IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future

Project No. 863129

Deliverable D3.4

System architecture patterns for enabling multi-stakeholder trust provisioning during production and maintenance

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: System architecture patterns for enabling multi-stakeholder trust provisioning during production and maintenance
Type: Public
Editor(s): Leo Botler
E-mail: leo.happbotler@tugraz.at
Author(s): Leo Botler (ITI-TUG), Stefan Jaksic (AIT), Dari Trendafilov (JKU), Albert Treytl (DUK), Silvio Stern (XNET)
Doc ID: D3.4

Amendment History

Version	Date	Author	Description/Comments
V0.1	29.10.2019	Leo Botler	Initial version prepared + Secure and Trustable Localization
V0.2	15.11.2019	Albert Treytl	Application of watermarks for data authentication and provenance
V0.3	19.11.2019	Dari Trendafilov	Dependable Orientation
V0.4	19.11.2019	Silvio Stern	Security by Isolation
V0.5	19.11.2019	Albert Treytl	Application of watermarks for data authentication and provenance - updates
V0.6	4.12.2019	Leo Botler	Pre-final for review
V1.0	18.12.2019	Leo Botler	Final version

Legal Notices

The information in this document is subject to change without notice.

The Members of the IoT4CPS Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the IoT4CPS Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

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

Federal Ministry
Republic of Austria
Transport, Innovation
and Technology

FFG
Forschung wirkt.

Content

Abbreviations

CPS	Cyber Physical Systems
BLE	Bluetooth Low Energy
FD	Field Devices
SH	Stakeholder
MiM	Man-in-the-middle
PAn	Positioned Anchor
CA	Certification Authority
TLM	Trusted Localization Module
SCM	Secure Communication Module
DOM	Dependable Orientation Module
AP	Access Point
DWRL	Dual Wireless Radio Localization
I-DWRL	Improved Dual Wireless Radio Localization
E-SALDAT	Efficient Single-Anchor Localization with Dual Antennas Tags
UWB	Ultra-wideband
ToF	Time-of-Flight
RTT	Round Trip Time
AGV	Automated Guided Vehicle
SNR	Signal-to-Noise Ratio
WM	Watermarking
PA	Provisioning Agent
WMG	Watermarking Generator
REG	Registration
KM	Key Management
CS	Control System

Executive Summary

In Cyber Physical Systems, cooperation plays a critical role. The increasing amount of devices and people collaborating in a single task raises the attention towards security and increases the demand for engineering tools capable of building trust among different participants of processes. Those tools cannot be generally attached to a running process as a building block and are often required to be incorporated in applications from the design phase.

In this deliverable, we focus on developing architectural patterns that enable trust provisioning among different stakeholders, which collaborate on the same task, either in production or maintenance. A real use case scenario, which highlights such cooperation among different entities, constitutes the starting point of this deliverable. After outlining the scenario, it is analysed regarding potential vulnerabilities and threats which yield the architectural requirements for multi-stakeholder trust in the system. Building blocks are developed to address the identified vulnerabilities and satisfy the requirements. They are also combined with consolidated system architectural patterns. The building blocks concern secure means of localization and orientation, as well as secure communication. In the context of localization, a new localization approach featuring low infrastructure and energy costs is outlined. In the next step, the orientation dimension is integrated in order to complement the localization block. For secure communication, a twofold approach is presented, which concerns secure communication among constrained devices as well as securing information among different stakeholders. For efficient secure communication among constrained devices, a Watermarking approach is presented since cryptographic primitives are not always an option. Simultaneously, the security among different stakeholders is established via security by isolation.

1. Introduction

This deliverable deals with architectural patterns and building blocks that are enabling close cooperation among different stakeholders during production and maintenance. Resulting from a joint effort of task 3.2 of IoT4CPS, the involved partners demonstrate their activities mainly related to hardware and software concepts for improving system resilience and hardware with inbuilt security properties and support. This document highlights threats that should be considered when designing cooperative IoT systems. In addition, the document outlines architectural patterns which allow addressing the identified threats in an efficient way, factoring in the resource and computing constraints, which are usually associated with industrial CPS and IoT scenarios. The resulting building blocks addressing reliability, integrity and maintainability for CPS are detailed and outlined in the context of the central use case described next.

1.1Use Case: Multi-Stakeholder Trust in CPS

Cyber Physical Systems in Industry 4.0 usually span across different domains, sub-systems and stakeholders and are relying on the cooperation and interaction of different entities. Naturally, this requires mechanisms of trust provisioning, to ensure the integrity of the system as a whole as well as its participating entities. This especially holds in the context of production and maintenance, where the interaction of different entities (e.g., device, third party service personnel, system operator) is required while protecting the rights of the involved parties among each other and ensuring the integrity and security of the whole system, against external attacks and interferences. In the context of this deliverable, a scenario regarding updating and servicing an industrial IoT system was developed in accordance with the requirements prescribed by the industrial partners of the project. The scenario reflects a majority of the challenges/vulnerabilities usually associated with such a process and allows us to assess the requirements to satisfy the use case. The resulting requirements are mapped to architectural patterns, which are combined to a general modular architecture. This allows to address the identified trust-related issues within the discussed use case and ensures that the architecture can be enhanced with additional building blocks (stemming from additional requirements of different use cases) in the future. For the identified building blocks, reference technologies which were developed in the course of IoT4CPS are outlined in detail.

1.1.1 Over-The-Air Configuration and maintenance of Automation Modules

As outlined above, IoT-enabled Cyber Physical Systems usually entail the interaction of different entities associated with or operated by different stakeholders. Such interactions demand mechanisms that ensure trust among all involved entities. Consider the configuration and installation of automation modules. Traditionally this process is very time consuming as the right devices/firmware/configuration have to be selected and a technician visits a production line to mount the respective device, put it into operation and perform final configurations. In addition, the parties involved in the process are not necessarily all stemming from the same stakeholders and such a process could involve the device manufacturer, the operator of the production line, as well as a third party technical contractor that takes over the installation/configuration process.

To ease the process a system could be devised, which supports the setup of modules on the production site and automates as much of the underlying configuration process as possible. The system allows the operator of the production line to issue the installation of specific modules at certain locations in the production line. These orders are forwarded to a technician (third party contractor) as requests (e.g., using a dedicated app on their mobile phone). If a technician accepts an order, they will in a first step select appropriate modules, which are required for the order and notify the system (e.g., by scanning module-specific QR codes, or other unique identifiers) of the selected modules. Based on the module information the system will select specific firmware for the modules and generate pre-configurations which are made available to the technician during the installation of the modules. The technician will now install the modules at the prespecified locations in the production line, with the system guiding them to the locations and providing them with module-specific firmware and pre-configuration. Installation and configuration are performed by connecting the third-party technician’s dedicated mobile device to the automation modules (e.g., via BLE) and transmitting firmware and configuration data to the module. After a successful setup (and before the module is integrated into the automation network), the mobile device acts as a proxy between production line backend and automation module to finalize parameterization and tests, i.e., connecting it to and integrating it in the automation network. Once the setup is complete and the automation module is successfully integrated into the overall production line, the order is completed. A sketch of the system’s architecture is shown in Figure 1.

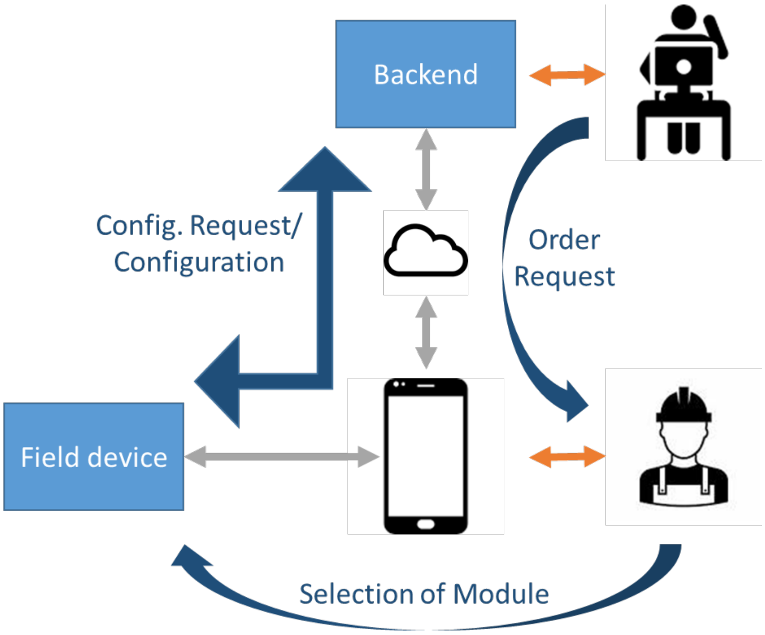


Figure 1: Illustration of the use case.

1.2 Trust among entities, attack scenarios and threats

The presented use-case involves two main stakeholders (however, additional stakeholders can be easily added), the owner (operator) of the production line as well as a third-party contractor/technician. The system requires multi-stakeholder trust provisioning in order to prevent the contractor from obtaining confidential information (e.g., regarding configuration/ firmware or applications) she is not authorized to access. This requirement intensifies when the automation device manufacturer becomes a stakeholder in the process. While gaining information on their currently operating devices will allow a device manufacturer to implement novel services (such as predictive maintenance) and improve future products, it must be ensured that the customer's data and information (present on the automation devices) is not leaked to the outside. In addition, a manufacturer's access must be limited to their own devices (and therein only to limited information). Besides preserving confidentiality among the different stakeholder's, trust mechanisms are required, which ensure that all steps taken during a set-up process (e.g., modules selected, location of installation) are documented and validated and verified along the way, to prevent the cascading of faults and allow an analysis.

Differently from Deliverable D4.1, which deals with the security in Ethernet-based networks, our focus here is to secure and build trust among stakeholders in industrial environments, where wireless technologies are replacing their wired counterparts at a fast pace. Still, the threats that we identified in this section can also be found in the threat model list (with 330 items), which was previously described in D4.1 and D5.4.1, and used as a reference in the context of this deliverable. When comparing the identified vulnerabilities with the threat models established previously, it can also be seen that the threats within this deliverable were identified at a higher level. This is due to the fact that here we try to identify the weaknesses regarding a certain system without having specific components for its realization in mind, while the previous work has aimed for the analysis and protection of a specific application, i.e. *Device.Connect*. Thus, the approach taken here is generic by design to keep it applicable in the context of different industrial systems. Likewise, our threat model applies to industrial systems, such as the use-case contemplated in this section.

