IoT4CPS
Trustworthy IoT for CPS

Secure and Reliable IoT Communication for Autonomous Driving and Manufacturing (incl. 5G)

Date: August 2020
Editor: Heinz Weiskirchner
Authors: Christos Thomos, Nikolaus Dürk, Christina Tiefnig,
Stefan Marksteiner

Contents

1. SUMMARY

The digitalization and increasing connectivity of cyber-physical objects enable the development of new applications. They also lead to new safety and security related requirements in terms of design, testing, production and operation of these systems. A cost-effective realization of the trustworthy and secure cyber-physical systems and applications in Automated Driving and Industry 4.0 requires a holistic approach that combines operational aspects as well as technology development.

This paper provides an overview of developed methodologies, architectures and IoT4CPS use-cases, all aiming to improve and guarantee the needed security requirements in the field of IoT communications.

Chapter 2 outlines the challenges originating from the fields of secure IoT communication for automatic driving and production plants. Four distinct areas are considered: communication inside the vehicle and its CPSs, communication between the vehicle and all external entities, communication inside the manufacturing plant, and communication between the manufacturing plant and all external entities (*Figure 1*).

Chapter 3 elaborates the IoT4CPS development that is focused on IoT communication issues. These are assembled and matched to the findings and approaches needed to mitigate security issues.

Chapter 4 deals with communication aspects based on predefined use cases, which employ described methodologies and the architecture. It also showcases the main results.

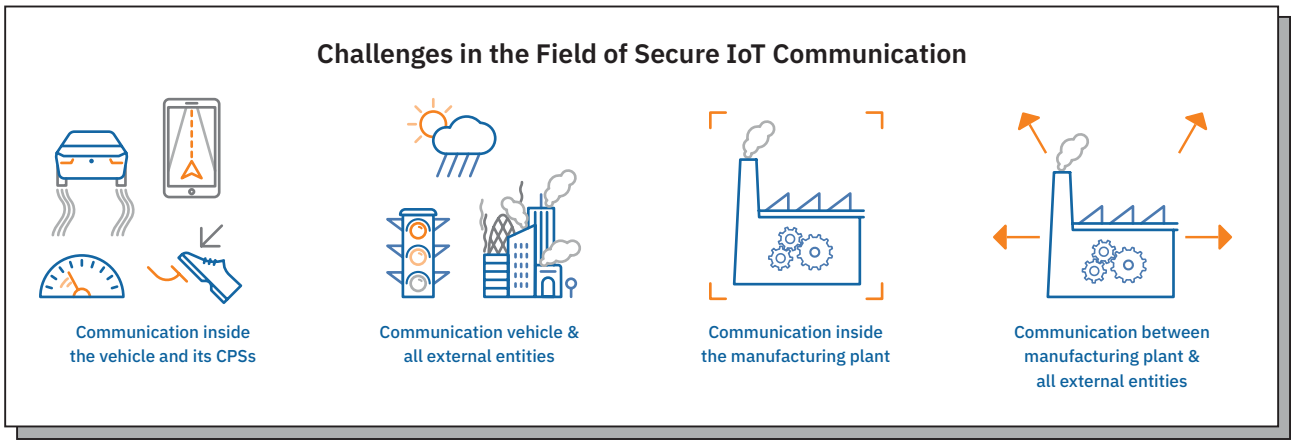


Figure 1: The challenges originating from the field of secure IoT communication for automatic driving and production plants

2. CHALLENGE

Digitalization over the entire product lifecycle accelerates the development, validation, instrumentation and deployment of complex industrial products while increasing product quality. In combination with the increasing connectivity of (critical) cyber-physical objects, digitalization enables the development of new applications. It also leads to new safety and security-related requirements that concern the design, testing, production and operation of these systems.

A cost-effective realization of the full potential of trustworthy and secure cyber-physical systems and applications in Automated Driving and Industry 4.0 drives the demand towards a holistic approach that combines operational aspects as well as the integration of the evolving technology. The objective is to integrate security levels across all dimensions to a) ensure trusted interaction across devices, machines and networks; b) maintain integrity, authenticity and confidentiality of information; and c) sufficiently protect production data and intellectual property.

IoT4CPS has developed guidelines, methods and tools to enable safe and secure IoT-based applications for automated driving and smart production. The project addresses safety and security aspects in a holistic approach along the specific value chains and the product life cycles.

The main focus of IoT4CPS is on developing, producing and operating, highly trustable components and applications for Connected and Automated Driving. As the design and production of these components require a high degree of integration and information exchange along the life cycle, the methods and tools investigated are

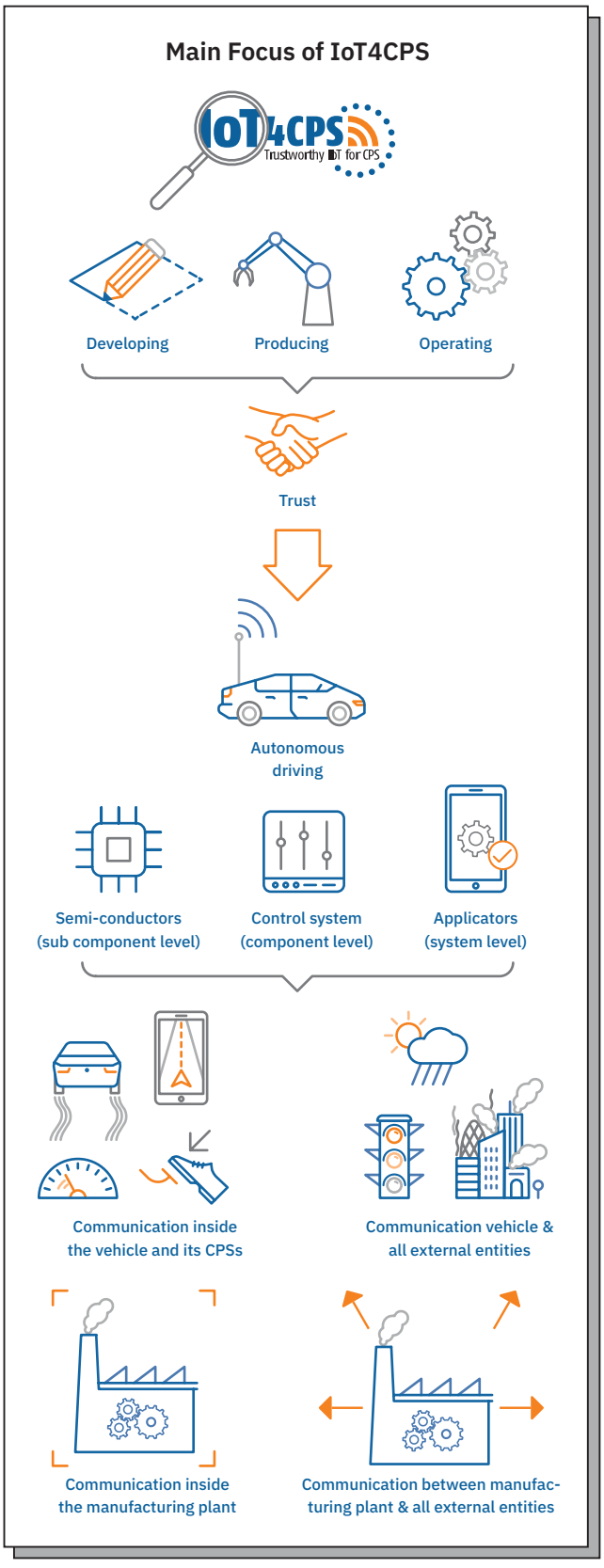


Figure 2: The main challenges presented in communication for autonomous driving and manufacturing.

also highly relevant for the Smart Production use case. Rather than considering the full bandwidth of Industry 4.0 applications, IoT4CPS' scope considers a subset of the Smart Production value chain that is linked to the automotive use-case.

