
# IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

# Deliverable D7.2

# Report on the applicability of tools, methods and models related to connectivity issues in I4.0

The IoT4CPS Consortium:
AIT – Austrian Institute of Technology GmbH
AVL – AVL List GmbH
DUK – Donau-Universität Krems
IFAT – Infineon Technologies Austria AG
JKU – JK Universität Linz / Institute for Pervasive Computing
JR – Joanneum Research Forschungsgesellschaft mbH
NOKIA – Nokia Solutions and Networks Österreich GmbH
NXP – NXP Semiconductors Austria GmbH
SBA – SBA Research GmbH
SRFG – Salzburg Research Forschungsgesellschaft
SCCH – Software Competence Center Hagenberg GmbH
SAGÖ – Siemens AG Österreich
TTTech – TTTech Computertechnik AG
IAIK – TU Graz / Institute for Applied Information Processing and Communications
ITI – TU Graz / Institute for Technical Informatics
TUW – TU Wien / Institute of Computer Engineering
XNET – X-Net Services GmbH

*For more information on this document or the IoT4CPS project, please contact:*
Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at


Document Control

**Title: Report on the applicability of tools, methods and models related to connectivity issues in I4.0**

**Type:** Public
**Editor(s):** Christos Thomos
**E-mail:** Christos.Thomos@infineon.com
**Author(s):** Christos Thomos, Adeel Ahmed, Franz Dielacher, Stefan Marksteiner
**Doc ID:** D7.2

Amendment History

| Version | Date | Author | Description/Comments |
|---|---|---|---|
| V0.1 | 25.05.2020 | Christos Thomos | Document organization |
| V0.5 | 09.10.2020 | Christos Thomos, Adeel Ahmed, Franz Dielacher, Stefan Marksteiner | Initial Version |
| V0.8 | 15.10.2020 | Violeta Damjanovic-Behrendt | Internal Review |
| V1.0 | 30.10.2020 | Franz Dielacher | Final Version |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |



The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

# Content

List of Figures ..... 4

List of Tables ..... 4

Abbreviations ..... 5

Executive Summary ..... 7

1 Introduction ..... 8

2 Connectivity Technologies ..... 9

2.1 Wired connectivity ..... 11

2.2 Wireless Connectivity ..... 11

2.3 Secure Connectivity in wired and wireless communication ..... 14

3 IOT4CPS Demonstrators ..... 15

3.1 Device Connect (AVL) ..... 15

3.2 Virtual Factory (X-Net) ..... 16

3.3 Device Application for Wireless Industrial connectivity (Infineon) ..... 17

3.3.1 LoRaWAN Architecture ..... 17

3.3.2 LoRaWAN Secure connectivity ..... 18

3.3.3 LoRaWAN Mapping to the OSI layer ..... 19

3.3.4 Industrial use case ..... 19

4 Conclusion ..... 24

5 References ..... 25

Appendix A. Article to Read ..... 26

# List of Figures

Figure 1 Requirements of Industry 4.0. ..... 9
Figure 2 IIoT Network Architecture (Alcácer, 2019) ..... 10
Figure 3 IoT4CPS main I4.0 architecture ..... 15
Figure 4 Trustworthy wide-area connection of an automotive system using AVL Device.CONNECT™ ..... 15
Figure 5 IoT4CPS Overview SBI-Concept ..... 16
Figure 6 LoRaWAN Wireless connectivity architecture ..... 17
Figure 7 LoRaWAN Security Mechanism ..... 18
Figure 8 LoRaWAN association with the OSI Layer ..... 19
Figure 9 Infineon site layout with gateways placed at different points A, B, C, D, E across the site ..... 20
Figure 10 RSSI at Gateway: RSSI versus spreading factor for all testing positions (A, B, C, D, E) ..... 21
Figure 11 SNR at Gateway: The SNR varies proportionally to the spreading factor for all the points ..... 21
Figure 12 PER (Packet loss) evaluation based on CR: 1-4 at different SF´s and points ..... 22

# List of Tables

Table 1 Wireless protocols comparison ..... 12
Table 2 Secure Communication Requirements (Zou, 2016) ..... 12
Table 3 Identification of Attacks and Measures for secure connectivity in wired / wireless communication ..... 14
Table 4 Testing Parameters for LoRaWAN ..... 20
Table 5 Advantages and Disadvantages of LoRaWAN Parameters ..... 22

## Abbreviations

| | |
|---|---|
| ABP | Activation by Personalization |
| ALOHA | Additive Links Online Hawaii Area |
| AP | Access Point |
| ARAN | Authentic Routing for Ad-hoc Networks |
| CPS | Cyber-physical system |
| CAN | Controller area network |
| CR | Coding Rates |
| dBm | Decibels per milliwatt |
| DCS | Distributed Control System |
| DOS | Denial of Service |
| EMI | Electromagnetic Interference |
| FEC | Forward Error Correction |
| HSMs | Hardware security modules |
| IEEE | Institute of Electrical and Electronics Engineers |
| IIoT | Industrial Internet of Things |
| IoT | Internet of things |
| IoT4CPS | Trustworthy internet of things for Cyber-physical systems |
| IP | Internet Protocol |
| I4.0 | Industry 4.0 |
| LoRa | Long Range Wide Area |
| LPWAN | Low Power Wide Area Network |
| MAC | Media Access Control |
| MIMO | Multiple Input, Multiple Output |
| MIC | Message integrity code |
| MTC | Machine-Type-Communication |
| M2M | Machine-to-Machine |
| MV | Megavolt |
| NB-IoT | Narrowband internet of things |
| OBD-II | On-board diagnostic |
| OPC-UA | Open Platform Communication - Unified Architecture |
| OSI | Open System Interconnection |
| OTAA | Over-The-Air-Activation |
| PER | Packet Error Rate |
| PLC | Programmable logic controller |
| P2P | Peer-to-peer communication |
| RSSI | Received Signal Strength Indicator |
| SBI | Security By Isolation |
| SCADA | Supervisory Control and Data Acquisition |
| SF | Spreading Factor |
| SNR | Signal-to-Noise Ratio |
| SSID | Service Set Identifier |
| TCP | Transmission Control Protocol |
| TEDS | Time-slotted Event-Driven Stack |
| TSN | Time-Sensitive Network |

| | |
|---|---|
| VPN | Virtual Private Network |
| V2X | Vehicle to everything |

## Executive Summary

This deliverable describes the applicability of tools, methods and models related to connectivity issues in Industry 4.0. It discusses challenges and limitation on the application of wired and wireless communication technologies for secure connectivity in smart manufacturing environments. The main IoT4CPS connectivity demonstrators that include AVL´s Device Connect, X-Net Virtual Factory and Infineon´s Device Application for Wireless Industrial Connectivity are presented.

# 1 Introduction

Industry 4.0 is a digital transformation of production that involves Information Technology (IT) to enable smart decentralized and autonomous systems in a cyber-physical environment (Armendia, 2019). This highly dependable industrial ecosystem requires advanced solutions for security, safety, resilience to failures and reliability to respond to the future connectivity issues. The addition of portable devices, modern sensors, and actuators for remote control, monitoring and maintenance in an industrial environment aiming to support the Industry 4.0 characteristics and capabilities, has raised the requirements for industrial connectivity. Within this concept and depending on the usage scenarios, the advancement from a limited wired communication network, w.r.t. installation flexibility and system maintainability, to a wireless connectivity platform offering the required mobility, scalability and coverage is imperative. This deliverable shows the implementation and evaluation of secure connectivity use-cases in real smart production environments with different sensors, tools and machinery. Also, the challenges and current status for secure connectivity solutions into a smart industrial environment are analysed in this report.