For reference purposes, we specify the mapping between the current threats and the extended threat list alongside each item in the list. The following list outlines the vulnerabilities which need to be addressed in the design of the system:

- Malicious or accidental access to confidential information of other involved stakeholders – inspired by threat 135 of the *Device.Connect* threat model, which deals with unauthorized access to privacy-relevant information within a vehicle;
- Attacks on the ICT infrastructure (spoofing, a man-in-themiddle attack) - closely related to threat 317 of the *Device.Connect* threat model, which deals with attacks on infrastructure where the *Smarthub* is used as a means to propagate an attack;
- Wrong integration of the automation device in the production environment (e.g., not at the location where it is required) – strongly related to threat 8 of the *Device.Connect* threat model, which deals with misconfiguration/erroneous use and accounts for the human factor;
- Wrong (malicious or accidental) configuration of the automation device – inspired by threat 203 of the *Device.Connect* threat model, which deals with spoofing of the source data configuration file;
- Attacks on the setup process (e.g., spoofing the location, identity etc. of a field device) – inspired by threat 238 of the *Device.Connect* threat model, which deals with identity fraud, where manipulation of the vehicle data is possible by setup.

All of the previously listed vulnerabilities may have a strong impact on a system. Depending on several factors such as specific applications and countermeasures adopted in parallel, the responsible person for the system may classify one or more items with lower impact according to the probability and applicability of the attack to the specific use case. An analysis of the probability of each attack/manifestation of vulnerability is extremely dependent on the application scenario and will not be contemplated here.

1.3Requirements

The vulnerabilities, which were identified in the previous section, can be used to infer key requirements for the target architecture.

In order to shield the system against cyber-attacks, i.e., attacks on the ICT infrastructure itself as well as attacks on the setup process and unauthorized access to production data from outside, the system as a whole must be secured against cyber-attacks. This entails the backend, the involved field devices as well as the application and device used by the third-party contractors and the communication networks that interface between those entities.

With the aim of maintaining the confidentiality among the stakeholders involved in the process, information which is not part of the setup process (e.g., production data) must be secured against being made available to other stakeholders participating in the process. This may even include configuration parameters that the third-party employee should not have access to.

The configuration and location of an automation device to be installed must not be changeable by anyone except the operator. In addition, the correct location, arrangement and installation of a device must be performed in accordance with the specified (untampered) setup and validated towards device operators.

The steps taken during installation must be stored/registered in a secure manner, to be made available (e.g., in form of logs) when the steps that are taken during an installation process need to be retraced.

From these requirements, three aspects can be immediately incorporated in the architecture, namely, private and secure communication, trusted localization and trusted orientation.

1.4Architecture patterns for enabling multi-stakeholder trust provisioning

In the next step, the system requirements, which were established in the previous section are exploited for a definition of a modular architecture. The requirements can be clustered in two areas securing communication (i.e., securing confidentiality among stakeholders and securing the authenticity of messages/information) and the secure contextualization of a device in an environment (via secure and dependable localization and orientation techniques).

The developed architecture comprises a basic module which connects different field devices to different stakeholders as illustrated in Figure 2. Within this module, there is a Contextualization Module (CM) and a Secure Communication Module (SCM), with roles as described previously. The Contextualization module comprises two sub-modules, which are responsible for providing trusted localization (TLM) and trusted orientation information (TOM). The Secure Communication module comprises two sub-modules, namely Security by Isolation (SBI) and Watermarking (WM). Each of these modules will be detailed in a dedicated section, which also describes its basic sub-modules/components.

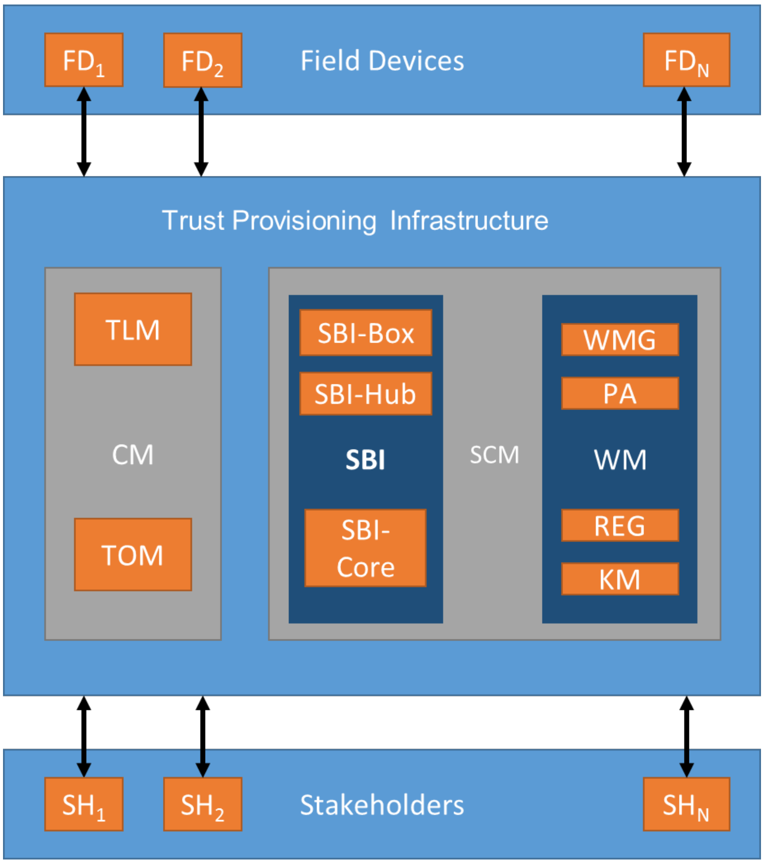


Figure 2: Architecture diagram for trust provisioning among different stakeholders.

2. Secure Communication

2.1 Security by Isolation

Trust is a very important component in the relationship between the customer and the manufacturer in the digitalization era. The manufacturer of digital components may have contact with sensitive data. It must therefore always be ensured that the customer's data does not reach the outside and the manufacturer of a device must never be given access to the customer's entire network, but only to their own devices. It is crucial to apply measures that build trust at all stages of the product lifecycle, from its planning phase through to its usage (see WP3 D3.2 and D3.3). This section focuses on how to address these issues, namely malicious or accidental access to confidential information of other involved stakeholders and wrong configuration of the automation device, described in section 1.2.

IoT is increasingly finding its way into the industry. Devices communicate with each other, collect data and analyze it, forming Digital Twins (WP5 T5.5). This involves the great danger that an organization can only survive if cooperating with partners that are trustworthy. Attacks on the systems are increasing year by year. This is also confirmed by the annual report of CERT 2018 ([CERT18], see **Error! Reference source not found.**). These dangers can only be dealt with by suitable procedures, such as Security by Isolation. Implementing such techniques requires external support for SMEs and startups. They need trustworthy partners

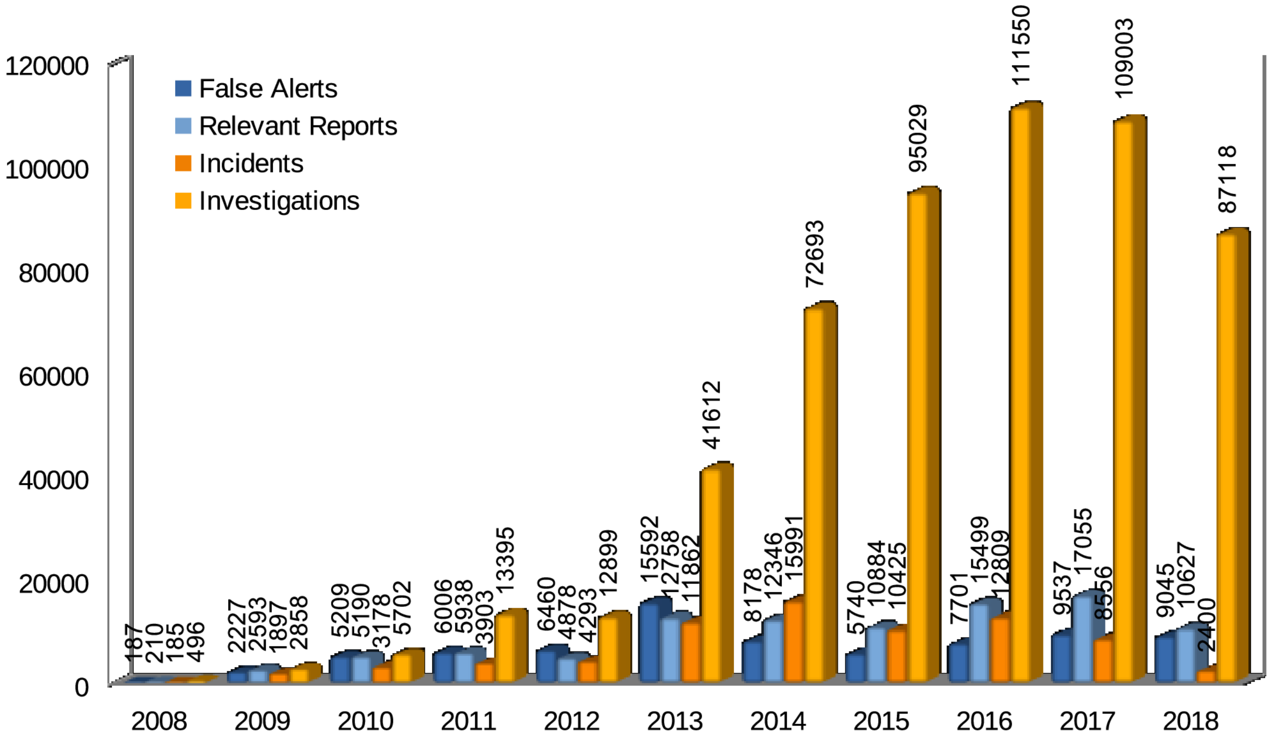


Figure 3: Threat forms over Time 2008 – 2018

to help them build a secure infrastructure. For this to occur, a firm relationship of trust must be established.

Transparency is an additional characteristic that increases confidence in manufacturers. All manufacturers' actions should be comprehensible for the customer. Traceability of the manufacturer takes place through several measures and over the entire process. From the initial design, implementation, delivery, support, maintenance, to the end of the device lifecycle, this must be guaranteed (see WP5 D5.5.1 and D5.5.2, T5.3). Additional transparency is created by open-sourcing both software and hardware, such that the customer can understand exactly what happens to collected data, because an evaluation of the data is important for both the customer and partially also for the device manufacturer.

In addition, the communication between manufacturer and customer should work well and be clearly defined as to when communication must take place, so that trust in one another is always on a solid ground. This is especially true when actions require intervening in the existing and well-functioning system and performing changes, such as configuration updates.

