IoT4CPS
Trustworthy IoT for CPS

Industry 4.0: Integration of Secure Connectivity Solutions into an Industrial Environment

Challenges, Technical Solutions & Application Use-Cases

Date: July 2020
Editor: Christos Thomos
Authors: Christos Thomos, Stefan Marksteiner, Nikolaus Dürk

Contents

1. SUMMARY

Industrial production has been continuously evolving since its introduction. Currently, it is entering its fourth phase called Industry 4.0, which is characterized by OT/IT convergence through a higher degree of digitalization for manufacturing and products which creates new value chains, business models and drives new revenue streams (*Figure 1*). The main goals involve a higher degree of production automation processes with increasingly intelligent and integrated supply chains, productivity optimization across operations, and predictive maintenance through monitoring, diagnostic and prescriptive frameworks, which aim to bring manufacturing closer to the customer needs.

Academic and Industrial Research in Industry 4.0 and Smart Manufacturing is mainly focusing on technologies such as Industrial IoT, collaborative CPSs, Big Data and Analytics, edge/could/fog computing, smart sensors and actuators, Digital Twins, and Artificial Intelligence (AI). Disruptive supply chain configurations

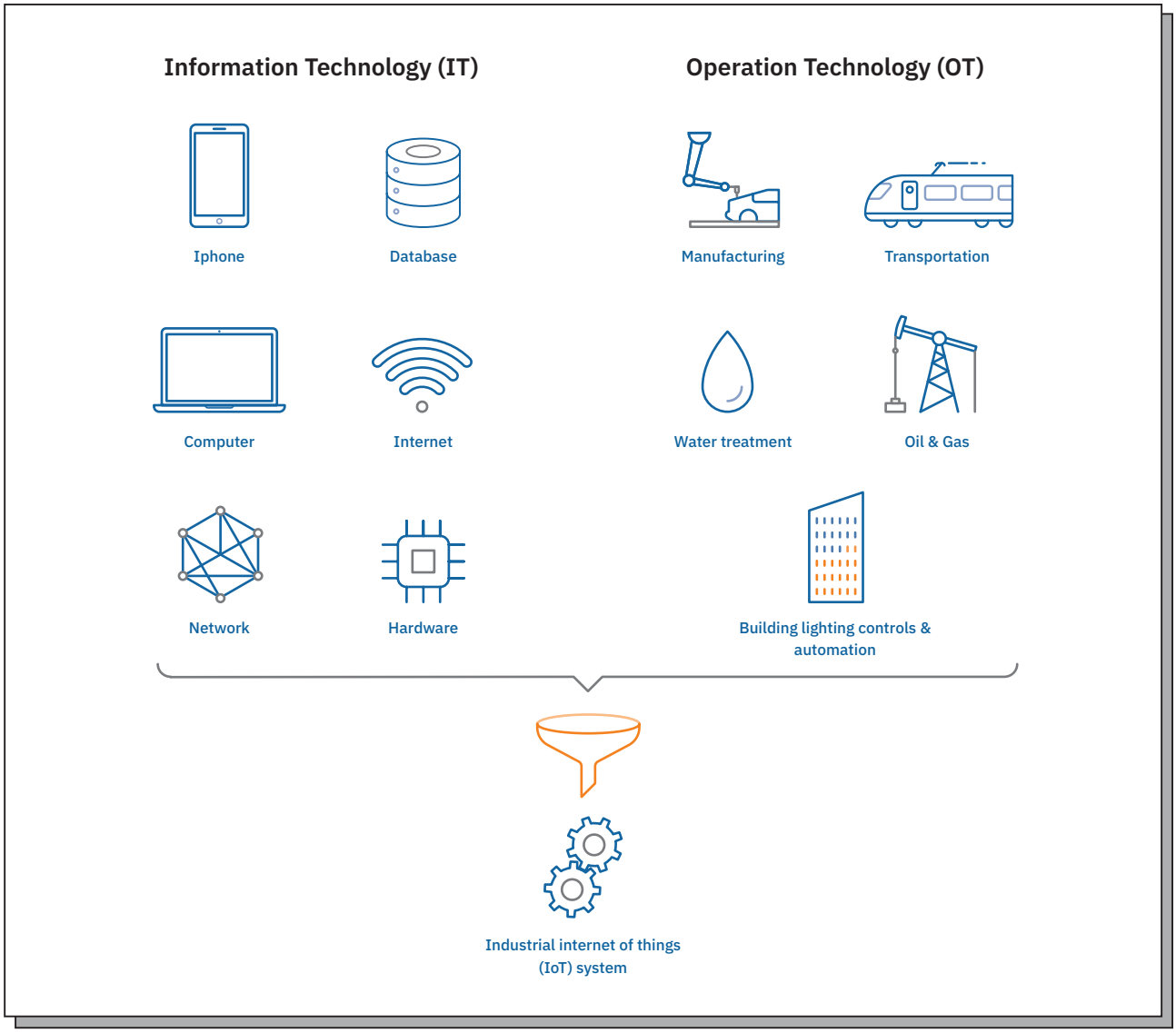

Figure 1: Industry 4.0 is characterized by the ongoing automation of traditional manufacturing and industrial practices, using modern smart technology