# 2 Connectivity Technologies

The reference models RAMI 4.0 (RAMI4.0, 2015) and IIRA (IIRA17, 2017) act as building blocks for industrial communication that is complying with the Industry 4.0 (I4.0 ) standard. Industrial communications is a mixture of Fieldbus systems, Ethernet-based approaches, and wireless solutions (Wollschlaeger, 2017). A hybrid approach bringing coherence to these wired/wireless communication methods is required to achieve the key requirements set by the I4.0 standard. Figure 1 describes the key requirements set forth by the I4.0 standard for industrial communication.

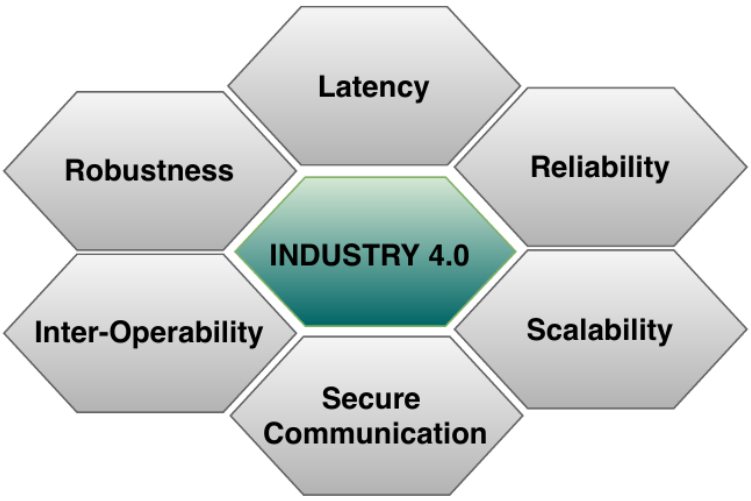


**Figure 1 Requirements of Industry 4.0.**

The requirements of IoT-based applications depend upon the type of environment that they are designed to operate in. For example, the requirements for a consumer-based IoT scenario such as home automation can tolerate a certain degree of freedom and flexibility. The mission-critical IoT applications that include manufacturing, healthcare, industrial and automotive sector pose stringent requirements, as any failure can be catastrophic in such an operating environment. Industrial automation comes under the mission-critical application world that has to comply with the Industry 4.0 standard. The main requirements of such applications include (Varghese, 2014.):

- Robust performance to withstand harsh remote environments,
- Low-latency for real-time communication,
- High-reliability for the devices to operate for a long time,
- Scalability to support large networks with many controllers,
- Interoperability to ensure operation of legacy and new devices and secure communication to end-point devices.

The wired and wireless connectivity of the IIoT scenario is shown in Figure 2.

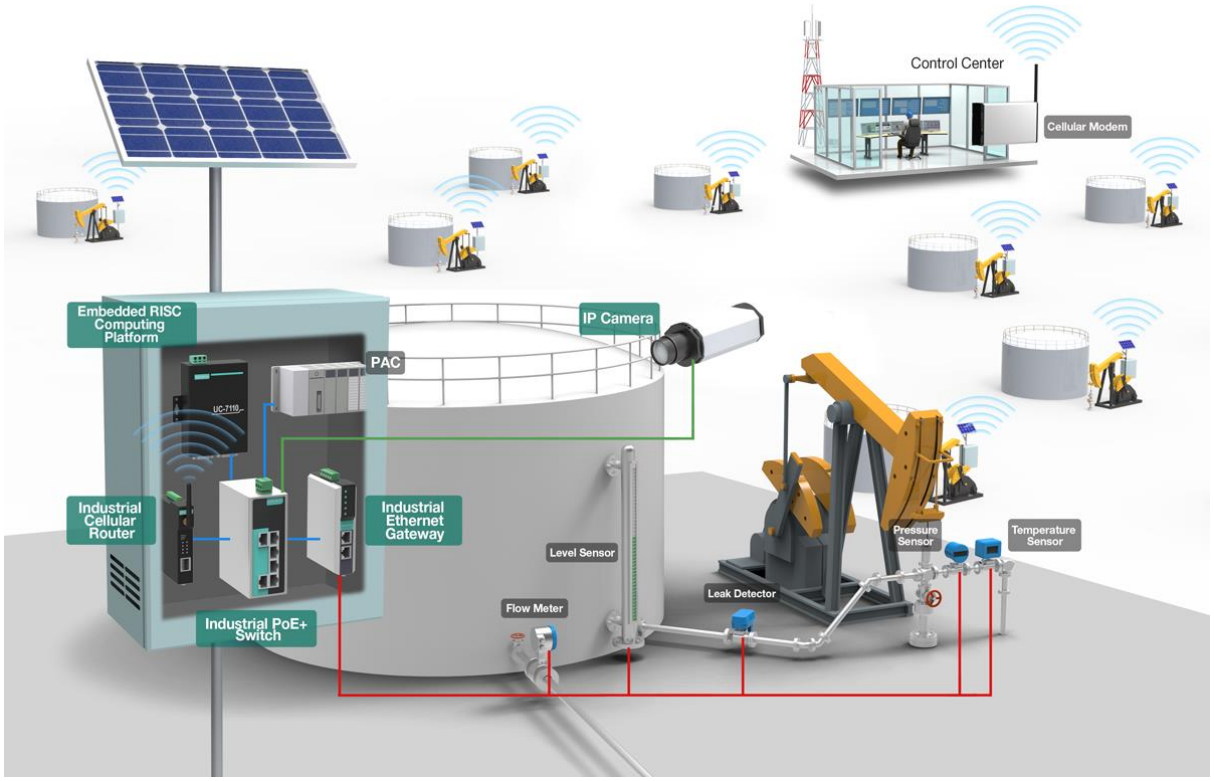


**Figure 2** IIoT Network Architecture **(Alcácer, 2019)**

A typical IIoT network is reliant on the structure of Machine-to-Machine communication (M2M) technology (Gilchrist, 2016). It consists of wired/wireless industrial sensors (pressure, temperature), flow meter, leak detector, level sensors at the field level connected to system-level industrial gateways, routers and switches. The sensors can be either wired or wirelessly connected to either the gateways or switches that forward the data to the application level. The application level is at the control centre comprising servers and SCADA systems to view, monitor, control and manage the data received from the system level. The data can also be forwarded to authorized clients through application layer protocols. Typically, Distributed Control System (DCS) or Programmable Logic Controller (PLC) units provide bi-directional communication between the application and the field level through the system level. The control centre can access multiple industries and is flexible to be situated outside of the industrial environment.

The present concept of Industry 4.0 is being adopted by many industries to optimize and improve the manufacturing and production scenarios. For this, there is a need to try and comply with the requirements set by Industry 4.0 and fill the gaps in the present-day industrial standards. Wired communications have been traditionally used for critical process control applications but the portability and maintainability are certain drawbacks of the entire system. The advent of wireless technologies in industrial automation has revolutionized the connectivity methods but is still in a development phase to cater to the requirements stated in Figure 1. The below section describes the wired and wireless connectivity methods for operation in an industrial environment.

### 2.1 Wired connectivity

The traditional Industrial communication is mostly wired with the usage of reliable protocols such as PROFINET, EtherNet/IP, CC-Link IE (Mahmood, 2019). These protocols provide M2M communication between machines in real-time. The M2M communication can often lead to protocol incompatibility, as the machines can be protocol- or vendor-specific and that leads to a concept called *manufacturer lock-in*. This prevents a machine operating on a different protocol to communicate with another machine, becomes vendor-specific, and leads to integration issues in networked systems. The usage of different protocols in different machines leads to the requirement of a universal protocol at the integration level to ease the communication of machines.