IoT4CPS follows the ubiquitous security paradigm and addresses the entire technology stack from semiconductors (sub-component level), via control systems (component level), to applications (system level). Additionally, specific aspects of accessing the surrounding infrastructures are also considered. (*Figure 2*) Thus, IoT4CPS supports digitalization along the entire product lifecycle, leading to a time-to-market acceleration for connected and autonomous vehicles. The project offers innovative components, leading to efficiency increases for the deployment of level 3 and level 4 autonomous driving functions.

This document compiles all aspects and findings elaborated in IoT4CPS project for secure and reliable IoT Communication for autonomous driving and manufacturing between all involved CPS's and their environment.

In general, there are 4 distinct communication areas:

- inside the vehicle and its CPS
- between the vehicle and all external entities, the V2X communication
- inside the manufacturing plant
- between the manufacturing plant and all external entities.

3. CURRENT STATUS

Figure 3 gives an overview of different perspectives and the focus of IoT4CPS partners is illustrated. The rest of this chapter describes the current development status per communication topic.

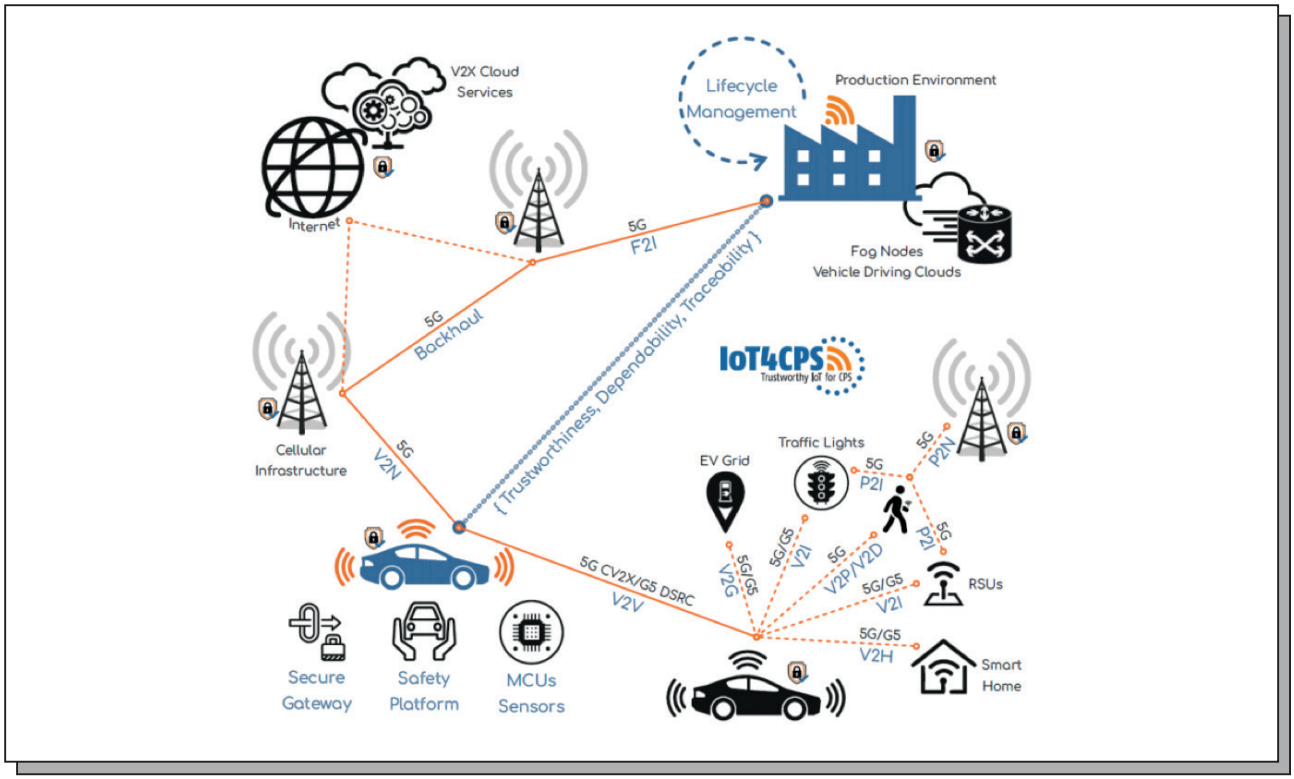


Figure 3: V2X architectural aspects for secure and reliable communications

3.1. V2X Communication in Autonomous Driving

V2X connectivity aims to enhance the safety of road users by extending the sensing capabilities of on-board sensors, as well as vehicles computing power through the specialized ad-hoc edge and cloud application services. Through data exchange with the communication network and the surroundings (e.g., nearby vehicles, the road infrastructure, pedestrians), the on-board sensor data is exchanged and enhanced through communication with surrounding entities. V2X communication comprises four main sub-categories: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I road infrastructure), vehicle-to-network (V2N backend/internet), and vehicle-to-pedestrian (V2P) communication, which can be extended by including a variety of other use-cases. When fully empowered, it will become a key enabler and a vital component of AD.

Current connectivity options applied to non-safety critical applications of SAE 0 and 1 level vehicles are in a basic form and are failing to meet the requirements of SAE Level 2-5 safety-critical applications. Higher levels of dependability, lower latency and higher capacity of wireless data communication are of paramount importance. AD strongly depends upon the integration of heterogeneous connectivity technologies (for in-vehicle and external radio access), with immense interoperability and cross-interference issues and a

great difference in technology life-cycle between the vehicle and the communication modems. Wireless links must withstand the extremely complex vehicular environment, in terms of mobility and dynamics, with highly diverse and contradictory demands concerning the communication characteristics, as well as to other properties such as positioning accuracy, security, privacy and functional safety. Also, wireless connectivity introduces multiple security vulnerabilities into vehicle controls, infotainment, telematics and navigation systems or the supporting cloud infrastructure. Therefore, security-by-design is imperative for sandboxing communication system drivers, embedding security across the entire V2X development phase and ensuring end-to-end encrypted communications and data privacy that safeguards autonomous vehicles at the system level.

An initial evaluation of the quality of V2X technologies employs established metrics, such as end-to-end latency, communication coverage, position accuracy, data rate, link reliability and security features. The assessment of fundamental parameters determines capabilities of main V2X technology options, system architectures, constraints and hardware specifications that fulfil envisaged connectivity scenarios. The limitations must be resolved early in the design through simulations and large sets of field trials for as many V2X use-cases as possible. However, modelling, development, integration and testing in such an environment is an exceptional challenge. Also, as connected and autonomous vehicles become a common part of this complex ecosystem, requirements are becoming stricter and more demanding for unfolding the full potential of autonomous and cooperative driving. It is a common understanding that commitment from all V2X stakeholders is necessary to establish a complete connectivity framework able to fulfil the ambition for evolution from SAE Level 2 to 5.

Main vehicle connectivity options are Dedicated Short Range Communications (DSRC) based on IEEE802.11p WLAN and 3GPP Cellular V2X based on cellular 4G (Rel. 14 and beyond) and upcoming 5G NR. Both options focus on lower layer definitions to offer long-range, non-line-of-sight abilities as an extension to vehicle sensors adding a redundancy factor towards enhanced safety and cooperative driving features. The upper layers are based on standardization activities such as IEEE (e.g., 1609), SAE, IETF, ETSI, ISO and CEN.