based on advancements in these areas can create a huge competitive advantage to manufacturers by offering them new opportunities for growth and profitability through a vertically-integrated advanced manufacturing framework with self-configuring, self-monitoring and self-healing properties. However, at the same time, many challenges must be dealt with when exposing industrial technologies and devices to the IT world that is full of malware and cyberattacks. Despite the rapid advancement on these ICT and autonomous CPS technological fields, most industrial manufacturers still want to retain full control over their data and ignore the benefits due to reliability, security and privacy concerns that yet pose challenges which are unanswered for the industrial domain.

Smart production is characterized by increased dynamicity in configuration, system context, system environments and even tasks. For that reason, potential risks should be considered and analyzed not only during the design time but also during the complete system lifecycle. To provide solutions for the main demand drivers and support the digitalization over the entire lifecycle of complex industrial products, IoT4CPS has developed an extensive design framework for highly dependable Industrial IoT elements towards the vision of safe and secure Industry 4.0. Throughout our project's technical work, a whole set of innovative security guidelines, methods and tools, established through the interconnection of engineering activities at multiple technology levels, have been investigated and built aiming to ensure the security, safety, reliability and resilience of IoT-based CPS systems for largely heterogeneous, distributed and dynamic environments. The outcomes of this project address those aspects holistically through a high degree of integration along the value chain and product lifecycle, leading to a significant time-to-market acceleration for complex products. For that reason, lifecycle management aspects have also been addressed through conceptual models and the development of a prototype data management infrastructure based on a Digital Twin concept.

Additionally, since IoT4CPS is a lighthouse project, aside from delivering technical results, it also guides the sustainable implementation of the project findings showing the benefits of these technical achievements to multiple stakeholders such as academic/research institutions, security solution vendors, governmental bodies, industrial automation practitioners, etc.. Therefore, a relevant set of the developed technologies and components are integrated into several demonstrators encompassing aspects of real industrial settings for smart production use-cases. The demonstrators are being set up in a way that considers the heterogeneity of the industrial IoT environment and at the same time focuses on a high degree of reusability. The corresponding demonstrators are aiming to exhibit how trustworthy connectivity and lifecycle management aspects can be successfully addressed by covering security concepts and solutions for connectivity, testing, validation and traceability. The aim is to offer applicability evaluation and recommendations to industries that are interested to further exploit the proposed solutions into real industrial settings. At the same time, this will generate the required experience for more advanced Industrial 4.0 platforms in the future.
This paper deals with the challenges and current status for secure connectivity solutions into a smart industrial environment and then presents the project's contributing technical solutions and smart production demonstrator use cases which integrate part of them to showcase their applicability and benefits.

2. CHALLENGE

The evolution of the traditional industrial systems towards Industry 4.0 and Smart Manufacturing creates a **highly dependable Industrial IoT (IIoT) ecosystem** of connected, heterogeneous, and complex production systems characterized by increased dynamicity in configuration, system context, system environments, and tasks. IoT-enabled industrial infrastructure differs from traditional communication networks in terms of security, safety, resilience to failures, and reliability requirements, which now become increasingly important and pervasive, while digitalization and connectivity are gradually manifesting themselves as the new business reality and a game-changer in many industrial sectors.