2.1.1 Concept of SBI

Security by isolation is a measure with which an industrial network can be secured (WP3 T3.1 T3.2). The goal here is to isolate all components in a virtual network in such a way that their communication is restricted to authorized partners and no access is possible to areas for which they are not authorized. However, the concept must be applied consistently. If the network is to be extended, the new components must be scrutinized in order to determine if they could compromise the system security and hence, if they are suitable for integration.

There are a number of basic conditions that must be met for the concept presented below, which can build trust between the individual stakeholders. The concept is based on Security by Isolation (SBI), a system that consists of several technical components and is part of this research project. Only through the smooth interaction of these components does such a concept work. All communication between the components must be via encrypted channels, which use the highest encryption levels currently available (e.g., AES-256) as recommended by the German Federal Office for Information Security [BSITR02102] (see also WP3 D3.5 T3.3), so that it is not possible to interfere with the data.

The security by isolation process presented here is based on the 4-component SBI-Core, SBI-Hubs, SBI-Boxes and technicians. An overview of the system can be seen in Figure 4.

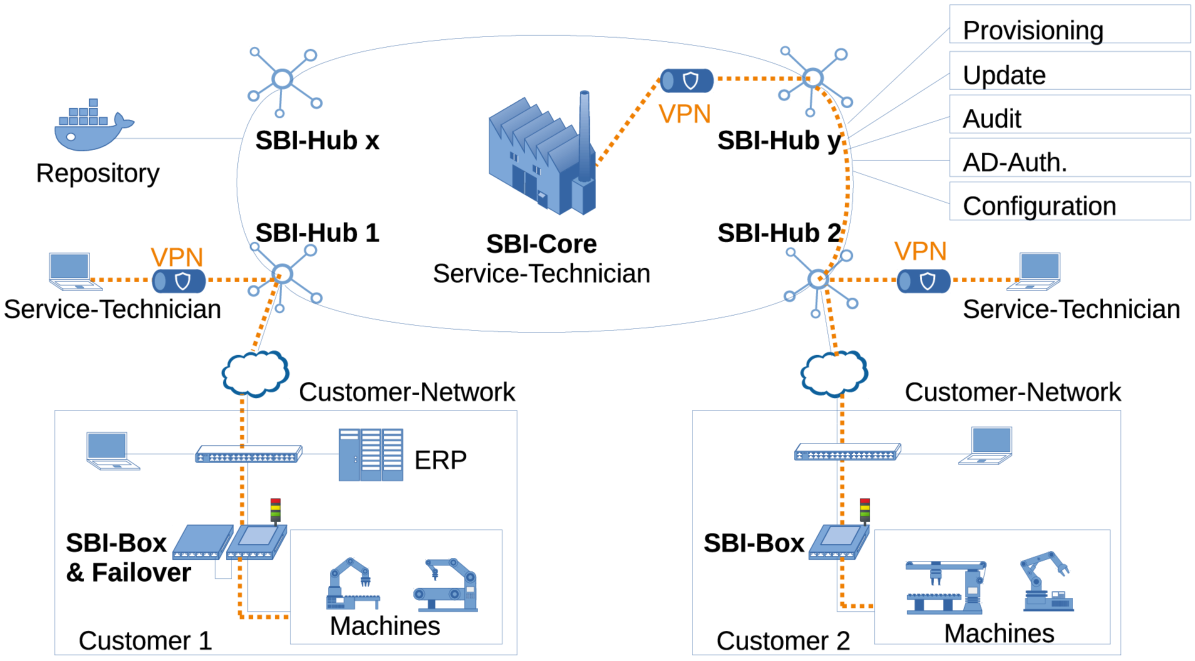


Figure 4: Overview of the SBI-Concept

The SBI-Core is a central database that manages customers, SBI-Hubs, SBI-Boxes, technicians, machines, audit-logs, firewall templates and rules and more. The main roles of the SBI-Core are the management of the certificates of the involved actors (SBI-Boxes, SBI-Hubs, technicians) and only via the SBI-Core settings and configurations take place and never directly at a device.

Worldwide SBI-Hubs are the next components, which allow device-to-SBI-Core or technician-to-device connectivity. The SBI-Hubs are the interfaces and thus the agents of communication. All connections of the provisioning and maintaining are running over them. Because the SBI-Hubs are networked together, even with the failure of one or more SBI-Hubs, it is still ensured that a secure connection between the individual components of the SBI-Concept is possible (see Figure 5). The SBI-Hubs are also responsible for creating audit logs when external access is made to an SBI-Box and thus to a machine network.

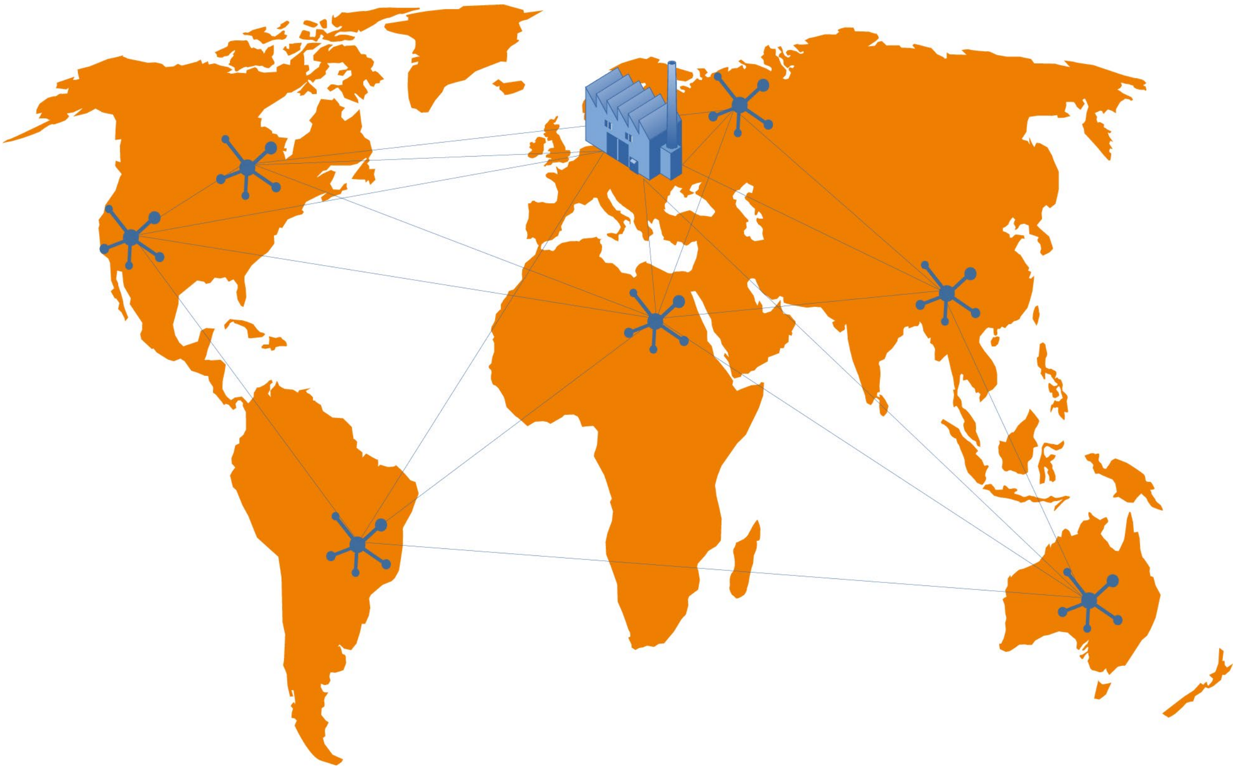


Figure 5: SBI-Hubs are redundantly working together

Of course, the device belongs to the components of the whole system. It is important that the device builds only connections to the outside via the SBI-Hubs to the SBI-Core through an encrypted channel.

A key role in the SBI-Concept is taken up by the SBI-Boxes. They form the element that stands at the customer's site. The SBI-Box is the link in the customer network to the machines and has several tasks. The status of the SBI-Box is indicated by a traffic light. It is also possible to detect at any time whether a connection to the outside is active or even a technician is currently operating a machine in the network.

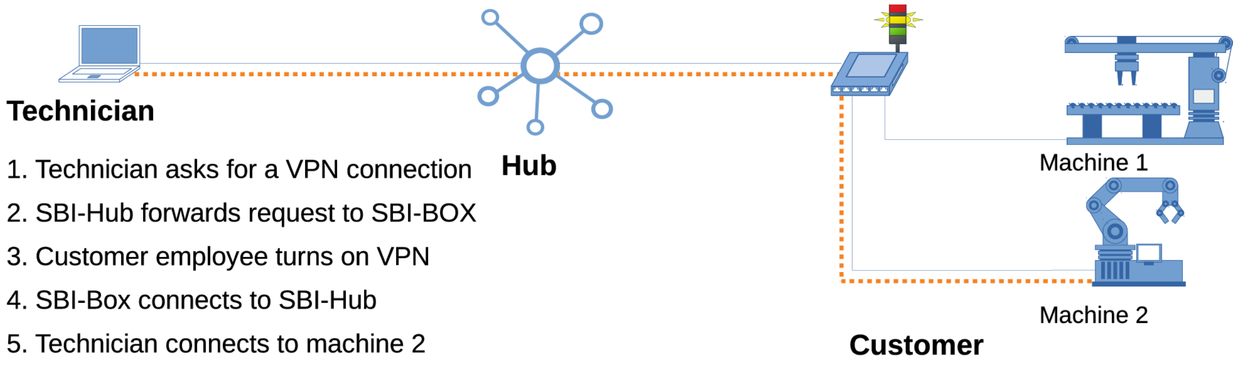
In standard mode, it is a firewall that allows only certain connections in the network. The entire machine network behind is divided into virtual LANs. Machines or machine components can only be accessed via the SBI-Box.

It is also the task of the SBI-Box to collect data for a digital twin (WP5 D5.2 T5.4 T5.5). One has to consider two interested parties: the customer and the manudacturer. Once the usage data are of interest to the customer, on the other hand, there is data, e.g., accesses or attacks that interest the manufacturer of the SBI-Box. To recognize more attacks the tools of WP4 or an intrusion detection system (e.g., OPNSense) should be installed on the SBI-Box.

Another task is the function of the gateway to enable provisioning and remote maintenance of machines in the network. For this purpose, a VPN connection is enabled, but must be actively released by the customer through a switch on the SBI-Box or through a special customer user interface. The customer is also able to interrupt this connection at any time.

Another important measure is the redundancy of the SBI-Boxes. The system is designed so that the customer network is interrupted as little as possible by a malfunction in an SBI-Box. The redundancy principle is utilized for this purpose: there is a second redundant box connected via a heartbeat line to the actual SBI-Box. If the SBI-Box fails, this so-called failover box takes over the task of the SBI-Box within a few seconds and thus maintains the network. Almost simultaneously, the SBI-Core learns of the failure of the SBI-Box. The actions that follow are described in section 5.3.