Various wired protocols used currently for communication are UART, CAN-Bus, RS-232, Ethernet. The applicability of the protocols depends on the overall compatibility of applications. For example, as discussed in the deliverable D7.1, the AVL demonstrator (Device-Connect) uses CAN bus and Ethernet for the communication. The Industry 4.0 requirement of interoperability has led to the emergence of a universal protocol in 2008, namely OPC-UA (Open Platform Communication - Unified Architecture) standard. It is based on a service-oriented architecture and integrates the communication protocols to a standard framework and caters to the goals of *Platform independence, Security and Functional equivalence* (OPC, 2020).

Ethernet is the most reliable wired communication method used to date. It offers speeds up to 10 Gbps and is frequently used to support process control applications with minimum delay. An enhanced version of the Ethernet used in Industrial scenarios is the Time-Sensitive Network (TSN). By bringing industrial-grade robustness and reliability to Ethernet, TSN offers an IEEE standard communication technology that enables deterministic communications for industrial applications (Cheruvu, 2020). Ethernet TSN communicates on the network layer through TCP/IP communication and thus eradicates the protocol dependency. It provides compatibility with Ethernet and can easily be integrated into existing technologies. Higher layer protocols can be combined with TSN, as the technology is implemented primarily at the data link layer (OSI model layer 2).

### 2.2 Wireless Connectivity

Wireless architecture (Radio connectivity) has revolutionized Industrial connectivity by providing remote equipment connection over long distances, reduced wire installation costs thus providing ease of mobility and portability within the industry. With the advent of 5G and its characteristics of fulfilling the requirements of an I4.0 environment, the usage of wireless networks is on a rise. Wireless protocols like Wireless HART (D. Chen, 2010), LoRa (Gambi E. e., 2018), IEEE 802.15.4 (Xiao, 2006) are currently used for communication inside the industries. Table 1 presents an overview regarding the parameters such as frequency, data rate, communication range, power consumption for different protocols.

**Table 1** Wireless protocols comparison

| Protocols | Frequency | Data Rate (kbps) | Range | Power Consumption |
|---|---|---|---|---|
| BLE | 2.4 GHz | 305 | 100 m | Low |
| WiFi | 2.4 / 5 GHz | 600 k | 500 m | Medium |
| IEEE 802.15.4 | 2.4 GHz | 250 | 500 m | Low |
| Zigbee | 2.4 GHz | 250 | 300 m – 1 km | 10-100 mW |
| Wireless HART | 2.4 GHz | 250 | 300 feet | Medium |
| LoRaWAN | 868 / 915 MHz | 50 | 1-3 kms | Low |
| SigFox | 868 / 902 MHz | 140 | 3- 10 kms | Low |
| NB-IoT | 180 kHz | 200 | 1-8 kms | Low |
| LTE-M | 1.4 MHz | 1000 k | 2.5-5 kms | Low |

Security in wireless devices poses a major concern with wireless network vulnerabilities like signal propagation in transit and component accessibility. The wireless topology requires secure communication at every path of data propagation: Access points (AP), radio NIC, routers, repeaters and antennas. Ad-hoc networks that provide peer-to-peer communication (P2P) directly between devices without the need for an access point have Authentic Routing for Ad-hoc Networks (ARAN) as an authentication based routing protocol to provide security between ad-hoc devices. MAC spoofing is a form of threat wherein the attacker has access to the MAC address of the authenticated device and tries to intrude the network through it. An AP can also be compromised by intruding through its Service Set Identifier (SSID). These type of attacks are prevented by broadcasting the Address Resolution Protocol (ARP) table to recognize the rouge MAC addresses not available in the table. In the OSI model, every layer requires a different type of security methodology to counter the threats.

Authenticity, Confidentiality, Integrity and Availability of data are the main benchmarks requirements for secure connectivity. Table 2 gives an overview of the requirements of the four main parameters of secure connectivity.

**Table 2** Secure Communication Requirements **(Zou, 2016)**

| Security | Authentication | Confidentiality | Integrity | Availability |
|---|---|---|---|---|
| Attacks | Unauthorized users.<br>MAC address authentication. | Key Encryption.<br>Data confidentiality. | Compromised Node (Access points).<br>Malicious information. | Denial of Service (DOS) attack.<br>Jamming attack. |
| Measures | Authentication at all layers. | Physical layer security.<br>Encryption algorithms. | Code update and recovery. | Spread spectrum techniques (DSSS, FHSS). |

**Massive broadband communications:** provide large-capacity communication access to any place and any time.

**Massive Machine Type communications:** is a communication paradigm where several devices or 'things' are attached to the Internet or directly connected and communicate with each other with little or without human intervention.

**Critical machine type communications:** represents automated data communication among devices and transportation infrastructure. Communication is possible between two Machine-Type-Communication (MTC) devices or with the server. Critical machine type communication is confronted with different issues, which need enhanced flexibility, coverage, capacity, security, data rate and low latency.

Industrial automation currently uses unlicensed frequency bands of 488 MHz, 868/915 MHz and 2.4 GHz for wireless applications (Gidlund, 2017). The major challenges in implementing 5G in the industrial environment involve having an infrastructure that requires a licensed frequency spectrum. This is mainly because the interference is less than that of an unlicensed band suiting the 5G requirements of reliability, availability and latency. Industrial environments possess hindrances like Electromagnetic Interference (EMI) that impact the wireless signals. Large industrial plants ranging a few kilometres can also make the distance a major factor for wireless usages. Latencies less than 1ms as specified by 5G standards is pragmatically stringent to achieve since the transmission and device losses have to be taken into consideration. Reliability and availability of all components is a critical requirement for factory automation that comes at cost expenses.

With device connectivity increasing exponentially with time, 5G technology requires secure connectivity across all the devices. Deployment of a large number of antennas in 5G systems and beamforming techniques can be utilized to improve the transmission performance to many users, by degrading the reception qualities of eavesdroppers (Zou, 2016). However, the application of massive Multiple Input, Multiple Output (MIMOs) for enhancing the physical-layer security brings challenges such as the deleterious effects of pilot contamination, power allocation, and channel reciprocity (Zou, 2016).

The technological advancements of 5G technologies allow its implementation in industrial environments to achieve high throughput, with a certain relaxation on the latency and reliability parameters. Industrial automation is a rather conservative domain, and the higher reliability of wired networks often outweighs the flexibility of wireless links (Wollschlaeger, 2017).

### 2.3 Secure Connectivity in wired and wireless communication

In the OSI model, every layer requires a different type of security methodology to counter the threats. Table 3 gives a comparative analysis of the attacks and measures concerning wired and wireless communication.

**Table 3** Identification of Attacks and Measures for secure connectivity in wired / wireless communication

| OSI Layers | Security | Wired comm. | Wireless comm. |
|---|---|---|---|
| **Application** | Measures | Authentication methods, Antivirus software, Firewalls. | |
| | Attacks | Malware attacks, SQL injection into websites, Cross-scripting attacks. | |
| **Transport** | Measures | Increasing TCP backlog and UDP response rate. | |
| | Attacks | TCP/UDP flooding by a large number of ping requests to congest the network. | |
| **Network** | Measures | Routers configured not to constantly respond to ICMP requests. | |
| | Attacks | IP Spoofing, Smurf attack (Network flooding with ICMP control messages). | |
| **MAC** | Measures | ARP tables to prevent unauthorized use.<br>Additional overhead security to prevent duplicating headers. | Using ARP table to identify false MAC addresses.<br>Use of Virtual private networks (VPN). |
| | Attacks | Intrusion into the system through MAC Spoofing.<br>Denial of Service (DOS) attacks by injecting MAC headers. | MAC Spoofing and Identity theft.<br>Man-In-The-Middle attacks. |
| **Physical** | Measures | Physical protection of wires, cables.<br>Encryption schemes like RSA, ECC between end nodes. | Improving Channel capacity of the main link to avoid eavesdropping.<br>Spread spectrum techniques like DSSS. |
| | Attacks | Attacks on physical links connecting devices.<br>Bit manipulation by accessing the data in transit. | Eavesdropping by malicious attackers.<br>Jamming by interference signals. |

Both wired and wireless networks share common protocols at the application, transport, and network layer and thus can be exposed to the same security attacks, requiring same control measures. The broadcast nature of a signal differentiates the form of attacks and measures in wired and wireless networks at the physical and MAC layers.