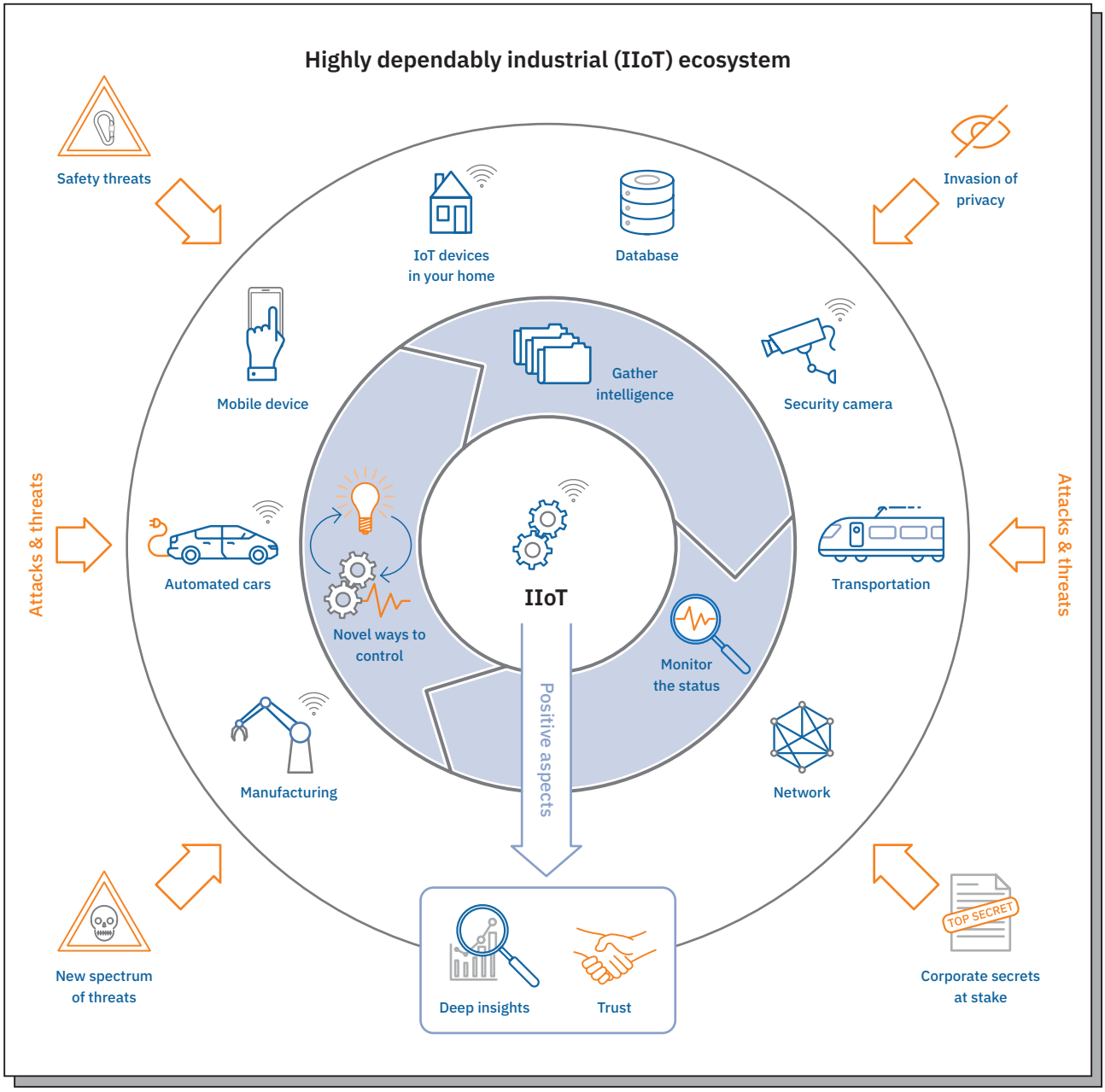

Figure 2: Highly dependable IIoT ecosystem of connected, heterogeneous, and complex production systems – its positive aspects and challenges

Connected smart production systems enable new data streams and novel ways to control, monitor the status, and gather intelligence from industrial operations aiming to coordinate everything towards a global optimum. This kind of cooperation and information exchange can provide deep insights into the behaviour of the systems and relies on trust between the associated systems for the received information. On the other hand, it requires massive connectivity of many types of heterogeneous elements for many use cases. This situation, which can be ever-expanding due to the constant appearance of new use cases, ultimately may lead to an entirely new spectrum of threats if connectivity is not sufficiently and efficiently protected by well-fitted **security mechanisms**. If industrial data are made accessible to non-authorized parties, privacy, and corporate secrets are at stake, while unauthorized access to systems and components can raise critical safety threats. The increased rate of industrial cyber threats in recent years caused millions of euros worth of damage, injuries, and in some unfortunate cases, even deaths (*Figure 2*).

Although state-of-the-art security solutions are available for many high-end security requirements, Industrial IoT applications require step-ups to meet the requirements set by the Industry 4.0 domain. Integral end-to-end security concepts still need to be developed, covering life-time and stakeholder considerations. Industrial IoT systems need to involve a large **diversity** of different elements from different manufacturers with cross-system **interoperability** issues. This implies a mixture of interconnected devices for both critical and non-critical applications in the same network that can provide easier access to critical applications via the low-security devices. Safety & security of such systems can be possible only if all elements are trustworthy and reliable. This requires a common understanding of trust and mechanisms for trust validation and management, however, a common IoT standard and interoperable security framework are not yet available. At the same time, many of these Industrial IoT devices are often limited in their computational **capabilities** due to power and resource limitations. Thus, highly efficient mechanisms with a sufficiently small footprint that can also distribute the security burden are needed for ensuring safety and security on these devices. What's more, **safety** must be considered together with security, to protect not only the data but also the physical elements (equipment and people) involved. This supports the need to validate and protect the transmitted data. At the same time, access control mechanisms have to be established to allow manipulation of involved elements only to trusted parties.

