984_HVM_CATAPULT_DIGITAL_TWIN_DL.pdf`.

[165] S. Corp. Digital twin siemens digital industries software. URL `https://www.plm.automation.siemens.com/global/en/our-story/glossary/digital-twin/24465`.

[166] I. Corporation. Digital twin data representation. URL `https://www.ibm.com/cloud/architecture/architectures/digital-twin-data-representation/`.

[167] 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)*, 13, 2021. doi:10.3390/su13020561.

[168] T. Moi, A. Cibicik, and T. Rølvåg. Digital twin based condition monitoring of a knuckle boom crane: An experimental study. *Engineering Failure Analysis*, 112, 2020. doi:10.1016/j.engfailanal.2020.104517.

[169] M. Short and J. Twiddle. An industrial digitalization platform for condition monitoring and predictive maintenance of pumping equipment. *Sensors (Switzerland)*, 19, 2019. doi:10.3390/s19173781.

[170] W. Kuehn. Digital twins for decision making in complex production and logistic enterprises. *International Journal of Design and Nature and Ecodynamics*, 13, 2018. doi:10.2495/DNE-V13-N3-260-271.

[171] S. West, O. Stoll, J. Meierhofer, and S. Züst. Digital twin providing new opportunities for value co-creation through supporting decision-making. *Applied Sciences (Switzerland)*, 11, 2021. doi:10.3390/app11093750.

[172] W. J. Herlyn and H. Zadek. "digital control twin". *ZWF Zeitschrift fuer Wirtschaftlichen Fabrikbetrieb*, 115, 2020. doi:10.3139/104.112338.

[173] W. Xu, J. Cui, L. Li, B. Yao, S. Tian, and Z. Zhou. Digital twin-based industrial cloud robotics: Framework, control approach and implementation. *Journal of Manufacturing Systems*, 58, 2021. doi:10.1016/j.jmsy.2020.07.013.

[174] G. F. Schneider, H. Wicaksono, and J. Ovtcharova. Virtual engineering of cyber-physical automation systems: The case of control logic. *Advanced Engineering Informatics*, 39, 2019. doi:10.1016/j.aei.2018.11.009.

[175] A. A. Malik and A. Bilberg. Digital twins of human robot collaboration in a production setting. In *Procedia Manufacturing*, volume 17, 2018. doi:10.1016/j.promfg.2018.10.047.

[176] M. Glatt, C. Sinnwell, L. Yi, S. Donohoe, B. Ravani, and J. C. Aurich. Modeling and implementation of a digital twin of material flows based on physics simulation. *Journal of Manufacturing Systems*, 58:231–245, 1 2021. doi:10.1016/j.jmsy.2020.04.015.

[177] F. Tao, H. Zhang, A. Liu, and A. Y. Nee. Digital twin in industry: State-of-the-art. *IEEE Transactions on Industrial Informatics*, 15, 2019. doi:10.1109/TII.2018.2873186.

[178] W. Xiaodong, L. Feng, R. Junhua, and L. Rongyu. A survey of digital twin technology for phm. In *Advances in Intelligent Systems and Computing*, volume 1031 AISC, 2020. doi:10.1007/978-981-13-9406-5_48.

[179] I. Rojek, D. Mikołajewski, and E. Dostatni. Digital twins in product lifecycle for sustainability in manufacturing and maintenance. *Applied Sciences (Switzerland)*, 11, 2021. doi:10.3390/app11010031.

[180] P. Aivaliotis, K. Georgoulias, Z. Arkouli, and S. Makris. Methodology for enabling digital twin using advanced physics-based modelling in predictive maintenance. *Procedia CIRP*, 81:417–422, 2019. doi:10.1016/j.procir.2019.03.072.

[181] Y. Koyama. Introduction to computational design. In *CHI Conference on Human Factors in Computing Systems*, pages 1–4. ACM, 5 2021. doi:10.1145/3411763.3445007.

[182] T. Doka and P. Horak. An approach to creating a simple digital twin for optimizing a small electric concept vehicle drivetrain. In *Conference: 34th International ECMS Conference on Modelling and Simulation*, volume 34, pages 328–333. ECMS, 6 2020. doi:10.7148/2020-0328.

[183] L. Rauch and M. Pietrzyk. Digital twins as a modern approach to design of industrial processes. *Journal of Machine Engineering*, 19, 2019. doi:10.5604/01.3001.0013.0456.

[184] L. Uhlenbrock, C. Jensch, M. Tegtmeier, and J. Strube. Digital twin for extraction process design and operation. *Processes*, 8, 2020. doi:10.3390/PR8070866.

[185] E. Negri, L. Fumagalli, C. Cimino, and M. Macchi. Fmu-supported simulation for cps digital twin. *Procedia Manufacturing*, 28:201–206, 2019. doi:10.1016/j.promfg.2018.12.033.

[186] S. Aheleroff, R. Y. Zhong, and X. Xu. A digital twin reference for mass personalization in industry 4.0. In *Procedia CIRP*, volume 93, 2020. doi:10.1016/j.procir.2020.04.023.

[187] Y. Wang, H. S. Ma, J. H. Yang, and K. S. Wang. Industry 4.0: a way from mass customization to mass personalization production. *Advances in Manufacturing*, 5, 2017. doi:10.1007/s40436-017-0204-7.

[188] C. Voell, P. Chatterjee, A. Rauch, and J. Golovatchev. *How Digital Twins Enable the Next Level of PLM – A Guide for the Concept and the Implementation in the Internet of Everything Era*, volume 540, pages 238–249. Springer, 2018. doi:10.1007/978-3-030-01614-2_22.

[189] T. Y. Lin, Z. Jia, C. Yang, Y. Xiao, S. Lan, G. Shi, B. Zeng, and H. Li. Evolutionary digital twin: A new approach for intelligent industrial product development. *Advanced Engineering Informatics*, 47, 2021. doi:10.1016/j.aei.2020.101209.

[190] E. Technology. What are industrial communication networks? an overview. URL `https://www.electricaltechnology.org/2016/12/industrial-communication-networks-systems.html`.

[191] Y. kuang Chen. S7-1 challenges and opportunities of internet of things s7-1. *Intel Labs series*, pages 383–388, 2012.

[192] OFCOM. M2m application characteristics and their implications for spectrum final report. Technical report, OFCOM UK, 2014.

[193] T. Sauter. The three generations of field-level networks - evolution and compatibility issues. *IEEE Transactions on Industrial Electronics*, 57, 2010. doi:10.1109/TIE.2010.2062473.

[194] J. P. Thomesse. Fieldbus technology in industrial automation. *Proceedings of the IEEE*, 93, 2005. doi:10.1109/JPROC.2005.849724.

[195] M. Felser. Real-time ethernet - industry prospective. *Proceedings of the IEEE*, 93:1118–1129, 6 2005. doi:10.1109/JPROC.2005.849720.

[196] E. Tovar and F. Vasques. Real-time fieldbus communications using profibus networks. *IEEE Transactions on Industrial Electronics*, 46, 1999. doi:10.1109/41.808018.

[197] L. Almeida, P. Pedreiras, and J. A. G. Fonseca. The ftt-can protocol: Why and how. *IEEE Transactions on Industrial Electronics*, 49, 2002. doi:10.1109/TIE.2002.804967.