DSRC (EU: ITS-G5, US: WAVE) was developed for safety-critical V2V and V2I, by specifying ad-hoc networks (no communication infrastructure) in dedicated license spectrum bands (5.9GHz ITS band). It exchanges basic safety data with very low latency (<50ms) in 2km radius, using public infrastructure and data security based on IEEE1609.2. The physical layer and lower MAC use the IEEE802.11p WLAN standard, which was finalised in 2010. Since then, IEEE802.11p [1] has passed broad and extensive validation tests and is very stable. It offers many mature products for deployment (e.g., C-ITS C2C-CC [2]). Its Delegated Act [3] is awaiting EU approval. Hence, DSRC technology could become a regulatory requirement for intelligent transport system (ITS).

As no immediate advances are expected, DSRC applicability to V2X is limited. That opens the space to 3GPP Cellular V2X (C-V2X), which will leverage on 4G LTE evolution to 5G NR [4]. Cellular infrastructure is essential for data exploitation aimed to provide specialized cloud services, critical software and firmware over-the-air updates, life-cycle management, predictive maintenance, remote monitoring, as well

as many alerts, warnings and notifications. The AD requirements are challenging for 4G LTE C-V2X and DSRC technologies, but 5G NR promises improvements in data rates, QoS support, ultra-low end-to-end latency, capacity and reliability, coverage and number of device connections, security, localization, energy efficiency, performance consistency and application support. These features aim to address ultra-reliable and low-latency connectivity for mission-critical services, device-to-device (V2V, V2I) communications, enhanced mobile broadband (V2P, V2N) and machine communication, as needed for a fully autonomous vehicle ecosystem. The upper layers of LTE C-V2X are making use of the same standards as the IEEE802.11p based technologies, as specified by the automotive industry. However, independent implementation of two technologies and lack of interoperability mechanism renders them incompatible.

The resulting technology selection dilemma is further complicated by the EC activities that could create a de facto mandate to integrate ITS traffic and safety-related communications. Considering the average 10-year vehicle lifespan, DSRC technology is likely to aid the upcoming vehicle generation in the 5.9 GHz ITS band. C-V2X is expected to enter markets in the early 2020s, as a complement to V2V and V2I connectivity (safety-critical ADAS and AD functions) and will enhance V2X connectivity with its unique V2N and V2P capabilities.

For faster deployment of C-V2X technology, wireless infrastructure technology advancements and achievements by the relevant stakeholders will play the most crucial role, since this is the important differentiating factor from a useful but outdated DSRC technology. In this context, IoT4CPS aims to examine 5G PHY layer technologies for the cellular access points, HW architectures and behavioral models, transceiver modules capabilities and limitations, specifications for key building blocks that can compellingly address the requirements of secure C-V2X connectivity taking also into account the progress for the vehicle communication modules, sensors, actuators and computing hardware, as well as the solutions and tools developed for secure and safe autonomous driving platforms.

3.2. Communication inside the Vehicle

In-vehicle networking is responsible for the exchange of data between vehicle's ECUs controlling the functions of sensors and actuators. It is usually based on central secure gateway architectures or domain controller architectures configured with security modules and service-oriented connectivity in specific functionality domains. The nature of the advanced vehicle sensors and the amount of data they produce would require fast and reliable transmission and real-time fusing, analysis and processing so that accurate ADAS decisions can be useful for the safety of the vehicle. Currently, in-vehicle networking is being supported by bus systems such as CAN (ISO 11898 – Controller Area Network – de facto standard for moderate data rates and reliability), LIN (Local Interconnected Network – main characteristic is low power consumption), FlexRay (used for higher data rates and high reliability), MOST (Media Oriented System Transport – used for infotainment vehicle infrastructure) and Ethernet. The framework, architectures and specifications that enhance the communication protocol stacks for these types of networking in order to include highly autonomous driving use-cases, are being developed further by the AUTOSAR consortium using standardized adaptive platforms and processes for different configurations and topologies. These are required to include

protocol enhancements for ETSI G5 and cellular (4G, 5G) technologies for external V2X connectivity. At the same time, GENIVI alliance is focusing on infotainment platforms and defines specifications and standards providing toolboxes for function domains that include vehicle's infotainment system connectivity utilizing wireless technologies such as Wi-Fi, NFC, Bluetooth, as well as Flexray, CAN, Ethernet (also HDBaseT) networking for SOTA/FOTA updates, multimedia, navigation, telephony and other advanced telematics services. These services also need to consider the challenges of the upcoming V2X connectivity technologies like 3GPP Rel.15 and onwards, in order to address robustness, safety, security and privacy issues.

3.3. Communication inside the Manufacturing Plant

Production companies are currently facing enormous challenges in the IT security area. On the one hand, manufacturers are forced to protect themselves from external attacks towards their production operations. On the other hand, they have to open up and network with suppliers and customers.

An additional aspect that the manufacturers need to consider is that their products require remote maintenance, updates and upgrades over their entire life (Life Cycle Management). They also need data for the analysis of errors and the further development of the product or the construction of artificial intelligence (AI).

In the past, the focus was on isolating the IT landscape of the production from the office network and external influences. Nowadays, completely new demands are placed on the production network and its infrastructure. Sub-suppliers of production systems and their components need secure access to their products to maintain their service and uphold quality standards. Furthermore, content owners need connections to provide the data (software, configurations etc.) that need to be integrated into the IoT product without granting data access to the on-site personnel. Not only the data transfer but also the recording processes on flash media, the flash media itself and the assembling have to be secure and to ensure that the data cannot be misused by third parties.

Likewise, the globalization of production and external conditions (e.g. Covid-19 restrictions, restrictions in air traffic, etc.) add a level of complexity to the rapid on-site services. Just as the shutdown at the start of 2020 taught us to communicate decentral in a new form, new structures in the IT sector are required for production companies.

Conditions in the IT area:

- Secure access for suppliers and sub-suppliers to their systems and products
- Access to sub-units of the machine (e.g. for sub-suppliers)
- Monitoring of data streams
- Safety aspect: protection of the systems & visualization of remote maintenance processes

The past practices that were based on a belief that being able to solve major issues via VPN and remote maintenance turned out to be very complex and time-consuming – sometimes even unsolvable for the simplest problems.

Concrete issues that need to be addressed:

- Connectivity (lack of bandwidth and internet connection)
- Too strong residual reactions, which in turn lead to the fact that existing security structures are bypassed
- Lack of awareness and knowledge in the security area associated with maintaining a production process
- Inadvertent loss of metadata due to the used systems
- Lack of monitoring for external connections

In our example, we consider the supply chains for the production process of a vehicle, in which different manufacturers deliver components that are in turn manufactured by sub-suppliers. The components are e.g. electronic components that need to be serviced by the manufacturer along its life cycle. In most cases, these include the following requirements:

- Updates/upgrades
- Failure analysis
- Data collection to build AI algorithms

3.4. Communication from Manufacturing Plant to External Entities

We need to consider two communication channels in this context:

1. Communication between the manufacturers and their suppliers
2. Communication between manufacturers and their products

Ad 1.) A manufacturer relies on one or more suppliers with sub-suppliers who e.g. provide part of the product or a machine of the production process. A closer look at a production machine reveals that it consists of different components (manipulators, sensors, servers, etc.). The manufacturer must provide the supplier with secure access to this production machine. The production machine is usually not separated from the entire production network in terms of safety. In this case, the supplier has access to the entire production network. The issue expands once the supplier has to forward sub-suppliers the access.
In most cases, VPN and remote maintenance tools (e.g. Teamviewer) are used and a transparent audit log (remote maintenance activities, changes and which data was transferred to and from the machine) is usually not possible. The current practice relies on trust between the manufacturer simply and the suppliers. Contracts are used to compensate for the security gap. Likewise, the supplier must trust that the manufacturer ensures that no devices or systems of the manufacturer can interfere with or influence their own systems.