To cope with dynamic environments, smart production systems have to be tested even more thoroughly **during development**, trying to anticipate future configurations and interconnections, but also **during operation**, when safety and security properties have to be ensured across sub-systems from multiple vendors, e.g. by fault tolerance features enforcing safe behaviours based on monitoring and the diagnosis of results. Also, to guarantee the highest degree of **maintainability** for industrial systems having a typical time of operation between 10 and 20 years, safety and security must be provided over their whole **lifecycle** through constant monitoring and adaptation to new requirements and threats. However, the lifetimes of heterogeneous devices are not centrally managed and could span an undefined number of years, which also means that there should be an assurance of updated security over an undefined lifetime which is currently a challenge. Moreover, for the efficient development, validation, instrumentation, and deployment of innovative solutions, it is crucial to enable safety and security for **highly accelerated processes** by creating methods and tools capable of constant validation and monitoring of the stated requirements.

In the past, a traditional production system was characterized by isolated, closed-loop architectures where proprietary solutions and protocols were dominant. Such systems could be thoroughly analyzed and tested for fulfilling such qualities. Potential interactions and goals could be considered during the design process and updates of system parts were completely under the control of the system operator, they were typically heavily tested, and not applied on the fly to the live system over the air. Within the Industrial IoT ecosystem, manufacturing systems will inevitably become more adaptive with flexible decision-making mechanisms, self-awareness, and self-optimization features to their core components and services.

In conclusion, the aforementioned challenges, although not completely new, they now advance into a new level and need to be addressed together to achieve secure and dependable Industrial IoT components. Uncertainties and unknowns must now be taken into account since the problem of potential emergent behavior is not easily recognizable during design time and thus difficult to analyze. Therefore, covering all risks and requirements during the design phase is not sufficient anymore, and achieving the required qualities in these largely heterogeneous, distributed, and dynamic Industry 4.0 environments, necessitates a clear understanding of the combined system properties and continuous risk management during the **complete system lifecycle**.

3. CURRENT STATUS

The evolution of IoT related technologies manifests itself in the industrial domain through the Industrial IoT and is eventually demonstrated into Industry 4.0 use cases. Hereby, underlying rapidly growing and increasingly mature ICT technologies, such as advanced machine-to-machine (M2M) connectivity, innovative sensing and actuation technology, cognitive computing platforms (artificial intelligence, machine learning), distributed computing resources (edge/fog/cloud computing) and data analytics (big/smart data), are widely adopted and fused with industrial Operational Technologies (OT). This integration of cyber technologies into the production environments sets a new framework not only for smart manufacturing based on self-controlled, intelligent cyber-physical systems (CPS) but also for the digitalization of business and production models and processes. Among others, the innovative services are promising data reliability & consistency, enhanced safety, production automation, supply chain management & integration, system interoperability, interface optimization, machine optimization, quality optimization, internet-based diagnostics, remote maintenance, predictive maintenance, etc.

A state-of-the-art production system is currently organized according to the classical automation pyramid, where each level (field, control, supervision, management, enterprise) includes Industrial Control Systems (ICS) with an increasing number of components and subsystems from top to the control level. ICS is a generic term for components (e.g. machinery, devices, sensors, actuators, PLCs, SCADA, HMI tools, access points, terminal units etc.) that are at the core of OT and thus, their system architecture is entirely different than that of the corporate IT system architecture since external connections were neither needed nor desired. This closed-loop architecture ensures isolation from the outside world. Until recently, security implementation was focusing on defending organizational parameters, e.g., unauthorized access to private networks by placing safeguards such as firewalls, intrusion-detection systems and malware protections at the system perimeter. ICS equipment and software were not designed with protection against cyber attacks. Security gaps are mostly identified at field, control and supervision levels, but these are the levels where security relevance is very high, which leads to a significant mismatch.

In the last few years, an increasing number of ICS have been equipped with Internet connectivity to benefit from the advantages of remote accessibility such as e.g., installation of software updates, or remote maintenance. This Internet connectivity, in this case, is simply achieved by establishing a remote desktop connection via a Virtual Private Network (VPN) to an industrial PC connected to the production line. From a security perspective, an attacker that gains access to this remote PC by compromising the VPN credentials or via malware injected to the PC can thus get full control on the production line. A remote desktop connection like this is not helpful for the acquisition of real-time data from a production line as data needs to be manually transferred from the industrial production line PC via the remote desktop link. Also, data acquisition within companies can currently be best described as “fog computing” implemented as a middleware that performs tasks locally without reserving resources of the end nodes or the remote servers. This provides better security since production-process related data is mostly used in the isolated network within the company, but not transferred to external servers or consumers. The term “fog computing” addresses the

local storage on edge nodes, as opposed to the “cloud computing” paradigm where data is accessed on-demand via the Internet. The secure implementation of this architecture helps to avoid additional drawbacks, e.g. large response times and other disruptions in the communication networks, bringing in many additional advantages such as network bandwidth optimization, decentralization, scalability, agility and system efficiency.