[198] N. McLauchlan and N. Bessis. A case for real-world smart environments: The development of a remote autonomous energy aware monitoring system using next generation technologies. In *2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 128–135. IEEE, 6 2011. doi:10.1109/IMIS.2011.70.

[199] J. R. Moyne and D. M. Tilbury. The emergence of industrial control networks for manufacturing control, diagnostics, and safety data. *Proceedings of the IEEE*, 95, 2007. doi:10.1109/JPROC.2006.887325.

[200] J. Feld. Profinet - scalable factory communication for all applications. In *IEEE International Workshop*, pages 33–38. IEEE, 2004. doi:10.1109/WFCS.2004.1377673.

[201] D. Jansen and H. Büttner. Real-time ethernet the ethercat solution. In *IEE Computing and Control Engineering*, volume 15, 2004. doi:10.1049/cce:20040104.

[202] Y. K. Chen, J. Chen, Y. S. Cheng, C. Y. Wu, P. C. Chiu, C. H. Kuo, K. H. Hu, and K. T. Hsu. Application of modbus-tcp in tps control system. In *Proceedings of IPAC 2010*, volume 4, pages 376–385, 2010. doi:10.1007/s11704-010-0385-8.

[203] J.-D. Decotignie. Ethernet-based real-time and industrial communications. *Proceedings of the IEEE*, 93:1102–1117, 6 2005. doi:10.1109/JPROC.2005.849721.

[204] E. Bassi, F. Benzi, L. Lusetti, and G. S. Buja. Communication protocols for electrical drives. In *Proceedings of IECON 95 - 21st Annual Conference on IEEE Industrial Electronics*, volume 1, 1995. doi:10.1109/iecon.1995.483494.

[205] S. Vitturi, L. Peretti, L. Seno, M. Zigliotto, and C. Zunino. Real-time ethernet networks for motion control. *Computer Standards and Interfaces*, 33, 2011. doi:10.1016/j.csi.2011.01.005.

[206] P. Danielis, J. Skodzik, V. Altmann, E. B. Schweissguth, F. Golatowski, D. Timmermann, and J. Schacht. Survey on real-time communication via ethernet in industrial automation environments. In *19th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2014*, 2014. doi:10.1109/ETFA.2014.7005074.

[207] K. C. Lee and S. Lee. Performance evaluation of switched ethernet for real-time industrial communications. *Computer Standards and Interfaces*, 24, 2002. doi:10.1016/S0920-5489(02)00070-3.

[208] P. Doyle. Introduction to real-time ethernet i. *The EXTENSION*, 5, 2004.

[209] L. Persson. A comparison between fieldbuses and remote i/o for instruments in the process industry. Master's thesis, Lulea University of Technology, 2007.

[210] P. Gaj, J. Jasperneite, and M. Felser. Computer communication within industrial distributed environment—a survey. *IEEE Transactions on Industrial Informatics*, 9:182–189, 2 2013. doi:10.1109/TII.2012.2209668.

[211] B. Martinez, C. Cano, and X. Vilajosana. A square peg in a round hole: The complex path for wireless in the manufacturing industry. *IEEE Communications Magazine*, 57:109–115, 4 2019. doi:10.1109/MCOM.2019.1800570.

[212] A. Chowdhury and S. A. Raut. Benefits, challenges, and opportunities in adoption of industrial iot. *International Journal of Computational Intelligence and IoT*, 2, 2019.

[213] A. Mahmood, M. I. Ashraf, M. Gidlund, J. Torsner, and J. Sachs. Time synchronization in 5g wireless edge: Requirements and solutions for critical-mtc. *IEEE Communications Magazine*, 57, 2019. doi:10.1109/MCOM.001.1900379.

[214] S. Gangakhedkar, H. Cao, A. R. Ali, K. Ganesan, M. Gharba, and J. Eichinger. Use cases, requirements and challenges of 5g communication for industrial automation. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE, 5 2018. doi:10.1109/ICCW.2018.8403588.

[215] L. F. C. S. Durão, S. Haag, R. Anderl, K. Schützer, and E. Zancul. Digital twin requirements in the context of industry 4.0. In *Cognitive Robotics*, volume 540, pages 71–92, 2018. doi:10.1007/978-3-030-01614-2_19.

[216] Y. Lu, C. Liu, K. I.-K. Wang, H. Huang, and X. Xu. Digital twin-driven smart manufacturing: Connotation, reference model, applications and research issues. *Robotics and Computer-Integrated Manufacturing*, 61:101837, 2 2020. doi:10.1016/j.rcim.2019.101837.

[217] S. K. Memon, K. Nisar, M. H. A. Hijazi, B. S. Chowdhry, A. H. Sodhro, S. Pirbhulal, and J. J. P. C. Rodrigues. A survey on 802.11 mac industrial standards, architecture, security and supporting emergency traffic: Future directions. *Journal of Industrial Information Integration*, 24, 2021. doi:10.1016/j.jii.2021.100225.

[218] K. E. GHOLAMI, Y. MALEH, and I. F. E. FATANI. The ieee 802.15.4 standard in industrial applications: A survey. In *Journal of Theoretical and Applied Information Technology*, volume 99. IEEE, 2021.

[219] M. R. Bhalla and A. V. Bhalla. Generations of mobile wireless technology: A survey. *International Journal of Computer Applications*, 5, 2010. doi:10.5120/905-1282.

[220] S. Andreev, O. Galinina, A. Pyattaev, M. Gerasimenko, T. Tirronen, J. Torsner, J. Sachs, M. Dohler, and Y. Koucheryavy. Understanding the iot connectivity landscape: A contemporary m2m radio technology roadmap. *IEEE Communications Magazine*, 53, 2015. doi:10.1109/MCOM.2015.7263370.

[221] J. Finnegan and S. Brown. A comparative survey of lpwa networking. *Procedia Computer Science*, 155, 2 2018.

[222] M. Serezhina, A. Moschevikin, R. Evmenchikov, and A. Sikora. Using radiating cable for time-of-flight css measurements indoors and outdoors. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, volume 1, pages 91–101. IEEE, 9 2015. doi:10.1109/IDAACS.2015.7340707.

[223] W. Zhang, Y. Qin, W. Zhao, M. Jia, Q. Liu, R. He, and B. Ai. A green paradigm for internet of things: Ambient backscatter communications. *China Communications*, 16, 2019. doi:10.23919/j.cc.2019.07.009.

[224] Z. Guo, K. Zhang, H. Xin, M. Bi, H. He, and W. Hu. An optical access network framework for smart factory in the industry 4.0 era supporting massive machine connections. In *2017 16th International Conference on Optical Communications and Networks (ICOCN)*, volume 2017-January, 2017. doi:10.1109/ICOCN.2017.8121481.

[225] M. Luvisotto, Z. Pang, D. Dzung, M. Zhan, and X. Jiang. Physical layer design of high-performance wireless transmission for critical control applications. *IEEE Transactions on Industrial Informatics*, 13:2844–2854, 12 2017. doi:10.1109/TII.2017.2703116.

[226] D. Fanucchi, B. Staehle, and R. Knorr. On the suitability of 6tisch for industrial wireless communication. In *Communication and networks for automation*, pages 34–48. Springer Link, 2020. doi:10.1007/978-3-662-59895-5_3.

[227] A. Karaagac, J. Haxhibeqiri, I. Moerman, and J. Hoebeke. Time-critical communication in 6tisch networks. In *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pages 161–166. IEEE, 4 2018. doi:10.1109/WCNCW.2018.8368987.