Wired and wireless networks need to adhere to certain security requirements to sustain attacks like Denial of Service (DOS), eavesdropping, jamming and spoofing.

# 3 IOT4CPS Demonstrators

This section contains the description of IoT4CPS's demonstrators and their architectures and includes contributions from partners participating in the WP7 demo, as shown in Figure 3. The following presentation aims to be a map of technologies that are necessary to achieve the objectives of the IoT4CPS project. The final demo will include additional contributions.

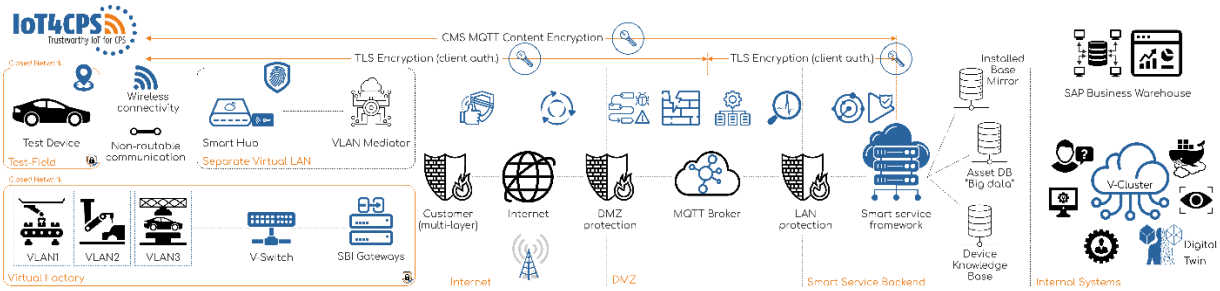


**Figure 3** IoT4CPS main I4.0 architecture

## 3.1 Device Connect (AVL)

AVL´s Device.Connect technology allows for trustworthy CAN communications over wide-area connections. Its architecture includes a component inside the vehicle (Smart Hub), which provides a secure connection by accepting a restricted set of commands. For outside connections, the Smart Hub acts as a subscriber to a message broker, which is the host of a publishing service. The remote station is posed by a backend system, which also subscribes to the broker. A state-of-the-art TLS connection enables a secure connection to the broker. Hardware Security Modules (HSMs) provide secure private keys for the devices. The security is enhanced from the network side by having the broker only single ports opened to allow inbound connections for the Smart Hub and backend. To prevent a compromised broker jeopardizing the overall system´s security, end-to-end content encryption is imposed. Linking the Smart Hub to a vehicle works via the vehicle´s on-board diagnostics (OBD-II) interface. The Smart Hub subsequently connects to a GUI in the backend and shows signals such as speed or the position of the braking pedal. Due to the bidirectional character of the channel, it is possible to flash and calibrate the vehicle. Moreover, a real-time stream of 99% of an IVNs CAN message enables remote vehicle maintenance. The architecture of Device.Connect is shown in Figure 4:

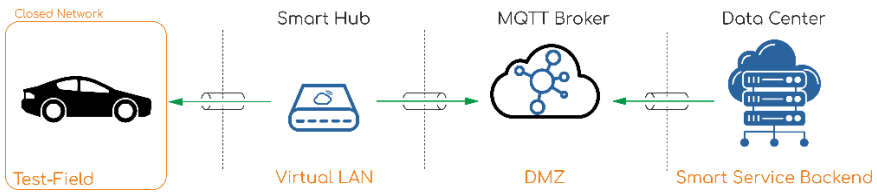


**Figure 4** Trustworthy wide-area connection of an automotive system using AVL Device.CONNECT™

### 3.2 Virtual Factory (X-Net)

X-Net developed the SBI-Box (Security By Isolation (SBI)) considering requirements for increased security within the industry, e.g. fast and uncomplicated integration of components, easy maintenance and update of the system or global decentralized commissioning. The SBI-Box consists of its private cloud system (SBI-Cloud) and includes several entry points (HUBs) and an administration system. It is possible to outsource the HUBs to company-specific servers or servers in the data centres. The developed SBI-Box allows expansion of the system at any time during operation.

The administration system configures, monitors and updates centrally all connections to the SBI-Cloud. Accesses are recorded and encrypted. Due to the Open Source components, no additional administration costs need to be considered. SBI-Boxes allow redundant and different configurations, such as 5G. The gateways can host different virtual machines and be integrated into the environment via virtual networks. For remote access and secure connections, a validate certificate, Open Source VPN client and a web browser are needed.

The future aim for the SBI-Box is to develop an open source-based industrial product. Major areas of interest are the integration of different hardware components and user-friendliness. Consequently, the security standard and affordability of the product can be enhanced. Concrete systems for possible further improvement include 5G or LoRa. The main focus is to ensure a secure connection while protecting the SBI-Box itself by using quantum encryption system. Figure 5 gives an overview of the SBI-Box concept, including SBI-Core, SBI-Hubs and the coordinating technicians.

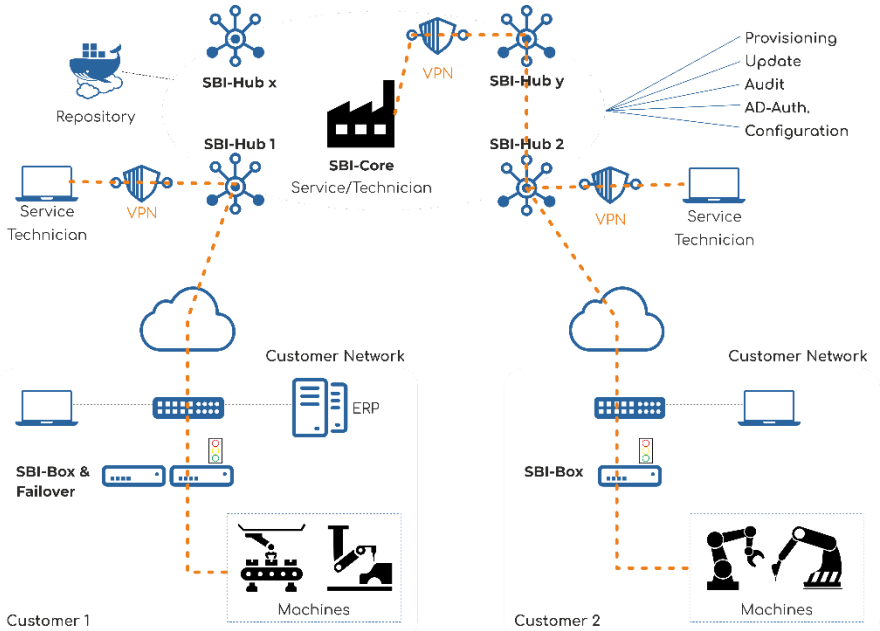


**Figure 5** IoT4CPS Overview SBI-Concept

## 3.3 Device Application for Wireless Industrial connectivity (Infineon)

The following sections give an overview of the Device Application for Wireless Industrial connectivity. Further details about Infineon's smart production use-case can be found in (Ahmed, 2020).