Connected ICS technology continues to be plagued by cyber threats that originate mostly due to the fundamental differences between IT and OT technologies in many key parameters necessitating a novel and holistic approach for end-to-end system security based on the peculiarities of the industrial domain. For example, in the IT domain, priority is given to confidentiality over availability, whereas in the OT is the other way around. Also, the qualities in the IT domain are mainly security, privacy and visibility, whereas some data and traffic latency can be considered acceptable to a certain degree. On the contrary, in the OT domain latency can be unacceptable in many cases and the main properties are control, efficiency and simplification of processes. IT security is usually provided by constant and mandatory firmware updates but for OT systems security updates can be irregular and probably disruptive to the processes. IT is also characterized by complex network architectures, user privileges, remote access and access control, which can be inapplicable or impose a tradeoff between security and efficiency in OT networks since they can downgrade the production and control processes. IT security options are vast and products from different vendors are easily integrated and interoperable, whereas in the OT domain there are many products with proprietary, insecure, legacy protocols and still very few options for secure connectivity. Finally, in the IT device lifecycles are quite shorter than the OT domain.

Currently, a dominant standard for industrial cybersecurity is the IEC 62443 which covers many aspects of two key goals for industrial processes, namely, availability and integrity for ICS security by introducing distinct security levels that categorize main threat actors. It also includes other elements such as user security, corporate and company security, cyberthreat mitigation, as well as issues of incorporating products and services from third parties and system integrators. The technical challenges for leveraging ICT mechanisms in the OT domain have also given rise to numerous reference architectures which are designed for helping on the development of Industrial IoT applications and architectures. Popular reference models serving this purpose are the Industry 4.0 reference architecture model (RAMI 4.0), the Industrial Internet Reference Architecture (IIRA) and NIST smart manufacturing.

4. CONTRIBUTING TECHNICAL SOLUTIONS

IoT4CPS overall goal is to support full product life-cycle and aspects of designing, testing, producing, and operating innovative and highly trustable IoT components in the fields of Automated Driving (AD) and Smart Production (SP). The generated guidelines, methods and tools for trustworthy and secure integration of IoT and CPS into AD and corresponding smart production (SP), are aiming to holistically address safety and security aspects both along the specific value chains and the product life cycles.

The technological activities are grouped into three main areas:

- Design & Development of CPS: Methods for the design of safe and secure industrial IoT applications. Provisioning of tools to support security-by-design or ease the integration of security mechanisms across partners.
- Verification & Analysis: Verification of system requirements to ensure system reliability and system monitoring to ensure system resilience.
- Life-cycle Management: Enable security throughout the system lifetime, including mechanisms to provide updates. Support integration of field learning in production processes for next-generation solutions.

The results of IoT4CPS in these areas are broadening fundamental knowledge for trustworthy CPS. Furthermore, the applicability of these solutions is demonstrated in the laboratory and into industrial environments to showcase secure connectivity solutions, traceability and security testing throughout the product lifecycle and consequently increase innovation capacity for AD and SP in Austria.

This section describes the contributing technical solutions toward a principal I4.0 demonstrator architecture as proposed by the project partners (*Figure 3*).