[228] T. Lennvall, J. Akerberg, E. Hansen, and K. Yu. A new wireless sensor network tdma timing synchronization protocol. In *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, volume 0, pages 606–611. IEEE, 7 2016. doi:10.1109/INDIN.2016.7819233.

[229] A. Slalmi, R. Saadane, A. Chehri, and H. Kharraz. How will 5g transform industrial iot: Latency and reliability analysis. In *Smart Innovation, Systems and Technologies*, volume 189, pages 335–345, 2021. doi:10.1007/978-981-15-5784-2_27.

[230] I. S. for Automation. *ISA TR100.00.03-2011 - Wireless Use Requirements for Factory Automation*. URL `https://webstore.ansi.org/standards/isa/isatr10000032011`.

[231] K. Montgomery, R. Candell, Y. Liu, and M. Hany. Wireless user requirements for the factory workcell nist advanced manufacturing series 300-8 wireless user requirements for the factory workcell. *Advanced Manufacturing Series (NIST AMS)*, 1, 2021.

[232] M. Mueck, A. Piipponen, K. Kalliojärvi, G. Dimitrakopoulos, K. Tsagkaris, P. Demestichas, F. Casadevall, J. Pérez-Romero, O. Sallent, G. Baldini, S. Filin, H. Harada, M. Debbah, T. Haustein, J. Gebert, B. Deschamps, P. Bender, M. Street, S. Kandeepan, J. Lota, and A. Hayar. Etsi reconfigurable radio systems: Status and future directions on software defined radio and cognitive radio standards. *IEEE Communications Magazine*, 48, 2010. doi:10.1109/MCOM.2010.5560591.

[233] N. Thornhill and W. Ikram. Wireless communication in process automation: a survey of opportunities, requirements, concerns and challenges. In *UKACC International Conference on Control 2010*, volume 2010, pages 471–476. Institution of Engineering and Technology, 2010. doi:10.1049/ic.2010.0328.

[234] L. Seno, G. Cena, S. Scanzio, A. Valenzano, and C. Zunino. Enhancing communication determinism in wi-fi networks for soft real-time industrial applications. *IEEE Transactions on Industrial Informatics*, 13, 2017. doi:10.1109/TII.2016.2641468.

[235] F. Tramarin, A. K. Mok, and S. Han. Real-time and reliable industrial control over wireless lans: Algorithms, protocols, and future directions. *Proceedings of the IEEE*, 107, 2019. doi:10.1109/JPROC.2019.2913450.

[236] M. Kaur, S. Kakar, and D. Mandal. Electromagnetic interference. In *2011 3rd International Conference on Electronics Computer Technology*, volume 4, 2011. doi:10.1109/ICECTECH.2011.5941844.

[237] M. Liu, K. Yang, N. Zhao, Y. Chen, H. Song, and F. Gong. Intelligent signal classification in industrial distributed wireless sensor networks based industrial internet of things. *IEEE Transactions on Industrial Informatics*, 17, 2021. doi:10.1109/TII.2020.3016958.

[238] L. Mucchi and A. Carpini. Aggregate interference in ism band: Wbans need cognitivity? In *2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, 2014. doi:10.4108/icst.crowncom.2014.255775.

[239] R. H. de Souza, S. Savazzi, and L. B. Becker. Network design and planning of wireless embedded systems for industrial automation: Applications and case studies in oil refineries. *Design Automation for Embedded Systems*, 19, 2015. doi:10.1007/s10617-015-9162-0.

[240] P. Zand, S. Chatterjea, K. Das, and P. Havinga. Wireless industrial monitoring and control networks: The journey so far and the road ahead. In *Journal of Sensor and Actuator Networks*, volume 1, 2012. doi:10.3390/jsan1020123.

[241] T. Olofsson, A. Ahlén, and M. Gidlund. Modeling of the fading statistics of wireless sensor network channels in industrial environments. *IEEE Transactions on Signal Processing*, 64, 2016. doi:10.1109/TSP.2016.2539142.

[242] S. Zelenbaba, M. Hofer, D. Loschenbrand, G. Kail, M. Schiefer, and T. Zemen. Spatial properties of industrial wireless ultra-reliable low-latency communication mimo links. In *2019 53rd Asilomar Conference on Signals, Systems, and Computers*, volume 2019-November, 2019. doi:10.1109/IEEECONF44664.2019.9048729.

[243] J. Mehami, M. Nawi, and R. Y. Zhong. Smart automated guided vehicles for manufacturing in the context of industry 4.0. In *Procedia Manufacturing*, volume 26, 2018. doi:10.1016/j.promfg.2018.07.144.

[244] W. Wang, S. L. Capitaneanu, D. Marinca, and E. S. Lohan. Comparative analysis of channel models for industrial iot wireless communication. *IEEE Access*, 7, 2019. doi:10.1109/ACCESS.2019.2927217.

[245] S. Vitturi, F. Tramarin, and L. Seno. Industrial wireless networks: The significance of timeliness in communication systems. *IEEE Industrial Electronics Magazine*, 7, 2013. doi:10.1109/MIE.2013.2253837.

[246] P. Ängskog, C. Karlsson, J. F. Coll, J. Chilo, and P. Stenumgaard. Sources of disturbances on wireless communication in industrial and factory environments. In *2010 Asia-Pacific International Symposium on Electromagnetic Compatibility*, 2010. doi:10.1109/APEMC.2010.5475862.

[247] T. M. Chiwewe, C. F. Mbuya, and G. P. Hancke. Using cognitive radio for interference-resistant industrial wireless sensor networks: An overview. *IEEE Transactions on Industrial Informatics*, 11, 2015. doi:10.1109/TII.2015.2491267.

[248] P. Szulewski, D. Śniegulska-Grądzka, and M. Nejman. Active systems for monitoring the cutting process in the industry 4.0 concept. *Mechanik*, 91, 2018. doi:10.17814/mechanik.2018.3.34.

[249] L. Alkama and L. Bouallouche-Medjkoune. Ieee 802.15.4 historical revolution versions: A survey. *Computing*, 103, 2021. doi:10.1007/s00607-020-00844-3.

[250] H. Harada, K. Mizutani, J. Fujiwara, K. Mochizuki, K. Obata, and R. Okumura. Ieee 802.15.4g based wi-sun communication systems. *IEICE Transactions on Communications*, E100B, 2017. doi:10.1587/transcom.2016SCI0002.

[251] Q. Wang and J. Jiang. Comparative examination on architecture and protocol of industrial wireless sensor network standards. *IEEE Communications Surveys and Tutorials*, 18, 2016. doi:10.1109/COMST.2016.2548360.

[252] J. Karaoğuz. High-rate wireless personal area networks. *IEEE Communications Magazine*, 39, 2001. doi:10.1109/35.968818.

[253] M. Mathiesen, G. Thonet, and N. Aakvaag. Wireless ad-hoc networks for industrial automation: Current trends and future prospects. In *IFAC Proceedings Volumes*, volume 16, 2005. doi:10.3182/20050703-6-cz-1902.01170.

[254] F. Chen, N. Wang, R. German, and F. Dressler. Performance evaluation of ieee 802.15.4 lr-wpan for industrial applications. In *2008 Fifth Annual Conference on Wireless on Demand Network Systems and Services*, 2008. doi:10.1109/WONS.2008.4459361.