The last entity is the technician, who can also connect only via the SBI-Hubs, using an encrypted channel (see orange line in Figure 6) to the SBI-Core or the individual devices. In addition, all components identify themselves with unique certificates.



1. Technician asks for a VPN connection
2. SBI-Hub forwards request to SBI-BOX
3. Customer employee turns on VPN
4. SBI-Box connects to SBI-Hub
5. Technician connects to machine 2

Figure 6: Connection of a Technician only with the knowledge of the customer

A very important point to build trust is the traceability of work steps. This includes capturing every action between each component in a fixed audit log, starting at the birth of the device until the end of its life-cycle At any time, the customer can view the audit logs that concern them and thus understand which actions took place when and where. Such actions may be Updates, Maintaining, access by technicians and many more. In addition, one could even document the actions of a technician through a video recording and store it in the system.

2.1.2 Installation of further components

The precautionary measures are not demanded only from the manufacturers. The customers themselves must also comply with the set rules, or else the provided system protection is jeopardised. Thus, the customer may not install any unauthorized components in the network, as they could endanger the security. Third-party machines must either have their own integration system or they must also be accessible through the manufacturer's security system. This works through firewall chains, which ensure that one can only connect to the third-party machine via the SBI-Box.

2.1.3 Replacement of a component

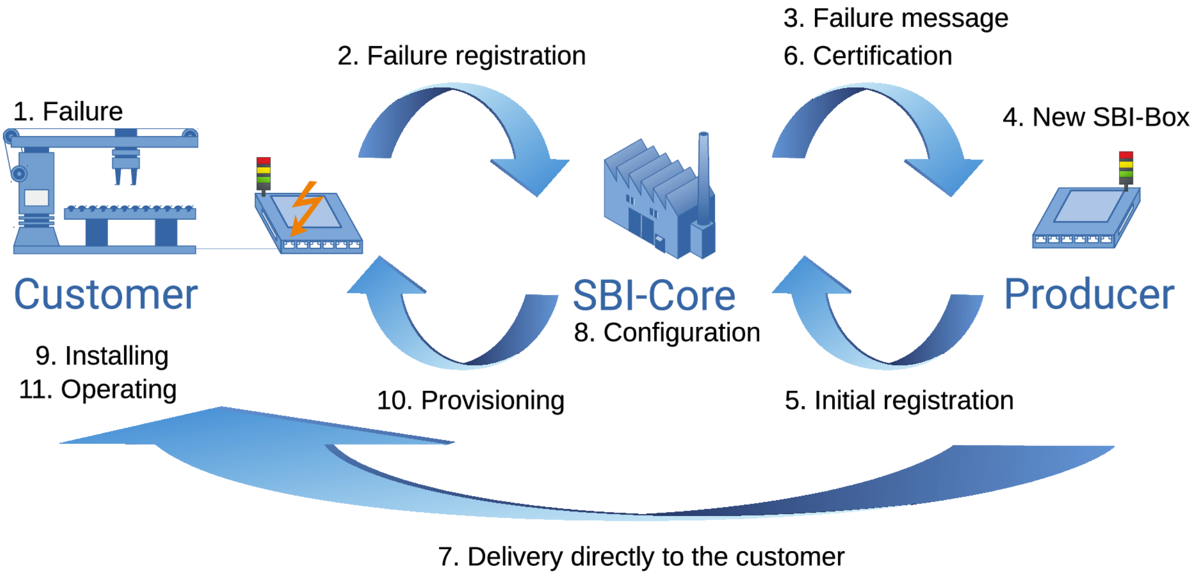


Figure 7: A safe way to replace a defective SBI-Box

If there is a need to replace an SBI-Box due to a defect at the customer side (1), then a schedule is automatically set in motion in which several stakeholders are involved (see Figure 7, WP5 T5.3). The registration of an error (2) is automatically detected, e.g., because the SBI-Box did not connect to the SBI-Core at a certain interval as planned or because a failure was reported directly by the SBI-Box or by the customer.

After receipt of the failure message (3) at the manufacturer, a new identical SBI-Box (4) is recorded in the SBI-Core (5) and assigned to the subsequent customer. The new SBI-Box receives a unique certification (6) and can be delivered directly to the customer afterwards (7). This ensures that no third parties have access to the SBI-Box before it is with the customer.

At the same time as the delivery logistics, the SBI-Box is configured in the SBI-Core (8). In the case of replacement of the defective SBI-Box, the complete configuration of the defective SBI-Box is simply assigned to the new SBI-Box.

Upon the arrival of the replacement SBI-Box at the customer's site, it may be installed by a technical staff who do not necessarily have to be the manufacturer technicians (9). Once the SBI-Box is installed on the site, it first connects to the SBI-Core (LAN, WLAN, mobile network) to get its configuration (10), and after it is installed and the configuration has been activated, it is ready for use again (11).

At no time does a third party have access to the configuration of the SBI-Box, since all processes are executed automatically and only encrypted. Thus, the configuration could not be changed on the way to the SBI-Box.

2.1.4 Discussion

To build a relationship of trust among the various stakeholders, all components and participants must work together. The foundations for trust in the form of a functioning and secure system must be laid by the IT company. It is important that the future user, i.e., the customer, is involved in the development process. It is only then that they develop an understanding of the technology in use.

It is also the responsibility of the customer not to make careless interventions in the system without considering the consequences.

2.2 Application of watermarks for data authentication and provenance

For industrial data, a special focus is on the authentication and data provenance of data delivered from field level (sensor) networks. These data and the respective networks are characterized by small data volume and strong constraints in terms of available bandwidth and computational resources and might also have the necessity of data aggregation and sensor data fusion.

Conventional cryptography might suffer from limited computational resources in field devices and from limited bandwidth, packet size and resulting energy constraints in wireless networks. Watermarks can be an alternative lightweight security measure ensuring authenticity and data ownership and therefore increasing trust, which simplifies applications and in particular without additional data volume as required by message authentication codes or digital signature.

This section describes a solution to attacks on ICT infrastructures, described in section 1.2.

2.2.1 Data taxonomy

Digital watermarking is a technique used for many years in the protection of multimedia content. For these applications, limitations in human perception are used to hide information in host data. The limiting factor for the strength of the watermark is its visibility concerning a human consumer i.e., the human user of the data sees a different image compared to the processing hardware, which of course sees the watermark.

In the context of IoT4CPS, the main focus is on machine-to-machine communication, which requires to change this definition of “visibility” since there are no limitations in perception by the machine. For machine-to-machine communication, the marked data should be accepted as valid data and the changes in data should not affect the operation of the system using the data or have negligible effect.

When talking about typical communication in industrial environments in general and data generated by sensors in particular, the following data types can be distinguished:

- Sequence data: This data is defined by an ordered list of items and can be subdivided in time series or symbolic sequences. Whereas the first one is characterized by equal time-intervals or following a special gap pattern, the latter is bound by a logical order between the symbols defined by the application, e.g., the sequence of messages defined in a protocol.

- Spatial data: This data type includes points, polylines, polygons and grids, which can additionally contain a number of non-spatial attributes. The dependencies are defined by the spatial context of the different items, which in general is location dependent.
    - Spatiotemporal data are an extension of spatial data and form multidimensional trajectories consisting of an ordered list of time-location pairs. In comparison to spatial data, the time dependency links the list items stronger and reduces the sparse redundancies in data, i.e., the trajectory of an AGV (automated guided vehicle) allows only a limited change of position between two consecutive readings.
    - General streaming data is an infinite sequence of data that is unstructured. Typical examples are data generated by sensors and sensor networks. Often this kind of data is overlayed by a sliding window for retrieving the data relevant for the watermark process. It is important that these data contain important features that can be used for embedding watermarks.

Since watermarks add or change the original host information, two types of data have to be distinguished to determine the kind of application:

- Noisy data: This data can embed a watermark in the noisy part of the sensor data by, e.g., altering the least significant bits of a sensor value. As long as the watermark does not exceed an acceptable level of distortion defined by the application, the watermark is invisible and causes no disturbance in the application. Measures to determine the level of distortion are SNR or PSNR (Peak Signal to Noise Ratio). Examples for such signals are temperature sensors, rotation speeds, or pressure values, containing natural noise, the application needs to be able to cope with.
- Noise-free data: Examples of these data might be control commands, binary sensor values (machine on/off) or sensor values cleared from noise. Here, changing a single bit will cause the data to become invalid or change its meaning significantly. For this data, the watermark needs to be encoded in a side-channel since no alteration of data is acceptable.

Particular decisions have to be taken for the actual sensor value used.

2.2.2 Structure of the watermarking system

To ensure authenticity and data ownership, a watermark system contains the following elements (see Figure 8):

1. Encoder or embedder, which creates the marked data (WMD): it applies a function f(HD, M, K) to the original or host data (HD) embedding a message (M) that is transported by the watermark. Using a secret key (K) will enable security.

2. A communication channel that can alter the signal either due to legitimate data processing (e.g., data aggregation or sensor fusion) or due to an attack as long as the

watermark is still detectable. The robustness of a watermark defines the amount of acceptable change.

3. A Decoder or detector, which detects the watermark and retrieves the message from the marked data. The detector is a function g(WMD,K) of the marked data and the secret key.

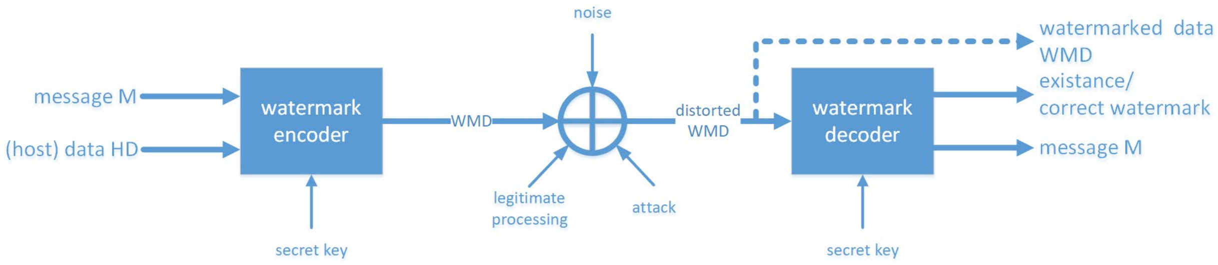


Figure 8: Components of a watermark system

The advantage of using watermarks is that they are integrated into the data, i.e., 1) they do not require additional storage, bandwidth or resources, 2) they are inherently attached to the data and 3) the watermark is (to a certain extent) preserved during legitimate operation.