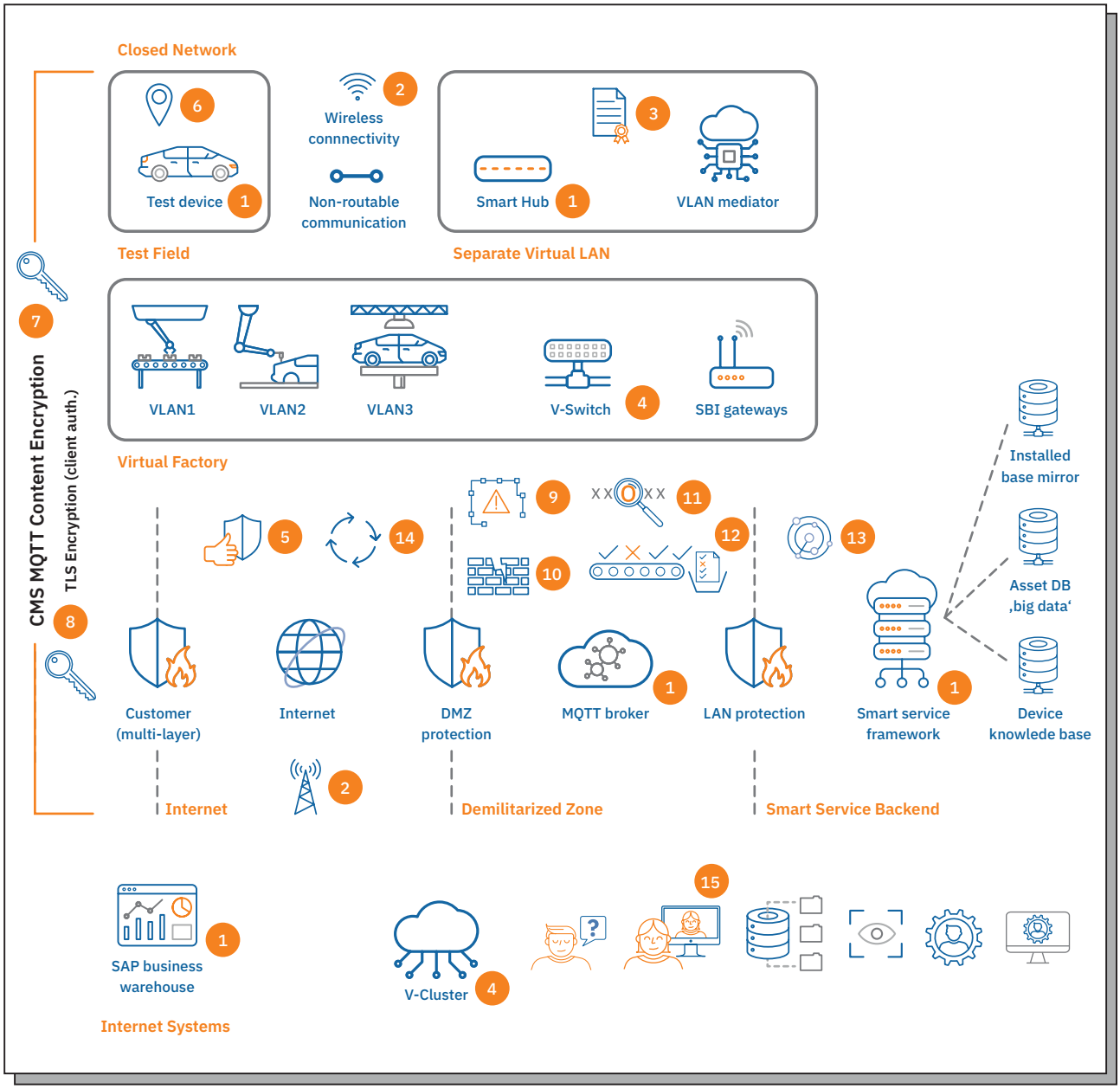

Figure 3: Principal I4.0 Demonstrator architecture and IoT4CPS contributing solutions

The numbers marked in *Figure 3* are showing the contributing technical solutions which have been identified as important for the Smart Production use case and explained below:

1. Data and Infrastructure
2. Industrial Connectivity Technologies
3. Integrity and Authenticity Check of Complex Systems
4. Security-by-Isolation and Link to the Virtual Environment
5. Dependability Design Methods
6. Trustworthy Localization
7. Communications Encryption
8. Content Encryption Using Forward Secure Key Exchange Protocols
9. Threat Modelling
10. Penetration Test Catalogue
11. Anomaly Detection
12. Automated Test Case Generation
13. Network Scanning Tools
14. Identity, Security and Safety in Product Lifecycle Data Management
15. Digital Twin Prototype

Based on this architecture, some of the technological components and techniques described in this section are integrated into main demo cases described in the final section of this document or into separate demonstrators (see IoT4CPS technical whitepapers and deliverables) to showcase that they are ready to be applied into real industrial settings.

4.1. Data and Infrastructure

The basic Smart Production infrastructure consists of three main components:

- The Smart Hub – responsible for connecting arbitrary non-routable devices to the Internet;
- The Message Broker – responsible for interconnecting different hubs to the backend;
- The Backend Framework (BEF) – responsible for carrying out big data analysis and issuing steering commands.

The security of this infrastructure lies amongst others in:

- Network security: all devices (1) are protected against network access – the smart hub and the Backend Framework do not have any open ports (they use only outbound connections to the broker) and are protected by firewalls; the broker has only the necessary port to receive connections from smart hubs and BEF open and is a DMZ;
- Communications Encryption: all communications (hub-to-broker and broker-to-BEF) are encrypted by state-of-the-art TLS (8).
- Content Encryption: in case of a compromised broker, the data traversing through it are still protected end-to-end from hub to DCF using content encryption (7);
- System Security: the devices run hardened operating systems;
- Hardware Security: sensitive keying material is protected by hardware security modules (HSMs).

4.2. Industrial Connectivity Technologies

Industrial connectivity has evolved from purely wired to wireless and is still undergoing a long-term transformation. The complexity and diverse nature of various industrial environments advocate the use of different technologies for different use cases.