Ad 2.) Communication from the Manufacturer to his product
A manufacturer, which produces a vehicle component e.g. the infotainment or sensor system, may desire to update or upgrade the delivered systems in the life cycle of the product. They may also wish to perform remote analysis of an unknown error. The transmission of different product metadata to the manufacturer becomes increasingly important. Above all, the establishment of artificial intelligence requires the data

that is related to the individual devices. These product data are of enormous importance especially for the construction of AIs for AD. Data anonymization and privacy protection are of enormous importance in this context and are considered in the concepts and solutions developed in IoT4CPS.

The connections in most areas can hardly be broken with simple rules and precautions. The complexity of networking is increasing enormously and requires new concepts and individually adapted security systems. Solutions have to consider the protection of each single IoT device, not only now but also in the future. The highest available level of security is the complete individualisation of security mechanism. This is the only logical and effective method to secure products against hacking and fraud. At the moment, IoT devices are configured all in the same way. If the security of one device is breached, many other devices may be affected too. Metadata, user data and product-specific data of many devices may be extracted without recognition of the user. Unique encryption, which means that each software distribution has its own key and is connected to a specific product, prevents that this software is used in another product (even in a product of the same batch) or ensures that no other IoT product is affected.

From a legal point of view, all of this can be regulated very easily by contract. However, such legal agreements do not ensure protection if data and secret information leave the organisation unknowingly (metadata, information about the production process, machine data and personal product-specific data etc.).

There is a need for processes and workflows that allow individual content and individual encryption. Systems to record flash devices have to be integrated directly in manufacturing environments and to support the error-free correlation of content and IoT products. Conventional process to provide data have to be adapted to meet the need of IoT communication for manufacturing, as data (e.g. software, configurations, metadata) has high value and contains the unique selling propositions against other products.

IoT devices are no longer pure hardware products. Their digital content (software, configurations, metadata etc.) is likely to be more valuable than their hardware. In modern manufacturing settings, content owners are not manufacturing products any more. They deliver their content to third parties where the manufacturing of IoT products takes place. Not only the delivering process has to be secure, it is furthermore important that the content is secure during the whole production process.

Data can be recorded to encrypted flash media and shipped all over the world to the production site. Besides the fact that this would mean having a lot of media on stock, many risks are associated with this strategy. The correlation of individually encrypted media to the corresponding IoT product is nearly impossible then. Software changes or new releases are not available immediately, as flash media has to be produced in advance. Many other questions may be raised over the events unfolding in situations such as when a container full of flash media is either damaged or lost, when managing access and identification processes to the SBI-Box or the IoT device, when needing to provide access during the production when the data to be recorded is decentralized etc. Secure Boot, unique and personalized encryption considering product-specific indicators and explicit identification are only some parameters that have to be considered already during the recording process of flash media.

Solutions to record the flash media directly on-site without any access to the data on-site and workflows that support error-free correlation and security features the control access, removals and other operation are needed. Only then, it is possible to record flash devices directly in the place they are needed: at the manufacturer, where they are directly assembled into the products.

4. APPLICATION

This chapter showcases the IoT4CPS communication aspects, which is depicted in *Figure 4*.

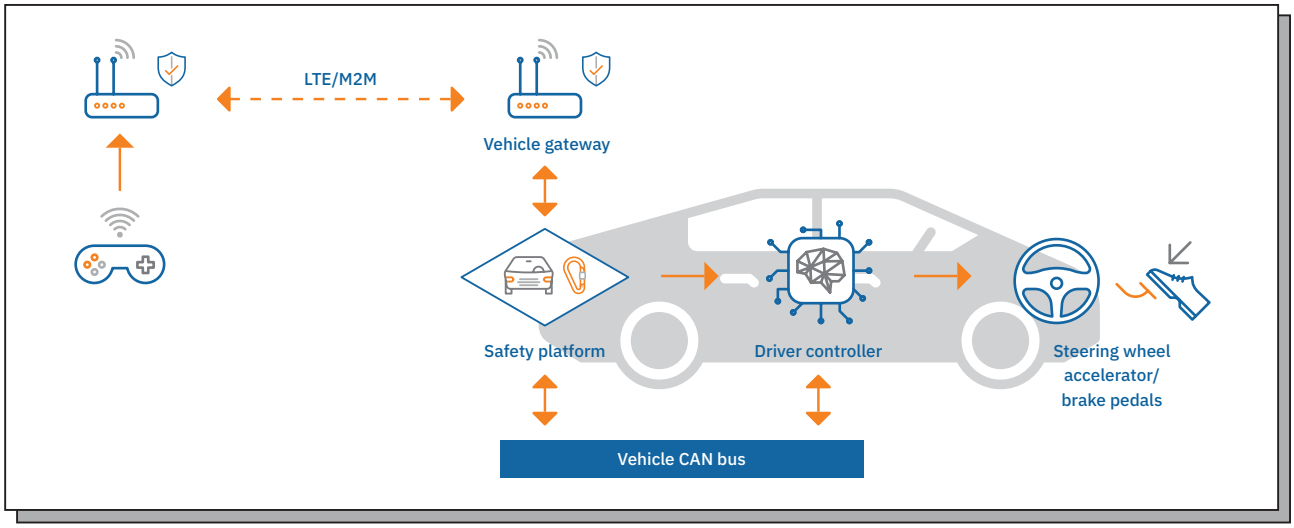


Figure 4: Use-Case for vehicle communication

4.1. Communication from Vehicle to Outside: Application of the Device.CONNECT System into a Vehicle Environment

The CAN-based communications of In-Vehicle Networks (IVN) are, by their nature, non-routable bus communications. However, the presented technology enables establishing trustworthy wide-area connections for CAN communications using an extended version of AVL's Device.CONNECT™.

Traditional CAN messages do not have built-in security features (apart from rudimentary plausibility checking capabilities). The protocol is designed for internal communications. However, with the demand for IoT technologies to enter automotive systems, there is a need for possibilities to transfer messages over hostile environments (specifically the Internet). The architecture proposed in this section consists of a component to be built into the vehicle, called Smart Hub. It creates a secure connection to the vehicular network, allowing only a very restricted set of commands. Hence, the integrity of the vehicle network is maintained. To establish outside connections, the Smart Hub connects as a subscriber to a message broker that hosts a publishing service. A backend system, also subscribing to the broker in the same manner, poses the remote station. Both devices connect securely to the broker via a state-of-the-art TLS connection, having their respective necessary private key secured by hardware security modules (HSMs). In order to prevent threats induced by a corrupted broker, the data is additionally end-to-end encrypted through content encryption. From a network security perspective, all ports are closed inbound on all devices except for each broker port to allow for accepting connections from the Smart Hub and Backend, greatly minimizing the attack surface of the overall system. *Figure 3* shows an architectural overview of the setup.