By enriching data with hidden meta-information the level of trustworthiness can be increased. When using watermarks with non-media data the following properties have to be considered specifically:

- Invisibility: The invisibility of data in the classic sense is mainly defined by the noise level (negligible information) in data. For sensor networks, the amount of noise is usually reduced to a minimum to achieve efficient data transmission and avoid the transmission of redundant data. For the implementation, it is extremely important that the marked data can be processed as non-marked data and the meaning of data is not (significantly) changed. This is application dependent. In many cases, data even does not contain any noise such as in coordinates, binary values such as counters or status indicators. The definition of invisibility therefore heavily depends on the application, the used data and the adversary. It is also possible that watermarks are embedded in the side channels such as the timing of a packet or the packet header. Such meta-information can be used in sensor networks. Although the classical definition of watermarks is demanding an integration in the host data, for sensor networks these data are usually also tightly linked to the host data or can be seen as the actual host data.
- Robustness against data manipulation: Like in multimedia applications the robustness is defined as resilience against operations performed on the data. Comparing both areas, the operations differ to a large extent. Multi-media operations are rather complex but limited in number (compression, cropping or change of resolution). Operations on sensor

data are comparably simpler (summarization, sampling, data reduction), yet are in general characterized by a high data reduction rate. Robustness and security are very similar properties in the respect that they are damaging the watermark.

- Capacity: the amount of data that needs to be transported via the watermark is a trade-off with the other properties for visibility, robustness and depends on the amount of redundant host data. That is, sensor data only contains a small amount of data and therefore a small capacity is favourable to be able to steer the other properties. For the application of authentication and data provenance protection only a small amount of data (e.g., an ID) or even a zero-bit-watermark only allowing to check the presence of the watermark is preferable and for most applications sufficient.

Typical classifications for watermarking functions are:

- Additive (e.g., LSB addition)
- Multiplicative (e.g., image watermarking in the magnitude-of-DFT domain)
- Quantization (e.g., Quantization Index Modulation)
- Spatial domain/frequency operations (e.g., Spread Spectrum techniques or Random number sampling/coding)

2.2.3 Protection by a watermarking system

The purpose of the watermarking system is to detect alterations in data and to prove the provenance of sensor data.

To meet these goals a fragile watermark is required to detect alterations of data. That is, the watermark should not be detectable or the message should not be retrievable after the alteration. For all end-to-end communication, this approach is feasible and will protect system security.

Yet, for the IoT4CPS environment, data alterations such as summarization or averaging might also be considered at data concentrators or processing nodes in the sensor network. This case of data processing during transmission requires a trade-off towards more robust watermarks that can be detected even after certain alterations need to be done. This, in particular, applies to side-channel watermarks, since they are inherently processed in the network by changing headers or influencing timing at forwarding or routing nodes.

2.2.4 Authentication of data streaming

After selection of a synchronization point, the data stream is divided into blocks. A chain watermark is formed by calculating the hashes of two blocks and storing them in the LSBs of one or two blocks of the group. This algorithm should be used in forward-chaining to reduce the required computational and storage resources. This algorithm has various advantages:

Using LSB, the watermark stays invisible to common operations and has the same length as the data that forms the basis of the watermark. It is robust against insertion, deletion and modification of data elements. The security lies in the secrecy of the keys used for determining the synchronization point and the keyed hash function used for watermark generation. Adding a timestamp or sequence number can further prevent replay attacks.

2.2.5 Provenance encoding of data streaming:

Self-identifying technique [CSV10]: >3 LSB required in data that can be sensor errors; applicable to (signed) integer and float and low entropy data. The scheme is resilient to sampling, rounding and truncation. Blind watermarking schemes are used for sender identification, whereas non-blind watermarking schemes are facilitated for receiver identification, i.e., to check if the received data is intended for a station.

Another possibility to encode data provenance is to add a watermark to the inter-packet delay encoding as suggested by [SSB13] or [HKB09]. Schemes for aggregation of watermarks at data concentrators are available to prove the aggregated data provenance. Utmost transparency is offered since the mark is not embedded in the host data, but in a side channel. In general, sensor networks, the delays inserted are also below the natural network jitter and therefore also resistant to traffic analysis. Yet, to associate data and timing information for each block of data, a message authentication code (MAC) is calculated. Security can be improved if the watermark is not transmitted sequentially but in an order that is defined by a separate hash value of a second secret key.

Modification of packet timings or other traffic-flow parameters and embedding a watermark in this side-channel has been used for retrieving the data origin even if anonymizer networks have been used. Traffic patterns are matched between different channels to retrieve the source. This research has been primarily used for attacking anonymous communication.

2.2.6 Secret message transfer

Although not considered in this context, watermarks' capability to transport hidden messages can also be used. [A15] suggests using beacon information in Vehicle Ad Hoc Networks (V2V) to hide information for lawful interception. This system uses the highly noisy signals for position, speed or heading transmitted in the beacon to hide messages to transmit notifications about unlawful behaviour. The main target of using the frequent beacon signals is to prevent other participants to identify misbehaving vehicles by hiding the information.

2.2.7 Integrity protection of small data sequences or queries

Watermarks applied to data streams or sequenced data require a certain amount of data or data items for side-channel watermarks. For queries or protection of configuration files as suggested in use case 1 of IoT4CPS these schemes can be applied only if the size of this data is sufficiently big. [YLCLL13] for example spreads the watermark by combining both requests and responses. Watermarks are then encoded by data from the predecessor.

Additionally, schemes coming from data forensics could be applied to structured data such as XML-Files often used for encoding configuration data. Integrity protection and authentication information (e.g., hash values of data) are encoded in the structure of the data, since the data itself cannot be altered – a configuration file contains no noise. The advantage of this method is that absolutely no additional space is required to store the hash values for authentication. Main application areas are XML or similarly structured data or unordered linked lists, which are preserving their semantics due to the structural equivalence.

2.2.8 Components of trust provisioning infrastructure

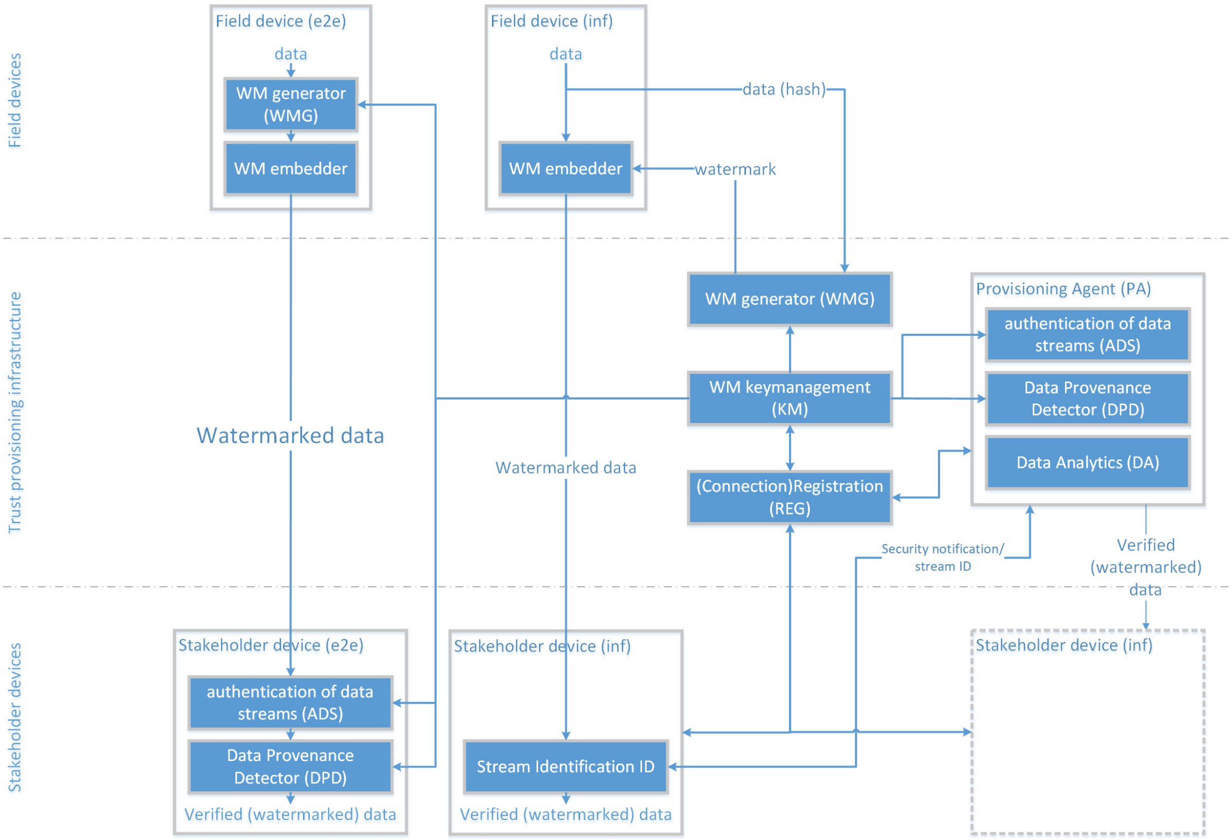


Figure 9: Elements of trust provisioning architecture (left: full end-to-end security, middle: infrastructure supported operation, right: full data provisioning by infrastructure)

Watermarks are light and efficient measures to protect small-sized often stream-oriented data. Figure 9 shows the application for data transfer between field devices and stakeholders. Whereas the key management is the only component that requires a centralized unit in terms of the trust (Trusted Third Party), it is a matter of available resources and watermark system used, whether components for watermark generation, authentication or data provenance detection are implemented as entities of the central infrastructure or as local components. This section describes the basic design options in the context of IoT4CPS industrial environments. Three possible use-cases can be implemented as shown in Figure 9:

1. Full end-to-end protection between field device and stakeholder device (e2e): only key management is located in the infrastructure;
2. Infrastructure-based trust provisioning without data provisioning (inf, middle): the stakeholder device required to do stream identification;
3. Infrastructure-based trust provisioning with data delivery (inf, right side): the stakeholder devices are decoupled from the field device by the infrastructure.

Field devices are characterized by low computational, storage and communication resources. Hence the watermark embedding is required to be implemented in the field device to prevent the system from sending or storing duplicated data. In case of side-channel watermarks, it might be prudent to shift watermark generation to the infrastructure, since only the identifier of the stream (e.g., hash value) needs to be transferred and the watermark is also lightweight. The origin of trust is set at the field device and infrastructure support can be added for downsizing the field devices.