Modern wireless architectures and protocols for radio connectivity aim to transform the industrial environments by providing remote equipment connection over long distances for control, monitoring and maintenance purposes, reduced wire installation costs, ease of mobility and portability within a smart industrial environment. The scale of the industries determines the technology that would fit its functionality. With the exponential growth of manufacturing and production, large scale industries have been prospering and 5G with its macro-cell coverage and mobility applications is at the helm of provisioning the required technologies.

In Deliverable 7.2 a wireless sensor network that has been implemented in a real smart production use case is evaluated by setting up a LoRaWAN network to provide usage feasibility for long-range applications

that can serve a fabrication environment which contains different types of sensors, tools and machinery. Experimental measurements show the impact of interference and reveal the trade-offs among the desired connectivity features by fine-tuning certain parameters.

4.3. Integrity and Authenticity Check of complex Systems

The foundations for security solutions of IoT setup are built upon edge nodes providing strong identity via secure hardware, public key infrastructure and certificates and auto-registration. The corresponding gateways protect communication via secure communication protocols and the cloud services provide access control solutions which enable strong user authentication as well as device authentication.

The important observation here is that the sum of the security requirements of the individual components might be smaller than the overall security requirements. In other words, just plugging everything together is not enough. The components need to be properly combined. A major concern in the security life-cycle is a question of how to securely recognize devices once they connect to the cloud and how to provision device keys that are needed to build those connections.

A common way to address these concerns in today's setups is to establish a Root of Trust (RoT) in the device. Such an RoT is a cryptographic identity used to uniquely identify a device, authenticate a device and start a chain of trust for the credentials stored in such a device. The RoT needs to be device unique, strongly isolated and tamper-resistant, with strong capabilities for cryptography and attestation. There are three main architecture options for secure RoT enablement, either via a secure microcontroller featuring an isolated HW RoT, an external secure element to act as a HW RoT or implement a SW based RoT and leverage isolation techniques such as trusted execution environments. In the case of HW based RoT, a core role is for silicon vendors to pre-provision the RoT credentials on the one hand but to also enable electronic delivery of RoT certificates from the silicon vendor database to the cloud service, to which the devices then finally need to connect.

These ingredients then allow the use of IoT components to be operated in non-controlled environments, for example at a semi-trusted vendor. Additionally, aspects such as SW and configuration distribution and update mechanisms can be created based on a chain of trust as mentioned above. The concept can also be used to realize commissioning or transfer of trust via attestation. Having in place such an architecture allows for end-to-end security via establishing secure channels to the backend that rely on pre-provisioned key material in the Root of Trust. This ensures confidentiality, integrity and authenticity of the received code updates. Platform security properties of the RoT ensure integrity for unmodified data transport and unmodified SW execution.

To prove to a customer that such an architecture achieves the claimed security properties at a certain security level, independent security evaluation and certification is a must. Such a certification includes, for example, the risk and threat analysis/threat modelling of a given scenario as well as an approved pen-testing catalogue. Currently, there is a lot of activity in the industry to translate existing and well-established

certification approaches to the IoT world. It will be crucial to monitor these approaches and to select appropriate ways to establish a maximum level of trust. Deliverable 7.3 deals with these issues and provides a report on the evaluation of the developed technologies against such aspects.

4.4. Security-by-Isolation and Link to the Virtual Environment

In the industry, many devices are connected via a network. For instance, some printers are in the same network as a production machine or the computers of the development department are in the same network as the webserver or the back office. This is more standard in SMEs, which statistically make up the lion‘s share of companies in Austria (more than 99% of all companies), and more often in start-ups (more than 12% of SMEs are start-ups) [SME18]. SMEs tend to avoid investing in necessary IT security measures. Particularly, Austrian companies refrain from investing heavily in their IT-security [STAT18]. Frequently, only necessary purchases are made and, therefore, both hardware and software are not state-of-the-art frequently. Furthermore, in-house processes and techniques that improve cybersecurity are also often outdated.

This gives an advantage to techniques that provide an adequate level of security but are also manageable and affordable for smaller companies or start-ups with different investment priorities. One such concept is Security-by-Isolation (SBI) which is based on the virtualization of the network and the virtual separation of the connected components. This concept requires only a few hardware components, which do not necessarily have to be on-site (except for the actual SBI-Box as shown in our demonstrator).