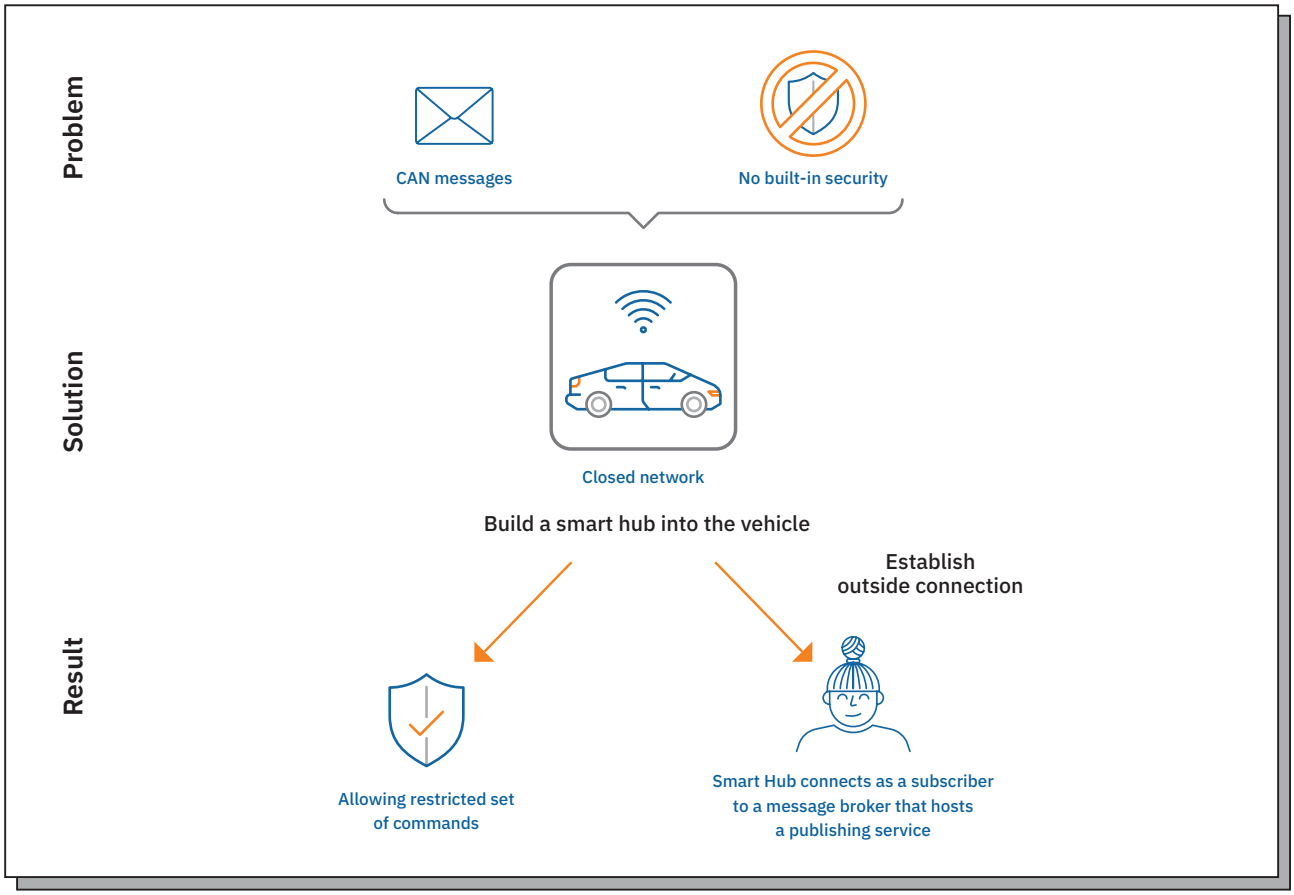
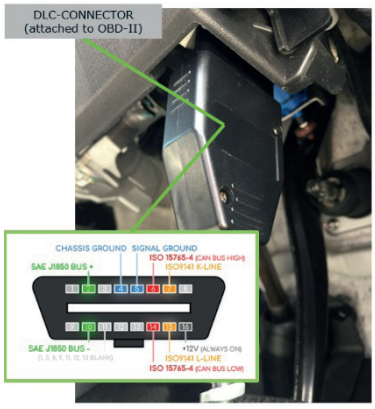


Figure 5: Trustworthy wide-area connection of an automotive system using AVL Device.CONNECT™

In a demonstrator, a vehicle could be trustworthily connected through this system using the vehicle's on-board diagnostics (OBD-II) interface (*Figure 5* depicts the setup). Through a router, the Smart Hub connected to the back end with a simple GUI that visualized signals like speed or the breaking pedal position. As the Channel is bidirectional, devices inside the vehicle can be flashed and calibrated. Together with a 99% available real-time stream of the IVNs CAN messages, this creates the opportunity to remotely perform vehicle maintenance tasks from the other side of the globe.



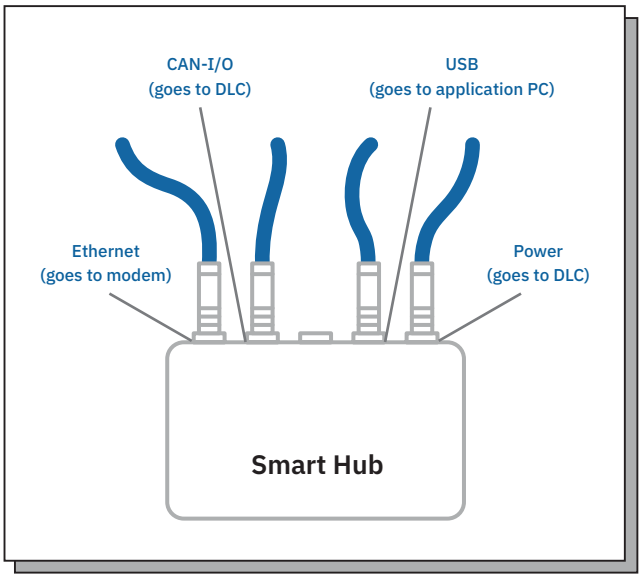


Figure 6: Smart Hub vehicle connection

4.2. Communication Inside the Manufacturing Plant: Secure Connection of Industrial Sensor Equipment to a Backend Framework for Data Analytics

Industrial Wireless Sensor Networks (IWSNs) have emerged in the wireless industrial domain as a collection of distributed wireless devices that wirelessly communicate to measure, monitor and control physical industrial environments. Communication inside a manufacturing plant involves many challenges caused by the interfering and noisy environment. Various wired protocols have been used to establish a robust and reliable communication inside the industrial plants. However, the advancements in the technology are bringing the transformation of communication to a wireless domain. Lately, wireless IoT protocols have pushed their existence into the industrial communication sector as they overcome the hindrances of cable laying, maintenance and deployment costs and also enabling device portability.

As a use case example, a wireless prototype is tested in Infineon's Pilot room for Industry 4.0. The scenario caters to industries requiring long-range for smart metering applications that is cumbersome with the present-day wired systems. For data critical process control operations, a wired solution offers better performance aspects. The use-case for the experiments concerning the wired/wireless technologies is an industrial wafer producing fabrication unit consisting of robotic arms, machines, external sensors, LAN and host systems as shown in *Figure 7*. The setup focuses on the external sensors of the fabrication unit.