Stakeholder devices could implement watermark decoder, authentication and data provenance detection locally or if these devices have a powerful backbone communication to the infrastructure, trust provisioning functions are better located in the infrastructure as a middleware. Backbone networks usually also can provide strong security measures for protecting the connection between infrastructure and stakeholder devices. Local implementation would create full end-to-end security, whereas the suggested solution is favoured for a simpler stakeholder device.

Mode of operation:

1. Stakeholder devices need to register a connection at the connection registration to be able to acquire the required keys from the key management and to get notification about security checks from the infrastructure.
2. Field devices create the watermark from the host data, embed the watermark in the data and send the data to the stakeholder (inf-modes and e2e-mode) and/or the provisioning agent (inf modes).
3. Since the watermark is invisibly hidden in the host data, any system component can instantly use these data. This includes also network components like data concentrators, which modify or aggregate the data. Such operations are acceptable to a certain extent without destroying the watermark.
4. e2e stakeholder devices will verify data by themselves to authenticate the field device and verify data provenance.
5. inf stakeholder devices will get the security attributes via the Provisioning Agent (PA), which retrieves and analyzes the watermark to authenticate the field device and verify data provenance in parallel. After checking the watermark, the PA informs the stakeholder device about the security status of the received data. In this operation mode, the stakeholder device only needs to perform a stream identification.

6. Alternatively, if no direct data connection between the field and stakeholder devices is foreseen in the application, the PA can also provide the data stream to the stakeholder device.

3. Trusted Contextualization (TC)

The concepts described in this section may be used to protect stakeholders from wrong integration of automation devices in the production environment and from attacks on the setup process, which are threats outlined in section 1.2.

3.1 Trusted Localization Module (TLM)

The main security challenge in the field of localization that is related to the use-case in question is to prove that a device is at a specific location. This section is intended to provide an overview of the existing solutions within this topic as well as additional concepts we developed that are useful for related and similar approaches. Location privacy is out of the scope of this section. However, a further reference on this topic is available at [PK14]. We initially consider a trusted scenario, in which the third party employee is honest and the environment is free of attacks. The goal is to prove to the operator that the device was correctly installed in the specified location within its production environment. Next, we consider the case where the third-party employee has an incentive to lie or cheat.

3.1.1 Overview and Limitations of Trusted Localization Techniques

A solution using existing WiFi Access Points (APs) is described in [SW09] in which a location-proof protocol is established using the proximity of a client to a set of trusted APs with a known location. Since the performance of GPS is limited indoors, it is advised to equip the APs with a suitable interface allowing it to be calibrated outdoors first. Another possibility is to set up the location manually. Four main disadvantages are listed in this paper, they are: (1) the orientation of the anchor is unknown. Although this allows the anchor to estimate the relative position of the tags about itself, an external system communicating with the anchor is not capable of estimating these positions, (2) the first localization of a tag is established by guessing its position (i.e., choosing one position of the semi-localization), (3) a high number of ranging messages is needed (at least 8n - 12, where n is the number of nodes) and, (4) all antennas within a localization estimation must be within communication range.

This list could be further extended with two additional items, namely, the security of GPS itself, which can be spoofed, and the requirement for nearby access points, which are not always in the facility.

The achievable accuracy of WiFi-based approaches depends on many factors, such as environmental changes, AP density, unstable Received Signal Strength Indicator (RSSI) measurements and Line-of-Sight (LoS)/Non-Line-of-Sight (NLoS) conditions. In practice, one can expect with the current technology a mean error above 4m.

Another solution entitled “LINK” [TCB15] uses short-range wireless connected devices such as Bluetooth transceivers and validates location claims based on a centralized analysis of spatio-temporal correlation between the users, trust scores associated with each user and historical trends of the trust scores. A noticeable advantage in comparison with the previous solution is that it does not require APs, but movable devices within the network.

In [BLFC15], a framework compatible with (and relying on) short-range technologies, such as BLE and iBeacon, is proposed. The authors argue that their proposal “enables the production of unforgeable proofs of fine-grained indoor location on unmodified commodity devices”. Nonetheless, the granularity of the proof may still not be enough for the use-case in question, since it aims at room-level accuracy only. The solution that we look for here should provide a centimeter to decimeter accuracy. Similar to WiFi, the typical mean error obtained with BLE beacons range between 1.6m and 2.5m.

Given the strict accuracy requirements imposed by the use-case and the inapplicability of GPS due to accuracy and scenario, which may be indoors, Ultra-wideband (UWB) transceivers can be used. They are able to provide sub-decimeter accuracy and are resilient to multipath. Typical systems using UWB anchors use trilateration [D13] to determine the exact position of a tag (unlocalized node), in which each anchor (localized node) estimates its distance to the tag via time-of-flight (ToF) measurements. In order to estimate the position of a tag in a 2D plane with this method, at least three anchors are needed. This increases the infrastructure costs and power consumption of the overall system. Prior work proposed a UWB-based system called SALMA capable of localizing a tag with a single-anchor [GRKB18] assisted by multipath components. Nonetheless, SALMA requires the knowledge of the surroundings of the environment where the localization takes place, which is undesirable in many practical use-cases. Other existing approaches rely on nodes featuring two spaced antennas and will be further detailed next.

3.1.1.1 Dual Wireless Radio Localization (DWRL)

[AE12] is the first paper, to our knowledge, presenting a localization mechanism matching the constraints already mentioned, and relies only on distance estimations. Each node is equipped with two spaced antennas, and the anchor initiates ranging measurements based on ToF from each of its antennas to each of the antennas of a tag, as illustrated by the green arrows in Figure 10.

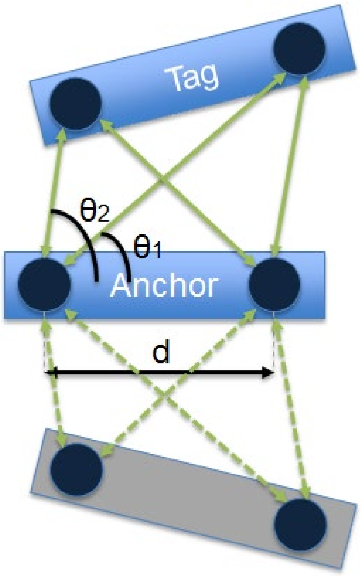


Figure 10: Illustration of the DWRL mechanism.

The anchor calculates the angles θ_1 and θ_2 by using cosines law. Two possible ambiguous positions are possible. Thus, DWRL requires also the estimations from a second localized node to eliminate this ambiguity. Since the system is a single-anchor one, the position of the first tag to be localized is randomly guessed (between the two possibilities). This may cause all the estimations to be flipped about the axis of the anchor, in case the wrong estimation is chosen for the first tag.

3.1.1.2 Improved Dual Wireless Radio Localization (I-DWRL)

The limitations of DWRL were addressed in [AKJ17], which proposed an improved localization mechanism called I-DWRL. This was done by adding a magnetometer to the nodes (tags and anchor) and slightly changing the localization mechanism in order to overcome the previously described drawbacks. Whenever the orientation of the tag is significantly different (considering the error of the magnetometer) from the orientation of the node localizing it, the insertion of the magnetometer allows I-DWRL to distinguish between the two mirrored positions. Thus, I-DWRL is able to localize a tag with a single semi-localization. When only one of the tag radios is within communication range of the localizing node, in specific situations, the magnetometer can also enable the localizing node to localize the tag. Still, I-DWRL needs four ranging messages for semi-localization.

3.1.2 Efficient Single Anchor Localization with Dual Antennas Tags (E-SALDAT)

Within our work in this task, we developed a novel strategy (called E-SALDAT) to reduce the number of range estimations (thus, energy) required to localize a tag. In E-SALDAT, only a single antenna from the localized node estimate its distance to both of the antennas from the unlocalized node, thus reducing the required range estimations by 50%. All the nodes must be equipped with an orientation provider (e.g., a magnetometer), as in I-DWRL. Two ambiguous position estimations are still possible, as illustrated in Figure 11.

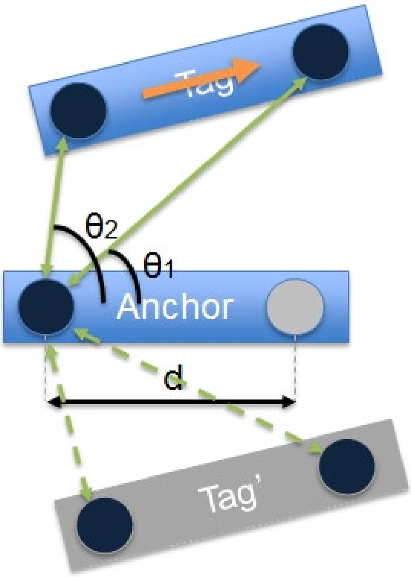


Figure 11: Illustration of the E-SALDAT mechanism.

This ambiguity can be addressed by letting two nodes (only one being localized) estimate the position of a tag and by intersecting the two estimations. This solves the initial guess, which constitutes a major problem in DWRL. This approach was evaluated via simulations, and compared with DWRL and I-DWRL, resulting in superior energy efficiency, as expected. Nonetheless, E-SALDAT increases the mean error of the location estimations when comparing with I-DWRL, which is undesirable. Further investigation in this direction is still necessary involving a fusion of the approaches and testing/simulation with current state-of-the-art modules/models to increase accuracy and precision, and achieve the performance required by the use-case.

3.1.3 Security in single-anchor localization approaches

Given that we know how to set up an accurate localization system with minimum overhead requiring a single-anchor and that all participating nodes are honest, which can be certified by a CA, the location of the tags can be provided to the system by the anchor(s), which are by definition devices with known location. The setting up of the anchor's location must be performed manually to the fine accuracy requirement, which can hardly be provided via GPS, even outdoors.

In this scenario, the manager can be sure that the device to be provisioned was indeed installed at the indicated place. Next, we analyze a scenario where the third-party employee has incentives to cheat in the localization process.

If no authentication of the nodes is provided, fake nodes could be inserted in the system capable of performing the *distance fraud*, which is a class of attacks in which the tag to be localized is untrusted and may delay the acknowledge of messages or process it faster in order to look as if it was further away or closer to the anchor. By using authentication we assume that this class of attacks is addressed. The same approach addresses the *terrorist fraud*, a different class of attacks in which a dishonest prover collaborates with an external attacker/Man-in-the-Middle. If the prover is trusted, it will not collaborate with attackers. Thus, we are left with two classes of attacks which do not rely on an untrusted prover, namely the *impersonation attack* and the *Mafia Fraud (Relay attacks).*

Since the system relies on ToF measurements, an external attacker could perform what is known as *relay attacks.* Relay attacks could be avoided by estimating the ranges with ToA, which requires the anchor and the tag to be synchronized, or with Round-Trip Time (RTT) [ABBC18] measurements. In [RC10], a practical approach to solve the relay attack is proposed and verified, for the case when the attacker intends to shorten the distance between the tag and the anchor. Alternatively, the attacker could also jam the channel during the response of the tag and send a delayed response, which is a copy of the tag response, to enlarge the distance between prover and verifier. Thus, the verifier could prevent this last attack by monitoring jamming signals during the response time. By combining both approaches, the verifier can assure that the attacker is not manipulating the estimated position of the anchor toward the tag or abort the position estimation and report the attack to the manager in case an attack is detected. Finally, in order to protect the system from impersonation attacks, the ranging could be performed as in the Brands and Chaum protocol, in which the probability of success from an attacker equals $(\frac{1}{2})^{n}$, where n is the number of rounds in the fast exchange phase.