### 3.3.1 LoRaWAN Architecture

The chosen fabrication unit is Infineons Pilot Room Industry 4.0, used for ion implantation. In addition to production, this unit serves for testing new communication and information technologies under real conditions. The reason for choosing this testing environment was its extremely disturbing environment because of voltages up to 5MV, magnet fields up to 15kGauss and high-frequency electromagnetic fields. The implemented LoRaWAN architecture is an unlicensed LPWAN technology, which is considered as the dominant technology for deployment in large scale IoT applications. It provides a range of up to 5 km under best conditions. LoRa Alliance and other research confirmed that the network can cover an area of 34.000m$^2$ (LoRaAlliance, 2020). Indoor performance testing showed that LoRa is resistant to multi-path and signal fading (Ayele, 2017), (Tessaro, 2018). However, the duty-cycle limitations restrict the network scalability (Mikhaylov, 2016), (Augustin, 2016). The LoRaWAN architecture in the fabrication unit is implemented for long-range communication of the external sensors for monitoring and controlling of the manufacturing process from various clients. The ease of installation and maintenance provides a significant advantage over wired communication for such long distances. Figure 6 shows the architecture implemented in the fabrication unit.

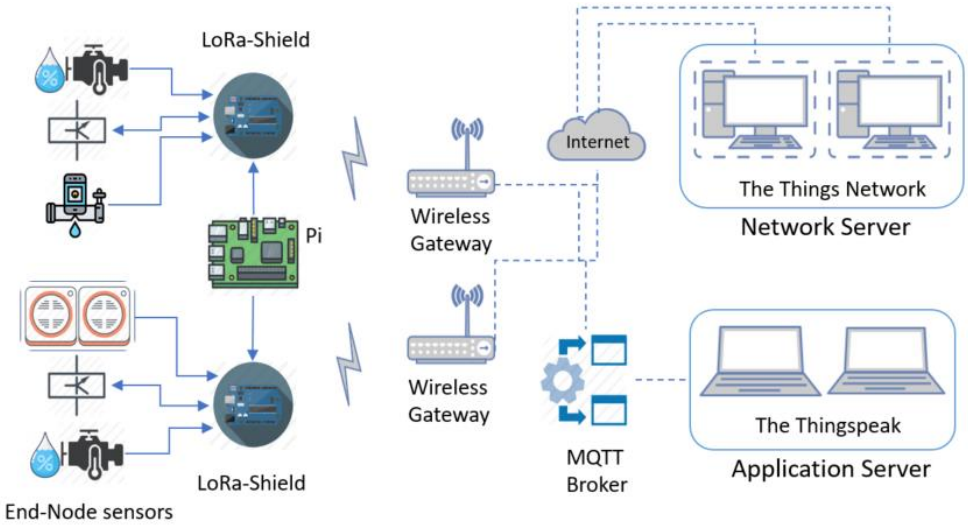


**Figure 6** LoRaWAN Wireless connectivity architecture

The end-nodes are the external sensors (temperature sensors, humidity sensors, leak detectors, relays) placed on the pipe-systems to monitor and control the flow of gases and liquids. They can be connected either wired or wirelessly. The sensors are connected to an Arduino-Uno LoRa shield transceiver with an integrated +20 dBm power amplifier for optimum transmission. The transceiver has a high 3rd order intercept point (IIP3) of -12.5 dBm that makes it robust against interfering signals in the same frequency region. The Raspberry Pi acts as the main controller that implements the control logic of the sensors and is also used for debugging. It is connected to the Arduino board using a serial USB and can be placed close to the LoRa-shields.

The transceiver transmits the wireless signals that are received by the LG-01 Dragino gateway and LoRa GPS-HAT (wireless gateways) placed at different locations. The Dragino gateway used for the implementation purposes is a single-channel LoRa gateway. The gateway bridges the wireless network to an IP network through cellular, Wi-Fi or other communication. The network server used for accumulating the sensor data is *The Things Network* and the application server used to distribute the data to various clients *The Thingspeak*.

### 3.3.2 LoRaWAN Secure connectivity

The LoRaWAN solution provides secure communication with Authentication and Encryption based on the AES-128 scheme (You, 2018) that is provided by two separate keys in the protocol. The authentication is provided by a Network session key NwkSKey and the user payload is encrypted by the Application session key AppSKey. The two authentication methods provided by the protocol are Over-The-Air-Activation (OTAA) and Activation by Personalization (ABP).

**Over-The-Air-Activation:** The devices are connected over-the-air to the network server through a Join procedure by exchanging the NwkSKey and AppSKey. The Join request/Join accept procedure has to take place securely for key exchange mechanism.

**Activation-By-Personalization:** The session keys, NwkSKey and AppSKey are pre-provisioned in the device along with the 32-bit Device Address (DevAddr). Securing key storage is the most critical aspect of this type of activation.

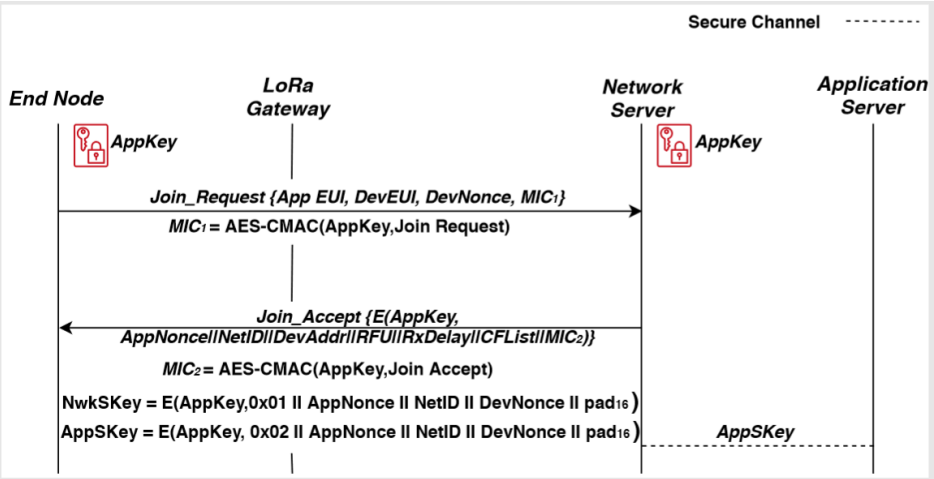


**Figure 7** LoRaWAN Security Mechanism

The join procedure is described in Figure 7. The *NwkSKey* and *AppSKey* are obtained by AES-128 encryption between the Network IDs and App Key. The end device computes a message integrity code (MIC) by AES-CMAC (Cipher-based message authentication code) along with an *AppKey* and this is sent along with a *Join_Request* initiated by the device. The network server authenticates the received request and computes a MIC to be sent along an encrypted *AppKey* with the *Join_Accept* message. The session keys, *NwkSKey* and *AppSKey* are generated as described in (You, 2018).

Join Accept message contains: a random AppNonce (3 octets), Network Identifier-NetID (3 octets), an end-node address-DevAddr (4 octets), a delay RxDelay between Tx and Rx (1 octet),

DL configuration parameters DLSettings (1 octet) and optional channel frequency list CFList (Ertürk, 2019). The network server forwards the AppSKey to the application server and the *AppSKey* is shared between the device and the network server after the *Join_Accept* message is communicated to the device.

### 3.3.3 LoRaWAN Mapping to the OSI layer

Figure 8 shows the mapping of the LoRaWAN layers to the OSI model.