[255] D. Egan. The emergence of zigbee in building automation and industrial controls. *Computing and Control Engineering*, 16:14–19, 4 2005. doi:10.1049/cce:20050203.

[256] J. Song, S. Han, A. K. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt. Wirelesshart: Applying wireless technology in real-time industrial process control. In *2008 IEEE Real-Time and Embedded Technology and Applications Symposium*, pages 377–386, 2008. doi:10.1109/RTAS.2008.15.

[257] ISA. Isa100 wireless compliance institute the technology behind the isa100.11a standard-an exploration. *Complete Guide Brochure*, 2017.

[258] T. Hasegawa, H. Hayashi, T. Kitai, and H. Sasajima. Industrial wireless standardization - scope and implementation of isa sp100 standard. *SICE Annual Conference 2011*, pages 2059–2064, 2011.

[259] L. E. Frenzel. *Handbook of Serial Communications Interfaces*. Elsevier, 2015. doi:10.1016/b978-0-12-800629-0.00077-2.

[260] T. P. Raptis, A. Passarella, and M. Conti. A survey on industrial internet with isa100 wireless. *IEEE Access*, 8, 2020. doi:10.1109/ACCESS.2020.3019665.

[261] M. Nixon. White paper: Comparison of wirelesshart and isa100.11a document title: A comparison of wirelesshart and isa100.11a a comparison of wirelesshart™ and isa100.11a title: A comparison of wirelesshart and isa100.11a. Technical report, Emerson, 2012.

[262] P. Sharma. Evolution of mobile wireless communication networks-1g to 5g as well as future prospective of next generation communication network. *International Journal of Computer Science and Mobile Computing (IJCSMC) - not index*, 2, 2013.

[263] M. Agiwal, A. Roy, and N. Saxena. Next generation 5g wireless networks: A comprehensive survey. In *IEEE Communications Surveys and Tutorials*, volume 18, 2016. doi:10.1109/COMST.2016.2532458.

[264] J. F. Monserrat, D. Martín-Sacristán, J. Cabrejas-Peñuelas, D. Calabuig, S. Garrigas, and N. Cardona. On the way towards fourth-generation mobile: 3gpp lte and lte-advanced. *Eurasip Journal on Wireless Communications and Networking*, 2009, 2009. doi:10.1155/2009/354089.

[265] V. Ilderem. The technology underpinning 5g. *Nature Electronics*, 3:5–6, 1 2020. doi:10.1038/s41928-019-0363-6.

[266] J. Agrawal, R. Patel, P. Mor, P. Dubey, and J. M. Keller. International journal of multidisciplinary and current research evolution of mobile communication network: from 1g to 4g. *J. of Multidisciplinary and Current Research*, 3, 2015.

[267] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli. 5g evolution: A view on 5g cellular technology beyond 3gpp release 15. *IEEE Access*, 7, 2019. doi:10.1109/ACCESS.2019.2939938.

[268] J. M. Chapin and W. H. Lehr. Mobile broadband growth, spectrum scarcity, and sustainable competition. In *TPRC*, pages 1–36, 2011.

[269] P. R. Newswire. The private lte and 5g network ecosystem: 2018 - 2030 - opportunities, challenges, strategies, industry verticals and forecasts. *LON-REPORTBUYER*, 2018.

[270] D. Rico and P. Merino. A survey of end-to-end solutions for reliable low-latency communications in 5g networks. *IEEE Access*, 8, 2020. doi:10.1109/ACCESS.2020.3032726.

[271] P. Marsch, S. E. E. Ayoubi, O. M. Boldi, T. I. Ö. Bulakci, P. Spapis, M. Schellmann, H. E. P. Marsch, M. Säily, T. Rosowski, G. Zimmermann, D. T. I. D. Silva, E. M. Tesanovic, M. Shariat, and S. M. A. Ibrahim. 5g ran architecture and functional design. *White Paper METIS II*, 2016.

[272] Cisco and Ericsson. Verizon 5g tf; network and signaling working group. Specification (release 1), Verizon 5th Generation Radio Access; 5G Medium Access Control Protocol (5G-MAC), 2016.

[273] M. Ehrlich, D. Krummacker, C. Fischer, R. Guillaume, S. S. P. Olaya, A. Frimpong, H. D. Meer, M. Wollschlaeger, H. D. Schotten, and J. Jasperneite. Software-defined networking as an enabler for future industrial network management. In *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation*, volume 2018-September. IEEE, 2018. doi:10.1109/ETFA.2018.8502561.

[274] G. P. Fettweis. 5g and the future of iot. In *ESSCIRC Conference 2016*, volume 42nd European Solid-State Circuits Conference, pages 21–24, 2016. doi:10.1109/ESSCIRC.2016.7598234.

[275] ITU-R. Imt vision – framework and overall objectives of the future development of imt for 2020 and beyond. Technical report, ITU, 2015.

[276] J. Ordonez-Lucena, J. F. Chavarria, L. M. Contreras, and A. Pastor. The use of 5g non-public networks to support industry 4.0 scenarios. In *2019 IEEE Conference on Standards for Communications and Networking, CSCN 2019*, 2019. doi:10.1109/CSCN.2019.8931325.

[277] J. Thota and A. Aijaz. Slicing-enabled private 4g/5g network for industrial wireless applications. In *MobiComm*, 2019. doi:10.1145/3372224.3417325.

[278] Z. Zhao. Research on 5g security technology for industrial internet. In *2021 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS)*, volume 1966, page 12044, 7 2021. doi:10.1088/1742-6596/1966/1/012044.

[279] Y. Siriwardhana, P. Porambage, M. Ylianttila, and M. Liyanage. Performance analysis of local 5g operator architectures for industrial internet. *IEEE Internet of Things Journal*, 7, 2020. doi:10.1109/JIOT.2020.3024875.

[280] D. Strametz, M. Reip, R. Pichler, C. Maasem, M. Höffernig, and M. Pichler. Increased agility by using autonomous agvs in reconfigurable factories. In *Advances in Automotive Production Technology – Theory and Application*, 2021. doi:10.1007/978-3-662-62962-8_50.

[281] N. Akkari and N. Dimitriou. Mobility management solutions for 5g networks: Architecture and services. In *Computer Networks*, volume 169. Springer, 2020. doi:10.1016/j.comnet.2019.107082.

[282] A. N. Kasim. A survey mobility management in 5g networks. *arXiv*, 2020.

[283] E. McCann. Wi-fi origins and history — mccann tech. URL `https://evanmccann.net/blog/wifi-101/origins-and-history`.

[284] J. P. D. Vries, L. Simić, A. Achtzehn, M. Petrova, and P. Mähönen. The wi-fi "congestion crisis": Regulatory criteria for assessing spectrum congestion claims. *Telecommunications Policy*, 38, 2014. doi:10.1016/j.telpol.2014.06.005.

[285] B. Dezfouli, V. Esmaeelzadeh, J. Sheth, and M. Radi. A review of software-defined wlans: Architectures and central control mechanisms. In *IEEE Communications Surveys and Tutorials*, volume 21, 2019. doi:10.1109/COMST.2018.2868692.

[286] G. Hardin. The tragedy of the commons. *Science*, 162, 1968. doi:10.1126/science.162.3859.1243.