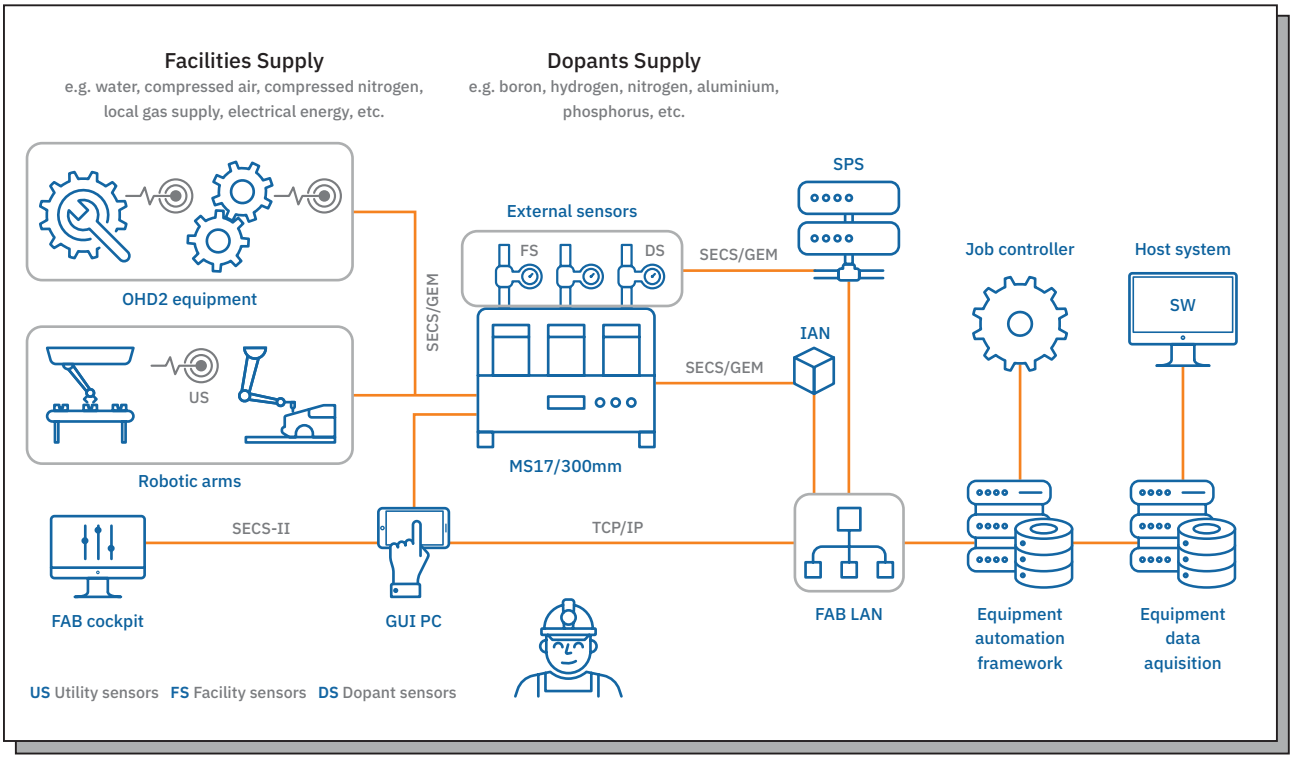


Figure 7: Infineon's Pilot Room Wafer fabrication unit

The environment for the conducted experiments is a silicon wafer production fabrication unit consisting of highly complex ion implant systems with assets of high vacuum system, high voltage components and mechanically moving parts. The connectivity model explores the areas where wireless technologies can potentially be implemented with the process systems under harsh industrial environments.

The current fab communication relies on RS-232/CANBus communication between the external sensors to the wafer production tool (MS-17) that has a SECS/GEM communication utilized in semi-conductor industries for communication between the Tool and Host. It also has a redundant path through a sensor-box that communicates to the host system through TCP/IP. Wireless connection is also established between the external sensors and the host system through a wireless adapter and a wireless gateway. The host system gets the information from the sensors and can transfer it to various clients, which might need to access this data. *Figure 8* gives an idea of the connectivity inside the manufacturing unit.
For the wireless prototype, LoRaWAN (Long Range Wide Area Network) is used. Long range and low power consumption are the main requirements considered to cater to the present-day large-scale industries.

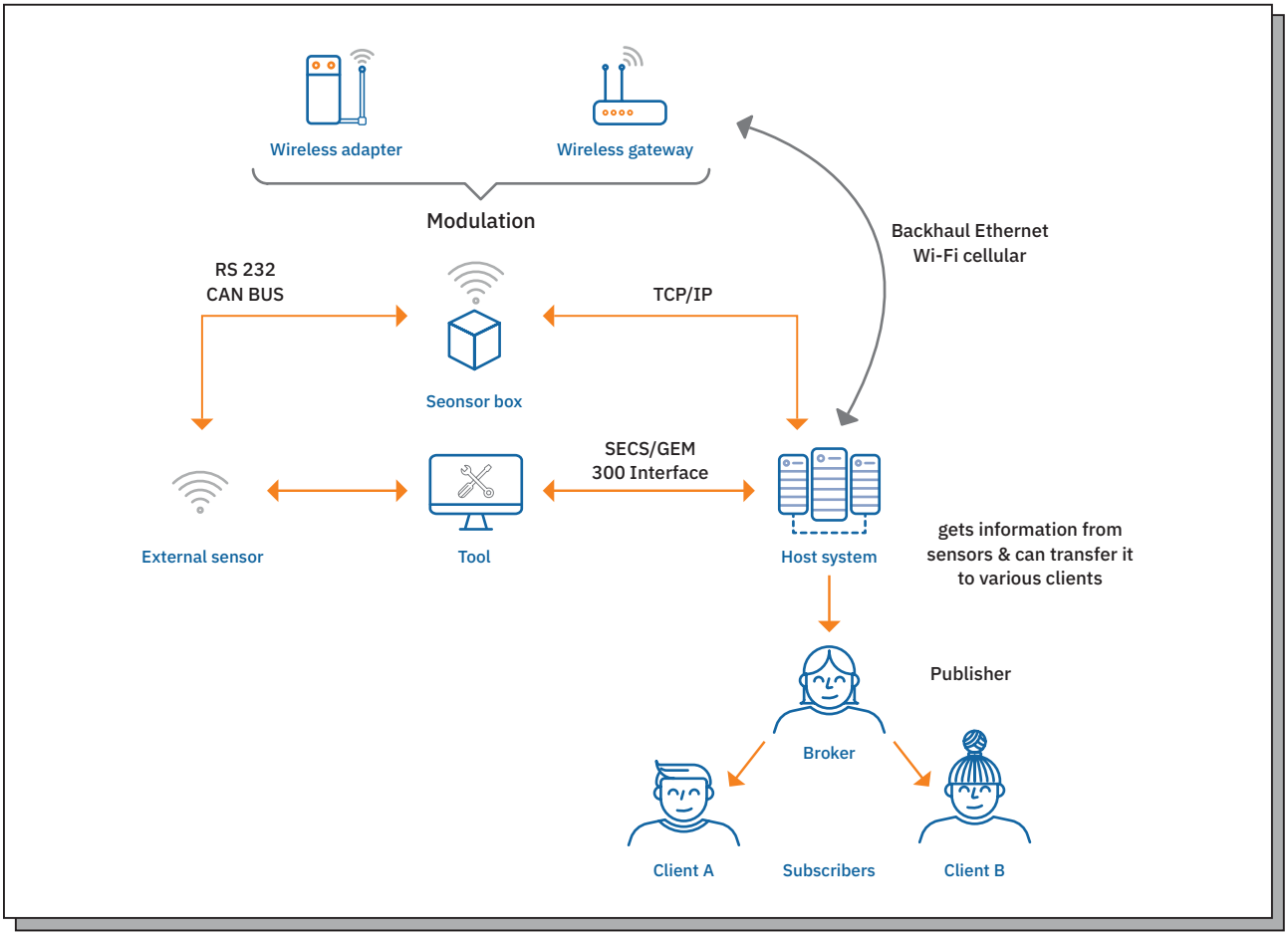


Figure 8: Wireless connectivity diagram inside the manufacturing unit

Low power wireless protocols like Long Range Wireless Area Network (LoRaWAN), SigFox and Wireless Highway Addressable Remote Transducer (HART) are currently used as a solution for wireless connectivity in advanced industrial setups. These requirements are a perfect fit for sensing, controlling, monitoring and are robust to harsh environments and electromagnetic interference (EMI). The technologies operating in frequencies of sub-GHz range provide maximum communication range, as frequency is inversely proportional to wavelength (f α1\λ). This develops the basic concept of LPWAN (Low Power Wide Area Network) devices operating in the sub-GHz range.