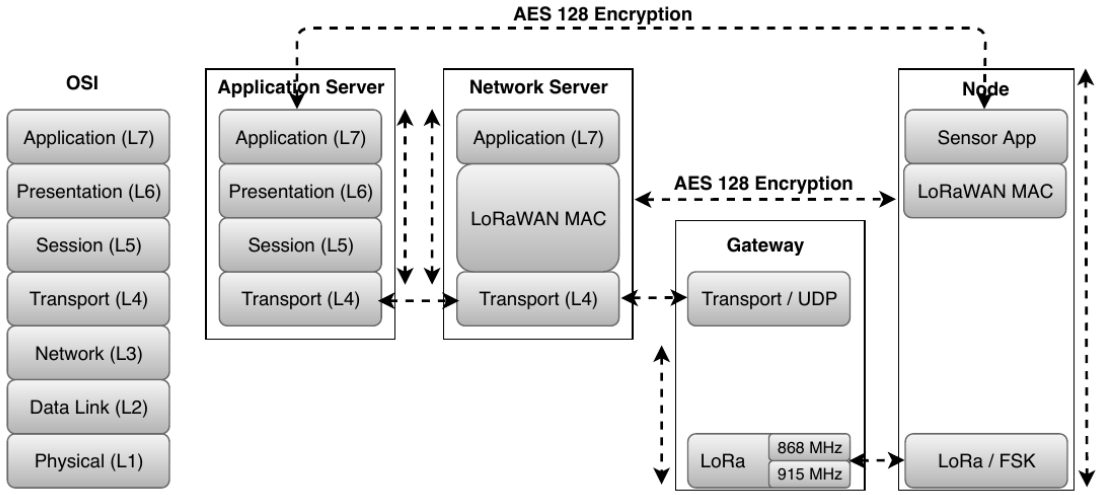


**Figure 8** LoRaWAN association with the OSI Layer

LoRa works on the physical layer of the OSI (L1) and modulates the signal to be sent over to the higher layers. LoRaWAN is a media access control (MAC) layer protocol (L2) built on top of LoRa that defines the access functions and end-node management (Ertürk, 2019). The OSI's network layer (L3) interfaces device addresses to the selected gateways. The OSI's transport layer (L4) manages the secure communication mechanism between the gateway and the network server by providing a session based on OTAA/ABP activation. The application layer (L7) connects the data to the end clients that can be monitored and controlled through an API.

### 3.3.4 Industrial use case

The measurement set-up was installed in Infineons Pilot Room Industry 4.0, a fabrication unit for ion implantation and technology testing with an extremely harsh environment, as described in Section 3.3.1. For the measurement, gateways were placed at five different points and the end nodes were arranged at a fixed location near to external sensors in the Pilot Room Industry 4.0. During the measurement, the distance between end-nodes and gateways was changed to evaluate connectivity features. The maximum distance reached about 0.5 km. Also, the position of the end-notes and gateways was minimum 1.5 to 2 meters above the ground to ensure a better signal-receiving.

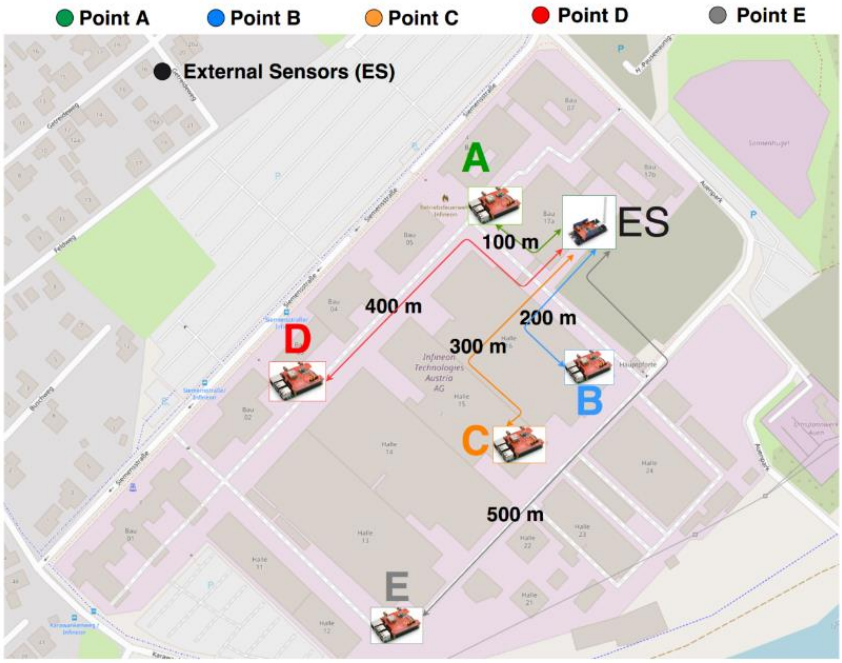


**Figure 9** Infineon site layout with gateways placed at different points A, B, C, D, E across the site

Figure 9 shows an overview of the Infineon site and the five different measurement points with various distances. Point A is near to the end-nodes and heavy machinery inside the fabrication building. Point B is similar to a greater distance to the heavy machinery, and Point C is placed on the other side of the fabrication building with a distance of about 300 m from the end nodes. Point D is located in an office with a distance of 400 m and Point E is outside at the ending of the Infineon site (500 m). The gateways were placed on these points to evaluate connectivity features based on different parameters such as Frequency, Channel Bandwidth, Coding Rate, Spreading Factor, Payload length and Transmission power (Table 4).

**Table 4** Testing Parameters for LoRaWAN

| Parameters | Values |
|---|---|
| Frequency ($f$) | 868.1 MHz |
| Channel Bandwidth ($BW$) | 125 KHz |
| Coding Rate ($CR$) | 1, 2, 3, 4 |
| Spreading Factor ($SF$) | 7, 8, 9, 10, 11, 12 |
| Payload length ($L$) | 26 bytes |
| Transmission power ($T_x$) | 14 dBm (25 mW) |

The measurement aimed to identify the range, robustness and reliability of the implemented network within a real industrial environment. The measured parameters RSSI, SNR and PER are explained in more detail hereinafter.

**Received Signal Strength Indicator (RSSI)**: RSSI indicates the range between the end-node and the gateway, which determines the signal strength. Due to its minimum value, the device range is limited. The implemented gateway has a minimum value of -120 dBm. Consequently, it is not possible to sense a signal with a lower RSSI value. If the spreading factor changes (SF), the transmission time (time-on-air) and the communication range may be influenced. Figure 12 presents the RSSI values for the testing scenario.

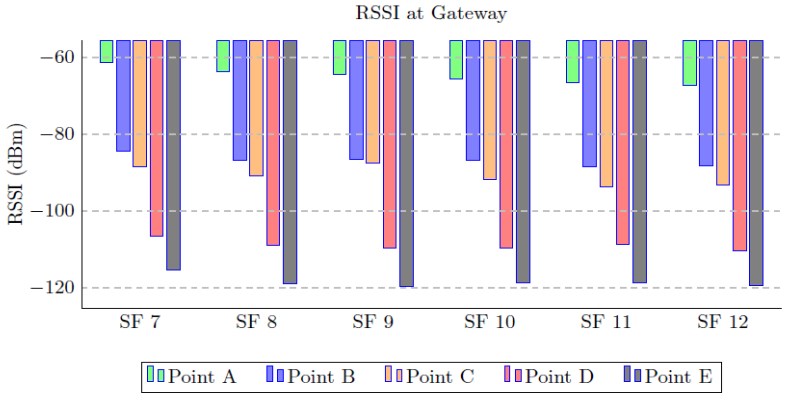


**Figure 10** RSSI at Gateway: RSSI versus spreading factor for all testing positions (A, B, C, D, E)

**Signal-to-Noise Ratio (SNR):** SNR determines the signal quality and transmission robustness in environments with a high noise level. In the described use case, the range is between 10 dB and -20 dB. However, SNR lower than the minimum limit is receivable due to the robust modulation scheme of the LoRa technology. (CSS). Heavy noises, such as machinery, speed motors or scale fading of the metallic environment have an impact on the SNR. The results of the evaluation are shown in Figure 13.