[287] T. Ngo. Why wi-fi stinks - and how to fix it. *IEEE Spectrum*, 53:44–50, 7 2016. doi:10.1109/MSPEC.2016.7498159.

[288] Cisco. Cisco annual internet report (2018–2023). *Annual Internet Report*, 2020.

[289] C. OfCom. Appendix to spectrum management strategy. Technical report, OFCOM UK, 2020.

[290] L. Ward. Ieee 802.11ax technology introduction. *White paper IEEE 802.11ax technology introduction*, 2020.

[291] C. Hetting. The evolution of speed: Moore's law still applies to wi-fi - wi-fi now global. URL `https://wifinowglobal.com/news-and-blog/the-evolution-of-speed-moores-law-still-applies-to-wi-fi/`.

[292] M. J. Ho, M. S. Rawles, M. Vrijkorte, and L. Fei. Rf challenges for 2.4 and 5 ghz wlan deployment and design. In *2002 IEEE Wireless Communications and Networking Conference Record. WCNC 2002*, volume 2, 2002. doi:10.1109/WCNC.2002.993368.

[293] E. H. Ong, J. Kneckt, O. Alanen, Z. Chang, T. Huovinen, and T. Nihtila. Ieee 802.11ac: Enhancements for very high throughput wlans. In *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 849–853. IEEE, 9 2011. doi:10.1109/PIMRC.2011.6140087.

[294] A. F. Rochim and R. F. Sari. Performance comparison of ieee 802.11n and ieee 802.11ac. In *2016 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, 2017. doi:10.1109/IC3INA.2016.7863023.

[295] A. Z. Yonis. Performance analysis of ieee 802.11ac based wlan in wireless communication systems. *International Journal of Electrical and Computer Engineering (IJECE)*, 9, 2019. doi:10.11591/ijece.v9i2.pp1131-1136.

[296] M. Park. Ieee 802.11ac: Dynamic bandwidth channel access. In *2011 IEEE International Conference on Communications (ICC)*, volume 10, pages 821–828, 2011. doi:10.1109/icc.2011.5963089.

[297] O. Bejarano and E. W. Knightly. Ieee 802.11ac: From channelization to multi-user mimo. *IEEE Communications Magazine*, 51, 2013. doi:10.1109/MCOM.2013.6619570.

[298] A. B. Flores, R. E. Guerra, E. W. Knightly, P. Ecclesine, and S. Pandey. Ieee 802.11af: A standard for tv white space spectrum sharing. *IEEE Communications Magazine*, 51:92–100, 2013. doi:10.1109/MCOM.2013.6619571.

[299] D. Y. F. Pilapil and A. S. Banacia. Development and implentation of a tv white space geolocation database for ieee 802.11af system using the itu-r p.1411 recommendation. In *2019 2nd World Symposium on Communication Engineering (WSCE)*, 2019. doi:10.1109/WSCE49000.2019.9040961.

[300] Q. Zhao and B. M. Sadler. A survey of dynamic spectrum access. *IEEE Signal Processing Magazine*, 24(3):79–89, may 2007. doi:10.1109/MSP.2007.361604.

[301] V. Baños-Gonzalez, M. S. Afaqui, E. Lopez-Aguilera, and E. Garcia-Villegas. Ieee 802.11ah: A technology to face the iot challenge. *Sensors (Switzerland)*, 16, 2016. doi:10.3390/s16111960.

[302] T. L. Kao, H. C. Wang, C. H. Lu, and T. H. Cheng. An energy consumption evaluation of non-tim strategy in ieee 802.11ah. In *IOP Conference Series Materials Science and Engineering*, volume 644, 2019. doi:10.1088/1757-899X/644/1/012008.

[303] C. W. Park, D. Hwang, and T. J. Lee. Enhancement of ieee 802.11ah mac for m2m communications. *IEEE Communications Letters*, 18, 2014. doi:10.1109/LCOMM.2014.2323311.

[304] H. S. Kim, J. Ko, D. E. Culler, and J. Paek. Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey. In *IEEE Communications Surveys and Tutorial*, volume 19. IEE, 2017. doi:10.1109/COMST.2017.2751617.

[305] J. W. van Bloem, R. Schiphorst, T. Kluwer, and C. H. Slump. Spectrum utilization and congestion of ieee 802.11 networks in the 2.4 ghz ism band. *Journal of Green Engineering*, 2, 2012.

[306] T. Narytnik, P. G. Akopyan, V. Saiko, V. Korsun, and S. Sarapulov. Comparative characteristics of wireless systems of 802.11 standards for capacity and performance. *Visnyk Universytetu "Ukraina"*, 2019. doi:10.36994/2707-4110-2019-2-23-08.

[307] S. Joo, T. Kim, T. Song, and S. Pack. Mu-mimo enabled uplink ofdma mac protocol in dense ieee 802.11ax wlans. *ICT Express*, 6, 2020. doi:10.1016/j.icte.2020.04.007.

[308] K. Kawamura, A. Inoki, S. Nakayama, K. Wakao, and Y. Takatori. Coordinated scheduling of 802.11ax wireless lan systems using hierarchical clustering. *IEICE Transactions on Communications*, 2021. doi:10.1587/transcom.2019EBP3254.

[309] H. Kim and J. So. Improving spatial reuse of wireless lan uplink using bss color and proximity information. *Applied Sciences (Switzerland)*, 11, 2021. doi:10.3390/app112211074.

[310] N. Sepic, E. Kocan, Z. Veljovic, and M. Pejanovic. Assessment of novel solutions for throughput enhancement in ieee 802.11ax networks. In *2019 27th Telecommunications Forum (TELFOR)*, 2019. doi:10.1109/TELFOR48224.2019.8971156.

[311] H. Yin and S. Alamouti. Ofdma: A broadband wireless access technology. In *2006 IEEE Sarnoff Symposium*. IEEE, 2006. doi:10.1109/sarnof.2006.4534773.

[312] D.-J. Deng, Y.-P. Lin, X. Yang, J. Zhu, Y.-B. Li, J. Luo, and K.-C. Chen. Ieee 802.11ax: Highly efficient wlans for intelligent information infrastructure. *IEEE Communications Magazine*, 55:52–59, 2017. doi:10.1109/mcom.2017.1700285.

[313] C. Yang, W. Shen, and X. Wang. The internet of things in manufacturing: Key issues and potential applications. *IEEE Systems, Man, and Cybernetics Magazine*, 4:6–15, 2018. doi:10.1109/MSMC.2017.2702391.

[314] H. A. Alobaidy, M. J. Singh, M. Behjati, R. Nordin, and N. F. Abdullah. Wireless transmissions, propagation and channel modelling for iot technologies: Applications and challenges. *IEEE Access*, 10, 2022. doi:10.1109/ACCESS.2022.3151967.

[315] Q. Zhang, Q. Zhang, W. Zhang, F. Shen, T. H. Loh, and F. Qin. Understanding the temporal fading in wireless industrial networks: Measurements and analyses. In *2018 10th International Conference on Wireless Communications and Signal Processing (WCSP)*, pages 1–6. IEEE, 10 2018. doi:10.1109/WCSP.2018.8555681.

[316] W. Ning, Y. Wang, M. Liu, Y. Chen, and X. Wang. Mission-critical resource allocation with puncturing in industrial wireless networks under mixed services. *IEEE Access*, 9, 2021. doi:10.1109/ACCESS.2021.3056202.