An overview of the LoRaWAN architecture is shown in *Figure 9*. The presented architecture includes three major components (i) End-nodes (Adapters) (ii) Gateways and (iii) Network servers. The communication is bi-directional (uplink and downlink). The end-nodes can communicate either wired/wirelessly to the adapter (LoRa Shield) that controls the processing logic and the data is communicated wirelessly to the network gateways. The communication up to this level is through LoRa RF modulation with a transmission frequency of 868-870 MHz. The gateway connects to the network servers through IP network and the data is forwarded via the Internet. The end-nodes can be controlled by the network servers with talkback (downlink) communication in downlink making the network completely bi-directional. The data can also be distributed from the gateway or network servers to authorized clients (API) to monitor and control the far-off end nodes. MQTT, as a lightweight application layer protocol, makes end-nodes as a publisher, a gateway or server as a broker and the authorized clients as subscribers to establish the communication.

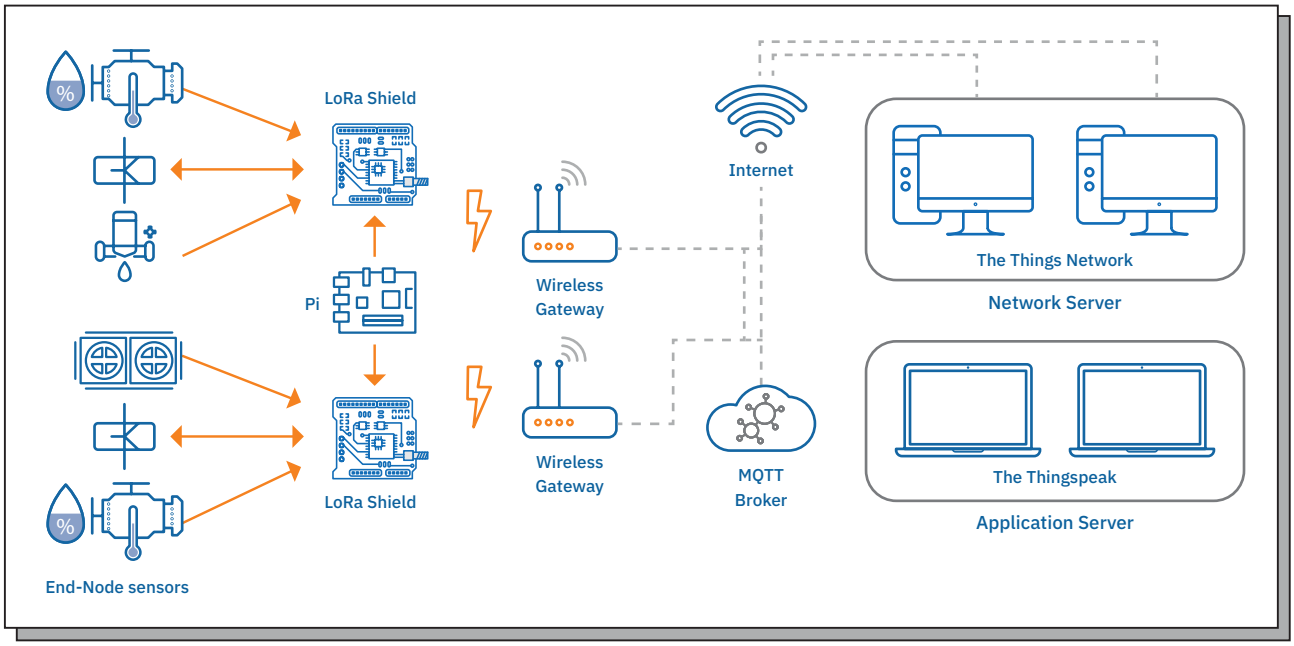


Figure 9: LoRaWAN Network Architecture

The wireless prototype is integrated into the existing fabrication unit in Infineon and the modified connectivity in the fabrication unit is shown in *Figure 10*.

The LoRaWAN solution provides secure communication in-built by Authentication and Encryption based on the AES-128 scheme and are 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.

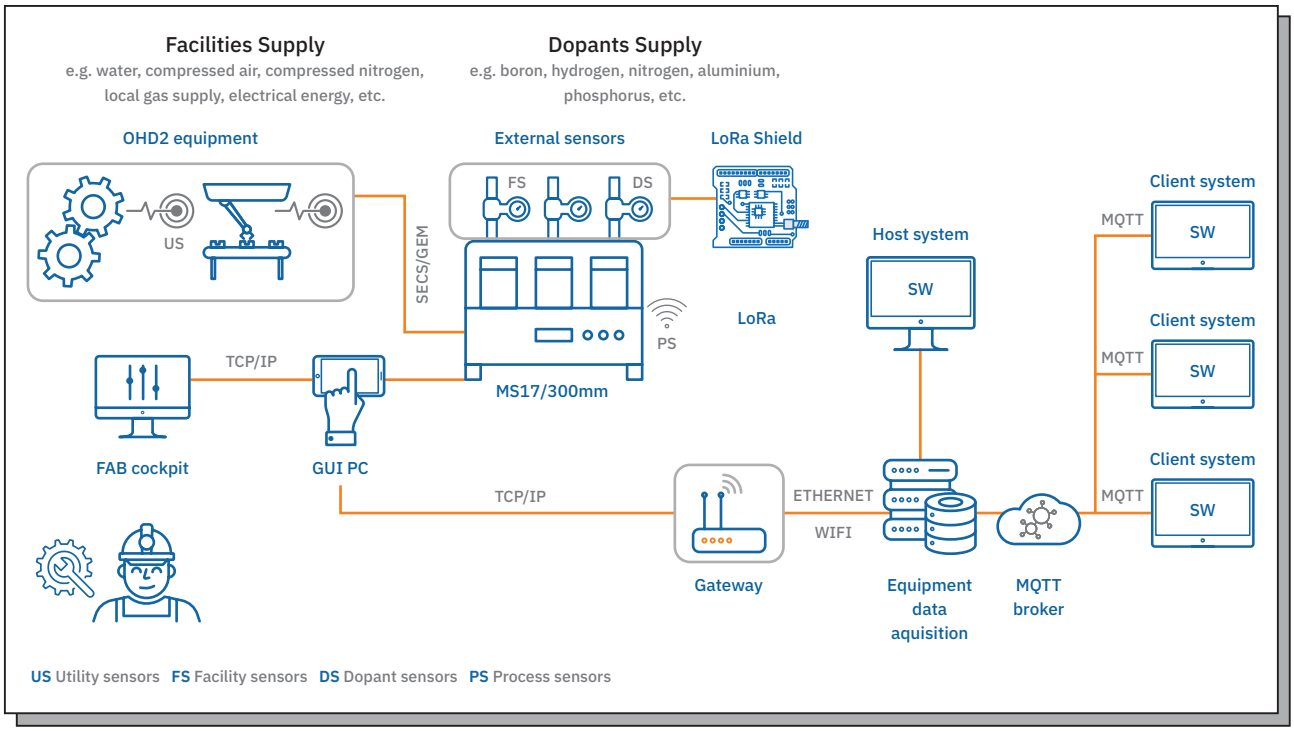


Figure 10: Modified fabrication unit with wireless connectivity

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

IoT4CPS has developed Security by Isolation (SBI) in the form of a special gateway and a suitable cloud service based on the requirements. The SBI-Box was designed in such a way that it is suitable for industrial use in SME as well as for large companies. In addition to the required new security aspects, the required safety aspects are also taken into account. The SBI-Box connects safety and security in one appliance.
The SBI-Boxes and the SBI-Cloud can be used for the isolation of the individual production cells as well as for the products of the manufacturer, which are in use worldwide.
The SBI-Firewall is characterized by the following key features:

- Safety traffic light
- Redundant system
- Virtual machine host
- Virtual switch and virtual firewalls
- Central profiting
- 4G/5G bypass
- Secure Boot System

In several iterations, the demonstrator of the SBI-Box was developed according to the requirements of different user groups from the industrial area. This process allowed important factors to be taken into account that justified the use of these devices for an increased security level.