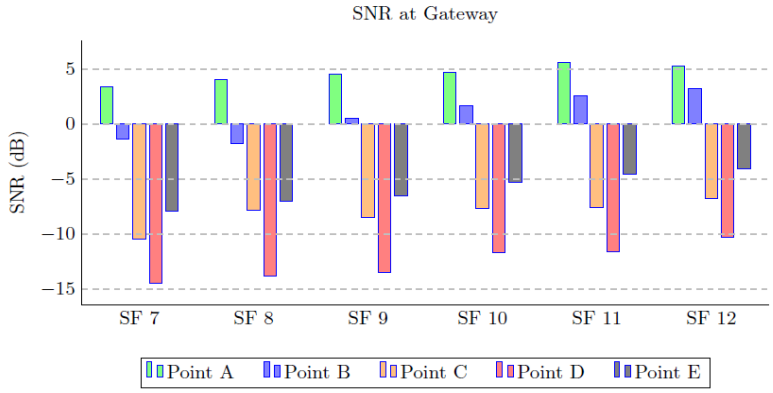


**Figure 11** SNR at Gateway: The SNR varies proportionally to the spreading factor for all the points

**Packet Error Rate (PER):** PER defines the reliability and performance of a network, based on the packet losses during data transmission. The packet can either not be received or with errors, which can not be corrected by the forward error correction (FEC) mechanism. FEC supports the recovery of partially received packets. Then, different values for Coding Rates (CR) can be used (1-4 for LoRa). Figure 14 presents the CR in a range of 1-4 for possible SF values.

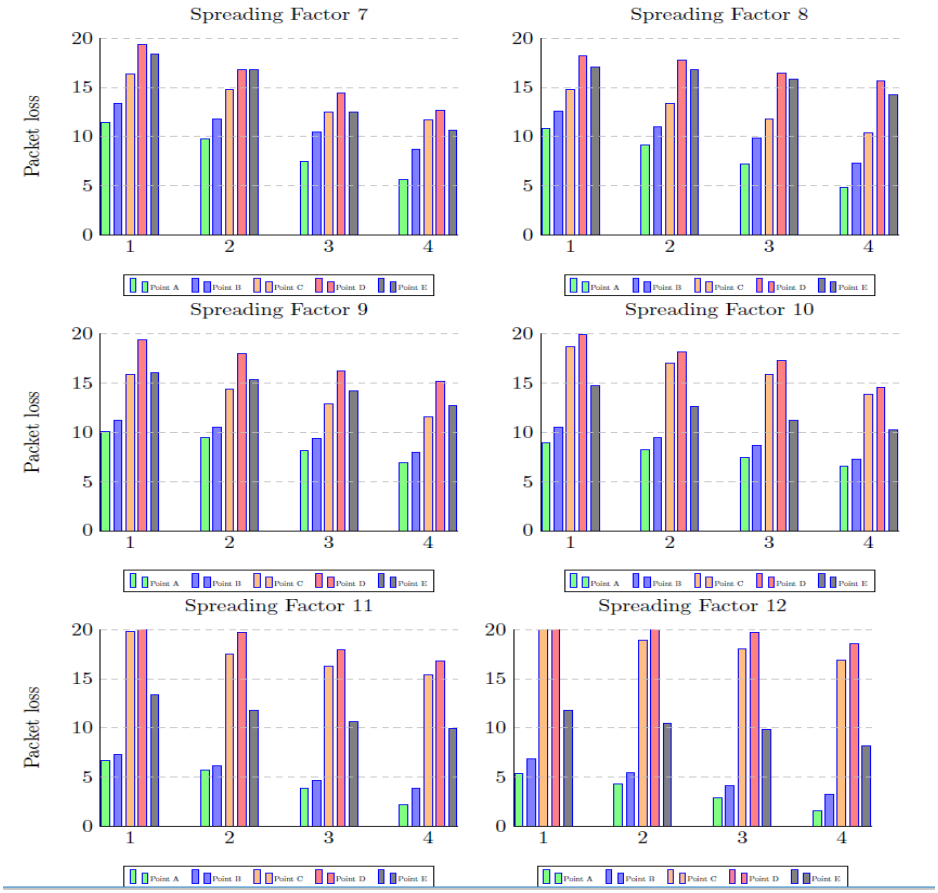


**Figure 12** PER (Packet loss) evaluation based on CR: 1-4 at different SF´s and points A, B, C, D, E to determine the robustness of the network.

The measurement environment with an acceptable and achievable range for the LoRa-shields and gates ways reaches a distance of about 500 m. The key findings are shown in Table 5:

**Table 5** Advantages and Disadvantages of LoRaWAN Parameters

| Parameters | Advantage | Disadvantage |
|---|---|---|
| **Spreading Factor** ↑ | Range ↑, Robustness ↑ | Data rate ↓, Power consumption ↑ |
| **Coding Rate** ↑ | Reliability ↑ | Packet length overhead ↑ |
| **Bandwidth** ↑ | Data Rate ↑ | Interference probability ↑ |
| **Transmission power** ↑ | Range ↑ | Power consumption ↑ |

Possible improvements for comparable use-cases include higher density deployment of network devices and a careful placement at certain positions to prevent Fresnel zone blockages. Static obstacles enhance robust and reliable backbone wireless infrastructure. A mesh-network topology with a mesh table based on RSSI increases the network awareness of end-node distances. A Time-slotted Event-Driven Stack (TEDS) enhances the ALOHA (random access MAC protocol where devices transmit at will when they have data to send, which can have a significant effect on the overall bandwidth) and the number of downlink messages must be considered for network scaling.

Wireless connectivity is implied as a fundamental enabler in the idea of smart production, opening the door for new efficiencies in industry through greater automation and optimization of production processes and enhancement of factory floor operations and productivity. However, in many respects, wireless technologies is still a large missing piece in the way towards truly connected production environments. The growing demand and coupling between smart industrial automation, IIoT, and CPS is currently a strong driving force for the ongoing evolution of wireless connectivity platforms and infrastructure solutions. Industrial environments pose a lot of challenges for wireless communication systems which are highly vulnerable to interferences from various sources, e.g. the operation in a shared ISM band, the existence of strong electromagnetic (EM) fields, the noise caused by the surrounding machinery, and the harsh metallic and very dynamic industrial environment that causes strong multipath fading. Such interference is very hard to predict and mitigate leading to communication robustness and reliability issues and high susceptibility to transmission errors. This causes a great deal of hesitancy for using wireless technologies in this setting and presents a set of constraints which are different from the benign lab environment, thus requiring many trade-offs for a successful and viable implementation of a wireless solution in the industrial space.

In IoT4CPS, the aim is to evaluate novel wireless technologies that address compellingly the unanswered connectivity requirements set by an Industry 4.0 environment and show the capabilities and limitations of these in a real use-case scenario. In this context, the implementation and performance evaluation of LoRaWAN in a real indoor and outdoor industrial environment, based on certain connectivity metrics and testing scenarios under various conditions, revealed suitable choices and compromises for smart metering applications in similar industrial use-cases. The results of this pilot implementation allow for a reality check of a low-power and low-cost connectivity solution that can offer true benefits to smart industrial use-cases, and for unique insights towards the integration
of similar wireless technologies as these are evolving along with Industrial IoT.

# 4 Conclusion

This deliverable deals with connectivity issues in Industry 4.0 and covers the applicability of tools, methods and models related to it. Communication in Industry 4.0 demands the following crucial requirements: Latency, Reliability, Scalability, Secure Communication, Inter-Operability and Robustness. Wired communications have certain drawbacks in the Industry 4.0 environment, therefore, wireless technologies are preferred for future deployments. To respond to the mentioned requirements, wireless technologies in industrial automation still need to be further developed.