[317] V. DIez, A. Arriola, I. Val, and M. Velez. Validation of rf communication systems for industry 4.0 through channel modeling and emulation. In *2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM)*, 2017. doi:10.1109/ECMSM.2017.7945906.

[318] L. Seno, S. Vitturi, and C. Zunino. Analysis of ethernet powerlink wireless extensions based on the ieee 802.11 wlan. *IEEE Transactions on Industrial Informatics*, 5, 2009. doi:10.1109/TII.2009.2019727.

[319] R. Bajracharya, R. Shrestha, and H. Jung. Future is unlicensed: Private 5g unlicensed network for connecting industries of future. In *Sensors (Switzerland)*, volume 20, 2020. doi:10.3390/s20102774.

[320] K. Sui, S. Sun, Y. Azzabi, X. Zhang, Y. Zhao, J. Wang, Z. Li, and D. Pei. Understanding the impact of ap density on wifi performance through real-world deployment. In *2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, 2016. doi:10.1109/lanman.2016.7548845.

[321] T. Pulkkinen, J. K. Nurminen, and P. Nurmi. Understanding wifi cross-technology interference detection in the real world. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, 2021. doi:10.1109/icdcs47774.2020.00061.

[322] A. M. Al-Samman, T. A. Rahman, T. Al-Hadhrami, A. Daho, M. H. D. N. Hindia, M. H. Azmi, K. Dimyati, and M. Alazab. Comparative study of indoor propagation model below and above 6 ghz for 5g wireless networks. *Electronics 2019*, 8:44, 2019. doi:10.3390/electronics8010044.

[323] S. Jaeckel, T. Heyn, N. Turay, L. Raschkowski, L. Thiele, R. Vuohtoniemi, M. Sonkki, V. Hovinen, F. Burkhardt, and P. Karunakaran. Industrial indoor measurements from 2-6 ghz for the 3gpp-nr and quadriga channel model. In *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, volume 2019-September, 2019. doi:10.1109/VTCFall.2019.8891356.

[324] R. Candell, M. Kashef, Y. Liu, K. B. Lee, and S. Foufou. Industrial wireless systems guidelines: Practical considerations and deployment life cycle. *IEEE Industrial Electronics Magazine*, 12, 2018. doi:10.1109/MIE.2018.2873820.

[325] Y. Zhou, H. Momose, S. Yasukawa, and M. Kim. Development of indoor device-free location estimation using commodity wifi device. In *2020 International Symposium on Antennas and Propagation (ISAP)*, 2021. doi:10.23919/ISAP47053.2021.9391207.

[326] E. Dahlman, S. Parkvall, and J. Sköld. *Channel Sounding*, chapter 8, pages 133–152. ScienceDirect, 2021. doi:10.1016/b978-0-12-822320-8.00008-8.

[327] S. Salous and R. Thomä. State of the art mobile radio channel sounding and data analysis. In *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)*, pages 1158–1160. IEEE, 2014.

[328] C. S. Park and S. Park. Implementation of a fast link rate adaptation algorithm for wlan systems. *Electronics (Switzerland)*, 10, 2021. doi:10.3390/electronics10010091.

[329] M. G. Mehrabi, A. G. Ulsoy, Y. Koren, and P. Heytler. Trends and perspectives in flexible and reconfigurable manufacturing systems. *Journal of Intelligent Manufacturing*, 13, 2002. doi:10.1023/A:1014536330551.

[330] ITU. *Multipath propagation and parameterization of its characteristics.* International Telecommunications Union, 2021.

[331] ETSI. Tr 138 901 - v14.0.0 - 5g; study on channel model for frequencies from 0.5 to 100 ghz (3gpp tr 38.901 version 14.0.0 release 14). *3Gpp*, 0, 2017.

[332] W. Wang, G. Wang, J. Zhang, and Y. Li. Robust weighted least squares method for toa-based localization under mixed los/nlos conditions. *IEEE Communications Letters*, 21, 2017. doi:10.1109/LCOMM.2017.2725274.

[333] D. Chizhik, J. Du, and R. A. Valenzuela. Universal path gain laws for common wireless communication environments. *IEEE Transactions on Antennas and Propagation*, 70:2928–2941, 4 2022. doi:10.1109/TAP.2021.3121173.

[334] V. Erceg, L. J. Greenstein, S. Y. Tjandra, S. R. Parkoff, A. Gupta, B. Kulic, A. A. Julius, and R. Bianchi. Empirically based path loss model for wireless channels in suburban environments. *IEEE Journal on Selected Areas in Communications*, 17, 1999. doi:10.1109/49.778178.

[335] T. K. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma. A survey of various propagation models for mobile communication. In *IEEE Antennas and Propagation Magazine*, volume 45, 2003. doi:10.1109/MAP.2003.1232163.

[336] S. Kurt and B. Tavli. Path-loss modeling for wireless sensor networks: A review of models and comparative evaluations. In *IEEE Antennas and Propagatio*, volume 59. IEEE, 2017. doi:10.1109/MAP.2016.2630035.

[337] A. Doukas and G. Kalivas. Rician k factor estimation for wireless communication systems. In *2006 International Conference on Wireless and Mobile Communications (ICWMC'06)*, 2006. doi:10.1109/ICWMC.2006.81.

[338] S. Mukherjee, S. S. Das, A. Chatterjee, and S. Chatterjee. Analytical calculation of rician k-factor for indoor wireless channel models. *IEEE Access*, 5, 2017. doi:10.1109/ACCESS.2017.2750722.

[339] I. Dolińska, M. Jakubowski, and A. Masiukiewicz. Interference comparison in wi-fi 2.4 ghz and 5 ghz bands. In *2017 International Conference on Information and Digital Technologies (IDT)*, pages 106–112, 2017.

[340] K.Nolan and M.Kelly. Ipv6 convergence for iot cyber-physical systems. *Information*, 9, 2018. doi:10.3390/info9040070.

[341] O. Givehchi, K. Landsdorf, P. Simoens, and A. W. Colombo. Interoperability for industrial cyber-physical systems: An approach for legacy systems. *IEEE Transactions on Industrial Informatics*, 13:3370–3378, 2017. doi:10.1109/TII.2017.2740434.

[342] R. Kabore, A. Kouassi, R. N'goran, O. Asseu, Y. Kermarrec, and P. Lenca. Review of anomaly detection systems in industrial control systems using deep feature learning approach. *Engineering*, 13:30–44, 2021. doi:10.4236/eng.2021.131003.

[343] M. R. Palattella, N. Accettura, L. A. Grieco, G. Boggia, M. Dohler, and T. Engel. On optimal scheduling in duty-cycled industrial iot applications using ieee802.15.4e tsch. *IEEE Sensors Journal*, 13:3655–3666, 10 2013. doi:10.1109/JSEN.2013.2266417.

[344] J. Kim, J. Lee, J. Kim, and J. Yun. M2m service platforms: Survey, issues, and enabling technologies. *IEEE Communications Surveys and TutorialsTutorials*, 16:61–76, 1 2014. doi:10.1109/SURV.2013.100713.00203.

[345] D. D. Guglielmo, G. Anastasi, and A. Seghetti. From ieee 802.15.4 to ieee 802.15.4e: A step towards the internet of things. *Advances in Intelligent Systems and Computing*, 260, 2014. doi:10.1007/978-3-319-03992-3_10.