The following factors are evaluated in different test beds:

- Fast and uncomplicated integration
- Easy maintenance and update of the system
- Global decentralized commissioning
- Central logging and monitoring
- Redundant system
- Individual single encryption, also for virtual machines and data containers
- Comprehensive logging and encrypted recording of remote access
- Full-automated exchange of systems in the event of failure by hardware suppliers
- Bypass internet connections through 3G–5G

The SBI-System is based on its own private cloud system, which can consist of several entry points (HUBS) and an administration system. These HUBs can be outsourced as virtual machines in company-specific server structures in the different destinations or outsourced to physical or virtual servers in data centers. The SBI-System can be expanded at any time during operation.

All SBI-Boxes connect to this SBI-Cloud via the closest / fastest HUB and are configured, monitored and updated centrally via the administration system. External users (service technicians, employees, product owners) also connect to the corresponding SBI gateway via this cloud. Every access is recorded and logged in encrypted form.

The SBI-System relies purely on Open Source components, eliminating administration costs. They can be configured redundantly and in different configurations (e.g. 5G). Thanks to the performant hardware, the gateways are able to host several virtual machines (e.g. Docker instances) and can also be securely integrated into the environment via virtual networks.

Remote access demands a valid certificate, an Open Source VPN client and a web browser. This constellation enables a secure connection to be established with any operating system and mobile device.
Future development ought to consider a transfer of the SBI-System into an open source-based industrial product. Different hardware components should be integrated into the SBI-Concept and the usability should be extremely simplified. As a result, the system is also affordable for small SMEs and a high-security standard can be introduced.

Simple provisioning of security roles and minimal, easy, worldwide administration are the targets of the SBI-System. Essentially, the connectivity of the SBI-Boxes in the private cloud system is to be improved with different systems. New technologies, 5G or LoRa are to be used and tested in different proof of concepts.

There is one crucial area with great potential for further research: ensuring a secure connection and protecting the SBI-System itself. The use of quantum encryption systems in the context of the SBI-System represents a secure alternative to the existing encryption systems. By expanding a quantum encryption system, the SBI-System could also be able to provide other communication connections with secure keys.

4.3. Communication from Manufacturing Plant to External Entities

In the course of the evaluation phase with users, different contact groups were collected, which should communicate more securely with systems or products produced using the SBI system:

- Manufacturer – Monitoring & Service
- Manufacturer – Upgrade Services (Life Cycle Management)
- External data storage
- Artificial Intelligence
- 3d party suppliers of subcomponents
- External service representatives who service on behalf of the manufacturer
- Product owner
- User of the product
- Content owner

To be able to assemble each product with unique software (e.g. BIOS, operating system, data, key, certificates) and explicit identifications, it is not enough to only focus on the hardware system that allows individual mass recordings. Also, the structures before (content collection, time of delivery of content, matching of data to semi-finished IoT products etc.) and after (validation of data, logging of recording but also of removal, matching during assembling, additional print material, distribution etc.) recording have to be taken into consideration. It is not about copying data to media (USB flash device etc.) any more when the output has to be individual.
These processes are considered in the advanced SBI flash recording demonstrator which allows flexible connection of several systems like manufacturing execution systems, document management systems or others and at the same time the automation of processes. The demonstrator is designed to transfer digital content from de-centrally located data sources into IoT products in a secure and customised way. It makes use of secure communication protocols, single encryption and quality control mechanism to take the recording of data carrier to a completely new level. Quality control mechanism avoids errors during production or in the matching of data to the products.

With the combination of different tools and methods like authentication, encryption, access control, remote access, validation and matching processes, high-level security is ensured:

- Production of the SBI-Box and secure recording of the flash media
- Mechanism to enable secure boot of the SBI-Box
- Personalised unique encryption by the means of product-specific indicators
- Personalised and secure token preparation for commercially available flash devices which enables secure access to the SBI VPN
- Explicit user identification
- Recording of USB flash drives for service technicians that can connect to the SBI-Hub with the corresponding certificate
- Data protection mechanism (for the whole life cycle of an IoT product)
- Secure remote management during and after recording processes

To secure data and keys not only on the USB flash device but also during production, the SBI flash recording demonstrator supports secure data transfer and communication. It also provides an authentication mechanism. Access during production is controlled and logging provides all relevant information to reconstruct recording processes. Product reliability and quality control mechanism are integrated and ensure error-free recording and assembling/distribution.

By setting up different demonstrators and workshops with users from the Industry 4.0 environment, the groups mentioned above were identified and taken into account in the system structure of the SBI-System. Each of the user groups requires different access to different areas of the system or the product.

In order to lower the possibility of attack, it is necessary to determine during the connection which user with which role connects to the system and which subsystems can be accessed at all. A new, centrally controlled firewall and routing concept make it possible to create different types of access for the different roles. The user and their role not only determine which subsystem they can connect to, but also define whether it is possible to intervene in the process or just get data visualized or transferred in one direction. For example, if using the SBI-System, an individual vehicle owner (e.g. vehicle) can use the cell phone to look at the display of the vehicle infotainment system using their smartphones or a workshop service technician can carry out updates to predefined subsystems when the vehicle is at a standstill (with maintenance mode activated) or read data from the vehicle subsystems.

All activities can be recorded in encrypted form via the SBI-System. Every direct interaction with the systems is logged and these records can be used in the event of a dispute. The log information can be encrypted so that only product owners and manufacturers can initiate decryption together. This guarantees a high level of protection for the product owner or the manufacturing employee.

Depending on the product and structure of the manufacturer, the access system must be individually adapted.

- Which concrete project results are used as an input to this work?
- How do they help solve the issue?
- Summary of the deliverables
- High level – no technical details
- Describe the solution
- The actual solution/application
- Possible future development – outlook:
- Use Case development (e.g. Autonomous Driving SAE 5)
- Technology development (e.g. 5G)
- Open/future research questions (e.g. post-quantum encryption)

REFERENCES

[1] IEEE 802.11p https://standards.ieee.org/standard/802_11p-2010.html

[2] "C-ITS by CAR 2 CAR Communications Consortium (C2C-CC)", https://www.car-2-car.org/

[3] "COMMISSION DELEGATED REGULATION (EU) supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems", March 13, 2019 https://ec.europa.eu/transport/sites/transport/files/legislation/c20191789.pdf

[4] "3GPP Release 14, 15, 16, 17" https://www.3gpp.org/specifications/releases/

ABBREVIATIONS

AD	Automated Driving
AI	Artificial Intelligence
API	Application Programmable Interface
DSRC	Dedicated Short Range Communications
EMI	ElectroMagnetic Interference
HART	Highway Addressable Remote Transducer
HSM	Hardware Security Moduls
ITS	Intelligent Transport System
IWSNs	Industrial Wireless Sensor Networks
LAN	Local Area Network
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
SBI	Security by Isolation
SME	Small Medium Enterprise
VPN	Virtual Private Network
V2I	Vehicle to Infrastructure Communication
V2P	Vehicle to Person
V2V	Vehicle to Vehicle Communication
V2X	Vehicle to All Other Communication

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

Layout & Grafik

Nora Novak, goldmaedchen Grafikdesign

Legal Notices

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