The increasing use of wireless technologies is due to the ability to fulfil the requirements of communication in Industry 4.0. Currently, the following protocols are applied: Wireless HART, LoRa and IEEE 802.15.4. However, within a wireless network, security issues such as signal propagation in transit and component accessibility may occur. Wired and wireless networks share common protocols at the application, transport, and network layer with the same kind of security attacks and measures. The broadcast nature of a signal differentiates the form of attacks and measures in wired and wireless networks at the physical and MAC layers. Mass adoption of wireless connectivity technologies in the industrial space has a long way until it becomes a reality and enables the promises and benefits of smart factories in the Industry 4.0 era.

The IoT4CPS demonstrators include AVL´s Device Connect, X-Net Virtual Factory and Infineon´s Device Application for Wireless Industrial Connectivity. Firstly, AVL´s Device Connect provides trustworthy CAN communication over wide-area connections. The application and evaluation of such technologies into real smart production environments perform a reality check for a low-power and low-cost solution that can offer true benefits and presents the results of a pilot implementation that allows for value establishment and unique insights towards the integration of similar wireless technologies as these are evolving along with IIoT. Secondly, X-Net developed the SBI-Box for increasing security requirements, considering fast and uncomplicated integration, easy maintenance and update of the system or global decentralized commissioning. The future aim for the SBI-System is to develop an open source-based industrial product. Thirdly, Infineon implemented a LoRaWAN architecture in the fabrication unit for long-range communication of the external sensors for monitoring and controlling of the manufacturing process from various clients. The ease of installation and maintenance provides a significant advantage over wired communication for such long distances. The performance measurement considering different connectivity metrics, testing scenarios and conditions demonstrates that LoRaWAN is appropriate for smart metering applications in related use-cases. However, it is not suitable for wireless use-cases with higher throughput, due to the trade-offs of the data rate for long-range. To raise the performance in comparable applications, Fresnel zone blockages and static obstacles need to be eliminated by a higher density deployment of the network. Furthermore, a mesh network topology for the awareness of end-node spans and a TEDS for enhanced ALOHA systems should be taken into consideration. To optimize the network scaling and avoid impairment of the network, the amount of downlink messages is important. Alternative, more pricey technologies, such as Kerling IoT station, Lorrier or Rak831+Pi, could be used to enhance capability, coverage, robustness and reliability (Ahmed, 2020).

# 5 References

Ahmed, A. e. (2020). Wireless connectivity in Industrial sensor and control networks: Challenges and issues in a real implementation for a smart production use-case. *2020 25th International Conference on Emerging Technologies and Factory Automation (ETFA).* IEEE.

Alcácer, V. a.-M. (2019). "Scanning the industry 4.0: A literature review on technologies for manufacturing systems. *" Engineering Science and Technology, an International Journal 22.3 (2019):*, 899-919.

Al-Qaseemi, S. A. (2016.). "IoT architecture challenges and issues: Lack of standardization." 2016. *Future Technologies Conference (FTC). IEEE.*

Andulkar, M. D. (2018.). "A multi-case study on Industry 4.0 for SME's in Brandenburg, Germany.". Hawaii: Proceedings of the 51st Hawaii International Conference on System Sciences.

Armendia, M. e. (2019). "Machine Tool: From the Digital Twin to the Cyber-Physical Systems." Twin-Control. Springer, Cham.

Augustin, A. e. (2016). A study of LoRa: Long range & low power networks for the Internet of Things. *Sensors*, 16(9), 1466.

Ayele, E. e. (2017). Performance analysis of LoRa radio for indoor IoT applications. *2017 International Conference on Internet of Things for the Global Community (IoTGC)* (pp. 1-8). IEEE.

Breivold, H. P. ( 2017). "A Survey and Analysis of Reference Architectures for the Internet-of-things." ICSEA 2017.

Cheruvu, S. e. (2020). "Connectivity Technologies for IoT." Demystifying Internet of Things Security. . Berkeley, CA: Apress.

D. Chen, M. N. (2010). WirelessHART - Real-Time Mesh Network for Industrial Automation. Springer.

Delsing, J. e. ( 2017). CRC Press.

Ertürk, M. A. (2019). "A Survey on LoRaWAN Architecture, Protocol and Technologies." Future Internet 11.10 (2019).

Gambi, E. e. ((2018)). A home automation architecture based on LoRa technology and Message Queue Telemetry Transfer protocol. *International Journal of Distributed Sensor Networks 14.10*.

Gambi, E. e. (2018). A home automation architecture based on LoRa technology and Message Queue Telemetry Transfer protocol. *International Journal of Distributed Sensor Networks 14.10 (2018): 1550147718806837.*

Gidlund, M. T. (2017). "Will 5G become yet another wireless technology for industrial automation?.". *IEEE International Conference on Industrial Technology (ICIT).* IEEE.

Gilchrist, A. (2016). Industry 4.0: the industrial internet of things. . Apress.

Han, S. e. ( 2013). Building wireless embedded internet for industrial automation. *IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society. IEEE.*

Han, S. e. (2013). "Building wireless embedded internet for industrial automation." *IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society. .* IEEE.

Han, S. e. (2013). Building wireless embedded internet for industrial automation. *IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society*.

IIRA17. (2017). *The Industrial Internet of Things. Volume G1: Reference Architecture. IIC:PUB:G1:V1.80:20170131.* Industrial Internet Consortium.

LoRaAlliance. (2020). *Lora Alliance-wide area network for IoT*. Retrieved from https://lora-alliance.org/

Mahmood, Z. (2019). *The Internet of Things in the Industrial Sector.* Springer International Publishing.

Mikhaylov, A. e. (2016). Analysis of capacity and scalability of the LoRa Low Power Wide Area Network technology. *22nd European Wireless Conference* (pp. 1-6). VDE.

New, W. K.-O. (2017). Resource management for symmetrical applications over heterogeneous services in IEEE 802.16. *" Wireless Networks 23.8 (2017): 2601-2616.*

OPC. (2020). *OPC Foundation. The Industrial Interoperability Standard.* Retrieved from https://opcfoundation.org/

RAMI4.0. (2015). *Reference Architecture Model Industrie 4.0 (RAMI 4.0).* ZVEI.

Sisinni, E. e. (2018). "Industrial Internet of things: Challenges, opportunities, and directions."14.11. *IEEE Transactions on Industrial Informatics*, (pp. 4724-4734.).

Tessaro, L. e. (2018). LoRa Performance in Short Range Industrial Applications. *2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)* (pp. 1089-1094). IEEE.

Varghese, A. e. (2014.). "Wireless requirements and challenges in Industry 4.0.". *International Conference on Contemporary Computing and Informatics (IC3I). IEEE.*

Wollschlaeger, M. e. (2017). The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. *IEEE Industrial Electronics Magazine*, 11(1), 17-27.

Xiao, Y. e. (2006). MAC security and security overhead analysis in the IEEE 802.15. 4 wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking 2006.2 (2006): 81-81.*

Yang, N. e. (2015). Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine, 53*(4), 20-27.

Yang, N. e. (2015). Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine, 53*(4), 20-27.

You, I. e. (2018). An enhanced LoRaWAN security protocol for privacy preservation in IoT with a case study on a smart factory-enabled parking system. Sensors 18.6 (2018).

Zou, Y. e. (2016). A survey on wireless security: Technical challenges, recent advances and future trends. *Proceedings of the IEEE 104.9*, 1727-1765.

## Appendix A. Article to Read

Online: https://www.postscapes.com/internet-of-things-protocols/