[346] X. M. Zhang, Q. L. Han, X. Ge, D. Ding, L. Ding, D. Yue, and C. Peng. Networked control systems: A survey of trends and techniques. *IEEE/CAA Journal of Automatica Sinica*, 7, 2020. doi:10.1109/JAS.2019.1911651.

[347] E. Trunzer, T. Schilling, M. Müller, and B. Vogel-Heuser. Comparison of communication technologies for industrial middlewares and dds-based realization. In *21st IFAC World Congress*, volume 53, pages 10935–10942, 2020. doi:10.1016/j.ifacol.2020.12.2836.

[348] D. Bruckner, M. P. Stanica, R. Blair, S. Schriegel, S. Kehrer, M. Seewald, and T. Sauter. An introduction to opc ua tsn for industrial communication systems. *Proceedings of the IEEE*, 107, 2019. doi:10.1109/JPROC.2018.2888703.

[349] S. Cavalieri and F. Chiacchio. Analysis of opc ua performances. *Computer Standards and Interfaces*, 36, 2013. doi:10.1016/j.csi.2013.06.004.

[350] Ö. Köksal and B. Tekinerdogan. Obstacles in data distribution service middleware: A systematic review. *Future Generation Computer Systems*, 68, 2017. doi:10.1016/j.future.2016.09.020.

[351] E. Foundation. The eclipse foundation releases 2021 iot and edge developer survey results | eclipse news, eclipse in the news, eclipse announcement. URL `https://newsroom.eclipse.org/news/announcements/eclipse-foundation-releases-2021-iot-edge-developer-survey-results`.

[352] J. R. Koelsch. Why the mqtt protocol is so popular | automation world. URL `https://www.automationworld.com/factory/iiot/article/22080946/why-the-mqtt-protocol-is-so-popular`.

[353] P. Koprov, A. Ramachandran, Y.-S. Lee, P. Cohen, and B. Starly. Streaming machine generated data via the mqtt sparkplug b protocol for smart factory operations. *Manufacturing Letters*, 33:66–73, 2022. doi:10.1016/j.mfglet.2022.07.016.

[354] A. Morato, S. Vitturi, F. Tramarin, and A. Cenedese. Assessment of different opc ua implementations for industrial iot-based measurement applications. *IEEE Transactions on Instrumentation and Measurement*, 70:1–11, 2021. doi:10.1109/TIM.2020.3043116.

[355] J. Gascon-Samson, M. Rafiuzzaman, and K. Pattabiraman. Thingsjs: Towards a flexible and self-adaptable middleware for dynamic and heterogeneous iot environments. In T. V. Batista, S. Delbruel, D. Bermbach, D. M. Eyers, D. Hughes, C. Taconet, and E. Wittern, editors, *M4IoT 17: Proceedings of the 4th Workshop on Middleware and Applications for the Internet of Things*, pages 11–16. ACM, 2017. doi:10.1145/3152141.3152391.

[356] A. Sumaray and S. K. Makki. A comparison of data serialization formats for optimal efficiency on a mobile platform. In S.-H. Lee, L. Hanzo, R. Ismail, D. S. Kim, M. Y. Chung, and S.-W. Lee, editors, *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication*, pages 48:1–48:6. ACM, 2012. doi:10.1145/2184751.2184810.

[357] C. Pahl, A. Brogi, J. Soldani, and P. Jamshidi. Cloud container technologies: A state-of-the-art review. *IEEE Transactions on Cloud Computing*, 7(3):677–692, jul 2019. doi:10.1109/TCC.2017.2702586.

[358] P. Sharma, L. Chaufournier, P. Shenoy, and Y. C. Tay. Containers and virtual machines at scale: A comparative study. In *Middleware 16: Proceedings of the 17th International Middleware Conference*, 2016. doi:10.1145/2988336.2988337.

[359] G. Laput, Y. Zhang, and C. Harrison. Synthetic sensors: Towards general-purpose sensing. In *CHI 17: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 3986–3999. Association for Computing Machinery, 2017. doi:10.1145/3025453.3025773.

[360] G. M. B. Efi Safikou. Sensor fusion and inferential sensing for fault detection and isolation in uncertain systems. In *2021 5th International Conference on Control and Fault-Tolerant Systems (SysTol)*, pages 85–90, 2021.

[361] S. Rounaq and M. Iqbal. Vision, challenges and future perspectives of low constrained devices iot operating systems: A systematic mapping review. *European Journal of Engineering and Technology Research*, 5:107–115, 2020. doi:10.24018/ejers.2020.5.12.2284.

[362] A. K. Kalakanti, V. Sudhakaran, V. Raveendran, and N. Menon. A comprehensive evaluation of nosql datastores in the context of historians and sensor data analysis. In *2015 IEEE International Conference on Big Data (Big Data)*, 2015. doi:10.1109/BigData.2015.7363952.

[363] B. Chardin, J.-M. Lacombe, and J.-M. Petit. Data historians in the data management landscape. In R. O. Nambiar and M. Poess, editors, *Technology Conference on Performance Evaluation and Benchmarking*, volume 7755, pages 124–139. Springer, 2012. doi:10.1007/978-3-642-36727-4_9.

[364] T. chung Fu. A review on time series data mining. *Engineering Applications of Artificial Intelligence*, 24(1):164–181, 2011.

[365] A. Bader, O. Kopp, and M. Falkenthal. Survey and comparison of open source time series databases. In B. Mitschang, N. Ritter, H. Schwarz, M. Klettke, A. Thor, O. Kopp, and M. Wieland, editors, *Lecture Notes in Informatics (LNI)*, volume 266, pages 249–268. GI, 2017. URL `https://dl.gi.de/20.500.12116/922`.

[366] J. Mostafa, Wehbi, and A. Sara; Chilingaryan, Suren; Kopmann. Scits: A benchmark for time-series databases in scientific experiments and industrial internet of things. In *34th International Conference on Scientific and Statistical Database Management (*. Association for Computing Machinery (ACM), 2022.

[367] A. P. S. Di Martino, L. Fiadone, A. Riccabone, and V. N. Vitale. Industrial internet of things: Persistence for time series with nosql databases. In *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pages 340–345, 2019.

[368] S. K. Jensen, T. B. Pedersen, and C. Thomsen. Time series management systems: A survey. *IEEE Transactions on Knowledge and Data Engineering*, abs/1710.01077, 2017. doi:10.1109/tkde.2017.2740932.

[369] H. Adelsberger and F. Korner. Data modeling with idef1x. In *Information Management in Computer Integrated Manufacturing. Lecture Notes in Computer Science*, volume 973. Springer Berlin Heidelberg, 1995.

[370] T.Li, Y.Liu, Y.Tian, and S.Shen. A storage solution for massive iot data based on nosql. *Green Computing and Communications*, pages 50–57, nov 2012. doi:10.1109/GreenCom.2012.18.

[371] M. Zhao, A. Kumar, T. Ristaniemi, and P. H. J. Chong. Machine-to-machine communication and research challenges: A survey. *Wireless Personal Communications*, 97(3):3569–3585, aug 2017. doi:10.1007/s11277-017-4686-1.

[372] Y. Mehmood, N. Haider, M. Imran, A. Timm-Giel, and M. Guizani. M2m communications in 5g: State-of-the-art architecture, recent advances, and research challenges. *IEEE Communications Magazine*, 55(9):194–201, 2017. doi:10.1109/mcom.2017.1600559.