3.2 Trusted Orientation Module (TOM)

The growing popularity and applications of indoor positioning technologies triggered the development of various approaches based on wireless network technologies, such as WiFi, RFID, and UWB, which estimate the position based on the intensity of received signals, the TOA (time of arrival), or TDOA (time difference of arrival). The UWB technology, in particular, can achieve a decimeter-level positioning precision. However, in certain cases, the UWB signals could be blocked by people, walls, or other obstacles in complex indoor environments, resulting in signal multipath effect or intensity attenuation. Therefore, high-precision positioning can hardly be achieved in NLOS (non-line of sight) environment through the UWB positioning approach alone.

Methods for orientation estimation are predominantly based on IMUs (inertial measurement units), such as accelerometers, gyroscopes, and magnetometers, which are very popular in pedestrian navigation. Inertial navigation is a self-contained navigation technique in which measurements provided by accelerometers and gyroscopes are used to track the position, velocity, and attitude (orientation) of an object relative to a known initial position, velocity, and attitude. It does not rely on external information sources and is highly popular in the design of autonomous systems for a variety of applications, where 100% coverage and a high continuity-of-service are needed, due to high update rates (100 Hz) and low-cost inertial sensors (accelerometers and gyroscopes). Theoretically, inertial navigation systems could perfectly track position, velocity, and attitude as long as the specific force and angular velocity are measured accurately. However, this approach also has a deficiency, which is the accumulative error. Since, in reality, all measurements are error-prone and due to the integrative nature of the inertial navigation equations, the overall error accumulates and introduces a drift in position, which grows indefinitely. For low-cost IMUs, the position error grows cubically with the magnitude of the bias in gyroscope measurements. Therefore, such systems can be used for stand-alone navigation only for very short periods of time.

Measurement errors have a large impact on the accuracy of the estimated position and orientation using inertial sensors only. This is particularly the case for the position, which relies on both, the double integration of the acceleration and the accurate orientation estimates to subtract the earth's gravity. Because of this, inertial sensors need to be supplemented with other sensors and other models to obtain accurate position and orientation estimates. In order to correct the accumulated system error, a ZUPT (zero velocity update) is usually applied in pedestrian navigation. Although the ZUPT method can compensate for the error to an extent, it cannot solve the problem of error accumulation for long-distances or non-pedestrian movement. Since inertial sensors provide pose estimates at high sampling rates, which are accurate on a short time scale but drift over longer time scales, they are, therefore, very suitable for being combined with sensors with a lower sampling rate, which provide estimates that do not drift over time.

For orientation estimation, inertial sensors are often used in combination with magnetometers, which measure the direction of the magnetic field. For estimating orientation, it is typically easier to obtain accurate pitch and roll than accurate heading estimates. The orientation errors from inertial measurements based on dead-reckoning of gyroscope data accumulate and introduce a drift over time. Therefore, if only inertial and no magnetometer data are available, the heading can only be estimated using the gyroscope signal and will inevitably drift over time. Although the accelerometer and the magnetometer measurement noise are of equal magnitudes, the heading angle is estimated with less accuracy compared to the pitch and roll angles. The reason is twofold. First, the signal-to-noise ratio for the magnetometer is worse than that of the accelerometer. Second, only the horizontal component of the local magnetic field vector provides heading information. The accelerometer provides inclination, while the magnetometer provides heading information. Furthermore, the presence of magnetic material in the vicinity of the sensor might cause a change in the magnetic field and affect the orientation estimation. However, by fusing all sensor data, provided by accelerometers, gyroscopes, and magnetometers, we can stabilize sufficiently well the overall 3D orientation estimate as demonstrated in Figure 12, which presents the change of the estimate along all three axes separately when an object is rotated by 90 degrees from an initial zero angle. Extensive tests revealed that the deviation in orientation is kept well under 5 degrees, which is the upper limit required for applying the UWB localization method, developed at TU Graz.

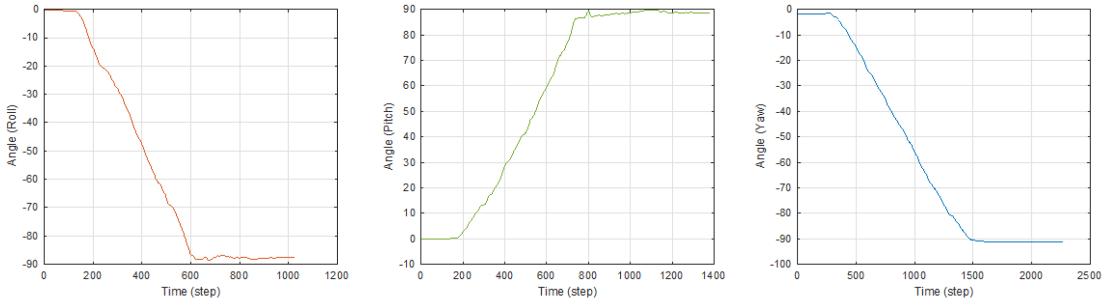


Figure 12: Roll (red), pitch (green) and yaw (blue) angles of an object rotated from the initial position by 90 degrees, demonstrating the accuracy of the orientation estimate.

3.2.1 State-of-the-art

For pose estimation, inertial sensors are often combined with measurements from, for instance, a global navigation satellite system (GNSS), an ultrawide-band (UWB) system or cameras. State-of-the-art approaches integrating IMU measurements with UWB data in order to achieve high-precision and real-time indoor positioning alleviate most of the presented issues and ensure the following benefits: (1) the position accuracy of a UWB-receiver; (2) full 6 degrees-of-freedom navigation; (3) high update rates; (4) provide a navigation solution during short periods of UWB-receiver outages; (5) higher system integrity by detecting faulty UWB-measurements; and (6) eliminate multipath and NLOS effects.

Figure 13 depicts a schematic diagram of IMU/UWB data fusion in a loosely-coupled closed-loop fashion. Whenever the UWB-receiver produces a position estimate, the difference between the position estimates of the two systems is calculated and used as the input for a filter compensating system errors, as well as IMU sensor errors. The error estimates are used both to correct the position estimate and recalibrate IMU sensors.

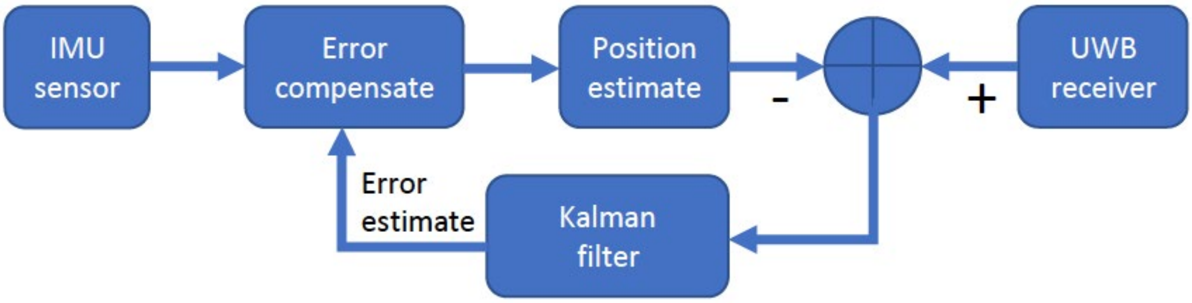


Figure 13: Schematic diagram presenting an example of IMU/UWB data fusion in which UWB readings are used to compensate for the drift in IMU estimates.

Figure 14 presents a position tracking simulation of the IMU/UWB fusion method for two different shapes of 2D trajectories. Here, the deviation from the ground truth is due to a simulated UWB outage during which the IMU-only estimate drifts gradually away, and as soon as the UWB signal is restored the error estimate is compensated appropriately.

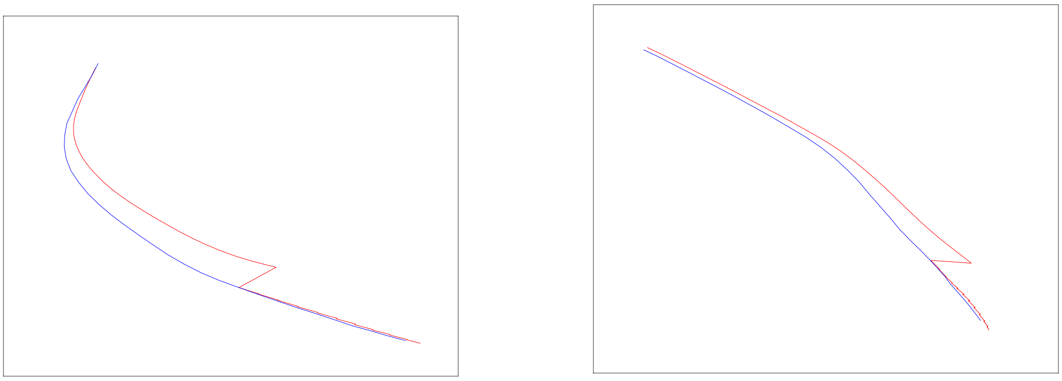


Figure 14: Position tracking simulation using a combination of IMU and UWB data fusion for two different shapes of 2D trajectories. The reference trajectories are shown in blue and the estimate in red. The sharp transitions represent the drift compensation provided by UWB signals.

Figure 15 presents the magnitude of errors, corresponding to Figure 14, along both axes.