[373] K. Montgomery, R. Candell, Y. Liu, and M. Hany. Wireless user requirements for the factory workcell nist advanced manufacturing series 300-8 wireless user requirements for the factory workcell. Technical report, NIST, 2018.

[374] G. Brown, P. Analyst, and H. Reading. Ultra-reliable low-latency 5g for industrial automation. *Technol. Rep. Qualcomm*, 2:52065394, 2018.

[375] H. Panetto, M. Zdravkovic, R. Jardim-Goncalves, D. Romero, J. Cecil, and I. Mezgár. New perspectives for the future interoperable enterprise systems. *Computers in Industry*, 79:47–63, jun 2016. doi:10.1016/j.compind.2015.08.001.

[376] H. Mostafa and Y. I. Ismail. Highly-linear voltage-to-time converter (VTC) circuit for time-based analog-to-digital converters (t-ADCs). In *2013 IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS)*. IEEE, dec 2013. doi:10.1109/icecs.2013.6815376.

[377] Y. Li, H. Li, X. Wei, and B. Wen. Verification of self-synchronism of a nonlinear oscillatory system with double homodromy rotors. In *2015 IEEE International Conference on Mechatronics and Automation (ICMA)*. IEEE, aug 2015. doi:10.1109/icma.2015.7237778.

[378] R. Guillaume, C. Thierry, and P. Zielinski. Robust production plan with periodic order quantity under uncertain cumulative demands. In *2013 10th IEEE INTERNATIONAL CONFERENCE ON NETWORKING, SENSING AND CONTROL (ICNSC)*. IEEE, apr 2013. doi:10.1109/icnsc.2013.6548753.

[379] B. M. Ferreira, A. C. Matos, N. A. Cruz, and A. P. Moreira. Homing a robot with range-only measurements under unknown drifts. *Robotics and Autonomous Systems*, 67:3–13, may 2015. doi:10.1016/j.robot.2014.09.035.

[380] M. Alefari, A. M. F. Barahona, and K. Salonitis. Modelling manufacturing employees' performance based on a system dynamics approach. *Procedia CIRP*, 72:438–443, 2018. doi:10.1016/j.procir.2018.03.161.

[381] P. Leitão, A. W. Colombo, and S. Karnouskos. Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. *Computers in Industry*, 81:11–25, sep 2016. doi:10.1016/j.compind.2015.08.004.

[382] S. S. P. Olaya, S. Matzler, M. Wollschlaeger, P. Varutti, and T. Szczepanski. Reliable wireless control: Wireless connection in the control loop. In *2016 IEEE World Conference on Factory Communication Systems (WFCS)*. IEEE, may 2016. doi:10.1109/wfcs.2016.7496523.

[383] L.-S. Kuo, H.-H. Huang, C.-H. Yang, and P.-H. Chen. Real-time remote monitoring of temperature and humidity within a proton exchange membrane fuel cell using flexible sensors. *Sensors*, 11(9):8674–8684, sep 2011. doi:10.3390/s110908674.

[384] R. B. Sorensen, D. M. Kim, J. J. Nielsen, and P. Popovski. Analysis of latency and MAC-layer performance for class a LoRaWAN. *IEEE Wireless Communications Letters*, 6(5):566–569, oct 2017. doi:10.1109/lwc.2017.2716932.

[385] J. Stój, A.-L. Kampen, R. Cupek, I. Smołka, and M. Drewniak. Industrial shared wireless communication systems—use case of autonomous guided vehicles with collaborative robot. *Sensors*, 23(1):158, dec 2022. doi:10.3390/s23010158.

[386] M. Uddin, S. Mukherjee, M. Kodialam, and T. Lakshman. GLAMAR: Geo-location assisted mobile augmented reality for industrial automation. In *2020 IEEE/ACM Symposium on Edge Computing (SEC)*. IEEE, nov 2020. doi:10.1109/sec50012.2020.00036.

[387] I. S. for Automation. Isa tr100.00.03-2011 - wireless use requirements for factory automation. Technical report, International Society for Automation, 2011. URL `https://webstore.ansi.org/standards/isa/isatr10000032011`.

[388] OfCom. Wi-fi performance testing of home broadband routers. Technical report, UK regulator for the communications services, 2020.

[389] R. Bell. Introduction and revision of iec 61508. *Advances in Systems Safety*, pages 273–291, 2011. doi:10.1007/978-0-85729-133-2_16.

[390] R. Mackiewicz. Overview of iec 61850 and benefits. In *2006 IEEE PES Power Systems Conference and Exposition*, pages 623–630. IEEE, 2006. doi:10.1109/PSCE.2006.296392.

[391] SPE Intelligent Energy International Conference and Exhibition. *Wireless Instrumentation in the Oil and Gas Industry - From Monitoring to Control and Safety Applications*. one petro, 03 2012. doi:10.2118/150249-ms.

[392] Y. Liu, R. Candel, M. Kashef, and K. Montgomery. A collaborative work cell testbed for industrial wireless communications - the baseline design. In *2019 IEEE 28th International Symposium on Industrial Electronics (ISIE)*, volume 2019-June, 2019. doi:10.1109/ISIE.2019.8781524.

[393] T. P. Raptis, A. Passarella, and M. Conti. A survey on industrial internet with isa100 wireless. *IEEE Access*, 8, 2020. doi:10.1109/ACCESS.2020.3019665.

[394] F. Psarommatis, G. May, and V. Azamfirei. Envisioning maintenance 5.0: Insights from a systematic literature review of industry 4.0 and a proposed framework. *Journal of Manufacturing Systems*, 68:376–399, jun 2023. doi:10.1016/j.jmsy.2023.04.009.

[395] D. K. Baroroh, C.-H. Chu, and L. Wang. Systematic literature review on augmented reality in smart manufacturing: Collaboration between human and computational intelligence. *Journal of Manufacturing Systems*, 61:696–711, oct 2021. doi:10.1016/j.jmsy.2020.10.017.

[396] S. Dietrich, G. May, O. Wetter, H. Heeren, and G. Fohler. Performance indicators and use case analysis for wireless networks in factory automation. In *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation*, pages 1–8. IEEE, 9 2017. doi:10.1109/ETFA.2017.8247605.

[397] P. Milgrom. Wi-fi and the spectrum commons. In *Understanding Spectrum Liberalisation*, pages 134–145. CRC Press, aug 2015. doi:10.1201/b18830-14.

[398] X. Zhou, J. Ma, Y. Li, Y. H. Kwon, A. C. K. Soong, and G. Zhao. Probability-based transmit power control for dynamic spectrum access. In *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*. IEEE, oct 2008. doi:10.1109/dyspan.2008.89.

[399] X. Fernando, A. Sultana, S. Hussain, and L. Zhao. Relay-based cooperative spectrum sensing. In *SpringerBriefs in Electrical and Computer Engineering*, pages 19–39. Springer International Publishing, may 2018. doi:10.1007/978-3-319-73957-1_2.

[400] M. Ibnkahla. Spectrum sensing. In *Cooperative Cognitive Radio Networks*, pages 11–38. CRC Press, sep 2018. doi:10.1201/9781315215969-2.

[401] G. Naik and J.-M. J. Park. Impact of wi-fi transmissions on c-v2x performance. In *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, nov 2019. doi:10.1109/dyspan.2019.8935647.