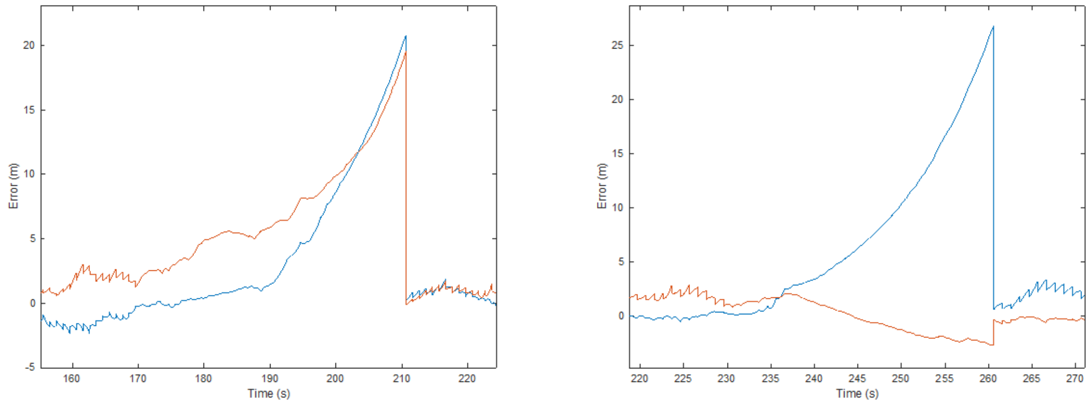


Figure 15: Error trajectories along the X and Y axes, corresponding to Figure 14, revealing the gradual drift of the estimate based on IMU data only.

3.2.2 Proposed Trusted Orientation and Localization concept

Many different filter algorithms can be used for sensor fusion in navigation systems. One of the most popular approaches is the extended Kalman filter (EKF), which simultaneously estimates the IMU sensors systematic errors and corrects the positioning errors. The EKF could prevent corrupted UWB sensor measurement data, due to obstructions, multipath, and other interferences, from degrading the positioning performance by detecting, identifying, and isolating faults. Most state-of-the-art methods have adopted the EKF for UWB/IMU fusion in position and orientation estimation. However, extended Kalman filters inherently assume that both the process (system) errors and measurement noise (observation errors) are Gaussian distributed. Applying extended Kalman filters in case of non-Gaussian noise is not straightforward. However, in an NLOS condition signal transmission might be affected by obstacles due to the blockage or reflection, which would have an impact on the time delay of reception. Under such circumstances, UWB errors would deviate from a Gaussian distribution, resulting in a considerable error.

As described above, all of the involved technologies (UWB, IMU, magnetometers) have characteristic limitations, creating uncertainty about the fused position estimate. This uncertainty could best be tackled with probabilistic methods, such as particle filters. Therefore, we chose a stochastic approach based on particle filters (see Figure 16) for fusing the UWB and IMU position data, as such an approximate approach could tackle the multimodal distribution of errors without normality assumptions. Particle filtering uses a set of particles (samples) to represent the posterior distribution of a stochastic process given noisy and/or partial observations. It is a well-established methodology for generating samples from distribution without making assumptions about the state-space model or the state distributions. The state-space model can be nonlinear and the initial state and noise distributions can take any form. Particle filters implement the prediction-updating step in an approximate manner. The samples from the distribution are represented by a set of particles; each particle has a likelihood weight assigned to it that represents the probability of that particle being sampled from the probability density function. In order to prevent a weight collapse when the weights become too uneven, a resampling step is used in which the particles with negligible weights are replaced by new particles in the proximity of the particles with higher weights. As long as there are sufficient particles available a reliable approximate estimate can be obtained efficiently.

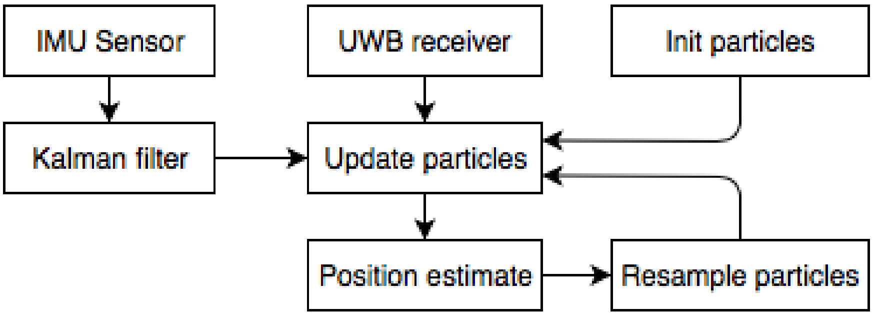


Figure 16: Schematic diagram describing IMU/UWB data fusion using a particle filter.

The proposed probabilistic approach integrates two different technologies for position tracking and as such offers reliable fall-back options in case of intermittent loss of operability of one of the technologies. Such situations can arise due to environmental constraints; however, they could also be triggered by an indirect attack targeting the accuracy, the integrity and the continuous flow of sensor data. To mitigate the potential effect on the tracking dependability of a multitude of uncertainty sources, some of which are unpredictable and previously unseen, we tackle the uncertainty with a probabilistic framework providing approximate, but reliable position estimates as well as the associated confidence levels. This complements the methods dealing with more direct forms of cyber-attacks, specialized on compromising the digital content by tampering, spoofing or repudiation. Also, this approach could offer higher resilience to attacks targeting the accuracy, the integrity, or the continuous flow of sensor data used in the position and orientation tracking. Particle filters could mitigate the detrimental effect of uncertainty created by such attacks by providing an approximate estimate and a confidence range based on the particles’ distribution. Integrating two different technologies for position tracking (UWB and IMU) within this probabilistic approach will allow for a smooth and reliable fall-back operation in cases when the system's integrity is compromised.

4. Conclusion

With the increasing need for connection and cooperation in CPS, ensuring trust and security during production and maintenance is a challenging task. Nonetheless, both trust and security are needed in several recurrent daily processes, like the one outlined in the presented use case, illustrated at the beginning of this document. This is followed by a detailed description of related threats, which reinforce the importance of accounting for these issues from the design phase of the system.

The core of this deliverable described potential architectural patterns and building blocks which may:

- Build trust among different stakeholders working in the same task
- Support provisioning and maintenance applications
- Increase the security level of communication within constrained devices

Section 2 demonstrates how to incorporate security in applications relying on and aiming remote configuration of devices. Despite the robustness of the component and interconnections, it is extremely important that the end-user of such a system, i.e., the customer, is involved in the development process and gets an understanding about the system itself, in order to avoid unintentional endangering of the system during legitimate interventions. Also, we showed how watermarks can be used as a light and efficient way to protect small-sized data between field devices and stakeholders. The system requires a centralized unit in terms of the trust (Trusted Third Party) and additional components which may be local depending on the resources available and watermark system used.

In section 3, localization and orientation were integrated and connected to the scope of trust in collaborative environments to enhance security and trustworthiness among different stakeholders, as well as their requirements to achieve the target protection.

D3.4 documents a set of measures that increase the level of trust, security and safety in future IoT applications, which can be directly applied to the IoT4CPS use cases. By adopting these measures and/or similar concepts, the next generation of IoT applications will benefit from enhanced security and dependability, as well as reduced engineering costs which are often expected when CPS is under (unexpected) attacks or misuse.

5. References

[A15] C. C. Aggarwal, Data Mining: The Textbook. New York, NY, USA: Springer, 2015.

[ABBC18] Gildas Avoine, Muhammed Ali Bingöl, Ioana Boureanu, Srdjan čapkun, Gerhard Hancke, Süleyman Kardaş, Chong Hee Kim, Cédric Lauradoux, Benjamin Martin, Jorge Munilla, Alberto Peinado, Kasper Bonne Rasmussen, Dave Singelée, Aslan Tchamkerten, Rolando Trujillo-Rasua, and Serge Vaudenay. 2018. Security of Distance-Bounding: A Survey. *ACM Comput. Surv.* 51, 5, Article 94 (September 2018), 33 pages. DOI: https://doi.org/10.1145/3264628

[AE12] H. Akcan and C. Evrendilek, "GPS-free directional localization via dual wireless radios," Computer Communications , vol. 35, no. 9, pp. 1151–1163, 2012.

[AKJ17] A. Aziz, R. Kumar, and I. Joe, "I-DWRL: Improved Dual Wireless Radio Localization Using Magnetometer," Sensors, vol. 17, no. 11, p. 2630, 2017. [Online]. Available: http://www.mdpi.com/1424-8220/17/11/2630

[BLFC15] Jacob T. Biehl, Adam J. Lee, Gerry Filby, and Matthew Cooper. 2015. You're where? prove it!: towards trusted indoor location estimation of mobile devices. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (UbiComp '15). ACM, New York, NY, USA, 909-919. DOI: https://doi.org/10.1145/2750858.2804284

[BSITR02102] German Federal Office for Information Security, Technical Guideline, Cryptographic Procedures: Recommendations and Conclusions. Online available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

[CERT18] Computer Emergency Response Team Austria Report Internet Security 2017. Online available: https://cert.at/media/files/downloads/reports/jahresbericht-2018/files/cert.at-jahresbericht-2018.pdf

[CSV10] S. Chong, C. Skalka, and J. A. Vaughan, Self-identifying sensor data, in Proc. 9th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw., 04/2010, pp. 8293.

[D13] Deka, Bhaswati. "Secure Localization Topology and Methodology for a Dedicated Automated Highway System." (2013).

[GRKB18] Großwindhager, B., Rath, M., Kulmer, J., Bakr, M. S. A., Boano, C. A., Witrisal, K., & Römer, K. U. (2018). SALMA: UWB-based Single-Anchor Localization System Using Multipath Assistance. in *SALMA: UWB-based Single-Anchor Localization System using Multipath Assistance* (S. 132-144)

[HKB09] A. Houmansadr, N. Kiyavash, and N. Borisov, "RAINBOW: A robust and invisible non-blind watermark for network ows," in Proc. NDSS, 02/2009, pp. 113.

[PK14] Píse, P. and Ratnaraj Kumar. "A Review on Privacy Preserving in Location Proof System." (2014).

[RC10] Kasper B. Rasmussen and Srdjan Čapkun. 2010. Realization of RF distance bounding. In Proceedings of the USENIX Security Symposium (USENIX'10). USENIX, 389–402.

[SSB13] S. Sultana, M. Shehab, and E. Bertino, Secure provenance transmission for streaming data, IEEE Trans. Knowl. Data Eng., vol. 25, no. 8, pp. 18901903, Aug. 2013.

[SW09] Stefan Saroiu and Alec Wolman. 2009. Enabling new mobile applications with location proofs. In *Proceedings of the 10th workshop on Mobile Computing Systems and Applications* (HotMobile '09). ACM, New York, NY, USA, Article 3 , 6 pages. DOI=http://dx.doi.org/10.1145/1514411.1514414

[TCB15] Manoop Talasila, Reza Curtmola, Cristian Borcea, Collaborative Bluetooth-based location authentication on smart phones, Pervasive and Mobile Computing, Volume 17, Part A, 2015, Pages 43-62, ISSN 1574-1192.

[YLCLL13] Y. Yi, R. Li, F. Chen, A. X. Liu, and Y. Lin, A digital watermarking approach to secure and precise range query processing in sensor networks, in Proc. IEEE INFOCOM, 04/2013, pp. 19501958.