Splitting networks within an industrial environment becomes more and more important with a growing number of IoT devices. For security reasons, it is necessary to create distinct network areas that restrict the capability of IoT devices to communicate otherwise attack vectors will be opened. On the other hand, a smart production architecture must allow for easy handling of attaching, provisioning and remote maintenance of new equipment or machines, as well as data analytics for process optimization. SBI architecture can provide the appropriate tools for achieving the necessary trade-off for that purposes. Security can be created by cryptographically protecting the complete communication (e.g. by using a secure VPN) of the individual components and using modern authentication and authorization methods (Active Directory, two-component authentication). To facilitate users’ trust into the system, its components are made available to users as open source. Thus, its processes are transparent, the product itself can be further developed and there are no hidden surprises like backdoors in the software. Reliability is also ensured since operations can be guaranteed at any time with appropriate measures, in this case by redundant systems.

Through virtualization, this is easily possible with manageable cost and, thus, affordable for start-ups and SMEs. SBI concept, guidelines and testbeds for securing IoT products and for the secure set-up of production environments are provided in Deliverable 7.4. Also, a demonstrator based on SBI architecture that integrates other technical components of this project is provided. The latter is described in more detail in the next section.

5. DEPENDABILITY DESIGN METHODS FOR IOT

The IoT4CPS project provides guidelines, methods and tools for building dependable IoT systems. These methods and tools tackle challenges across all four CPS architecture layers: information layer, control layer, network layer and physical layer.

The physical-level tools and methods include sensor security measures for discovering faulty and hacked sensors as well as a forward-secure key exchange mechanism for improved cryptography. In an Industrial IoT context, enabling authentication and data provenance of data delivered from field level sensor networks is an important ingredient in achieving trustworthiness. The data and the respective networks are characterized by small volume and constrained bandwidth and computational resources and might also require data aggregation and sensor data fusion. On a network level, a recommender system for architects of dependable IoT systems helps the users to choose the appropriate protocols and system configurations depending on the security requirements and risks, development costs, as well as the nature of the environment and the target application and its scope. As a result, the system recommends to the user which IoT system is feasible concerning the current constraints.

An orthogonal approach to achieve dependability, apart from active protection measures against security threats and failures, is to apply methods that make the entire system more resilient to failures. A fault-tolerant system should be able to overcome internal failures and continue operating safely. On a platform-level, a specifically defined method called Self-Healing by Structural Adaptation allows the system to react also to failures not specifically considered during design-time, such as faults caused by functional, environmental or technological changes or zero-day malware. This technique leverages implicit redundancy to achieve resiliency to failures.

One of the security challenges in the field of localization, related to the I4.0 use-case is to prove that a device is in a specific location. Considering both a trusted scenario, in which a third-party employee is trustworthy and the environment is free of attacks, as well as the scenario where when the third-party employee cannot be trusted, one is drawn to the conclusion to suggest E-SALDAT, a novel low-power strategy to localize a device. E-SALDAT reduces the number of range estimation by from four to two, by using a single antenna from the localized node to estimate its distance to both antennas from the non-localized node. The method relies on an orientation provider which must be integrated into each of the nodes.

Regarding the application level, there are tools for a variety of relevant challenges in cyber-security. A secure system can be designed and developed only if security issues are well-identified and addressed appropriately in the early stages of the system development. That is considered a significant advantage because once the system is developed, it becomes harder to add security countermeasures. ThreatGet is a toolbox for Enterprise Architect, which is a widely used tool for Model-Based Systems Engineering. ThreatGet identifies, detects, and understands potential threats in the foundation level of system models. It supports the initial steps of the developing system process to guarantee the security-by-design. The correct security

requirement identification and efficient security requirement management are essential for any security engineering process. One can design, implement, and test a secure system only if he or she knows the exact security requirements. Achieving efficient requirement management is a challenge in system development. The Model-based Security Requirement Management Tool (MORETO) serves as a tool for security requirements analysis, allocation, and management using modelling languages such as SysML/UML.

IoT4CPS has also developed GSFlow, a tool for standard-based product development management. It is one of the results of a more general effort to develop tools to support model-based development approaches and Safety & Security by Design. The goal of GSFlow is to support the complete engineering lifecycle of safety and/or security-relevant systems based on pre-defined processes, by guiding the user through the development process. Its main objective is to make standard driven development straightforward, especially for companies that are unacquainted with functional safety and security standards.

Safety and Security are often analyzed separately. However, for achieving dependable IoT it is also important to consider their mutual dependencies. This topic is in the focus of the explored methods for Safety and Security Co-engineering. Deliverables D3.1 up to D3.7 of our project provide guidelines on hybrid methods for safety and security risk assessment and formalize it into a V&V pattern.

5.1. Trusted Localization

Localization helps in tracking and tracing any device in a remote location (field level) and obtaining its data wirelessly. Secure and accurate localization information is still an open challenge within the context of industrial IoT applications. Many of the existing localization attacks, such as man-in-the-middle, distance fraud and terrorist fraud, cannot be prevented by cryptographical means and require different countermeasures. Consequently, there is no free lunch for trusted localization and, depending on the attack model, a specific technology, approach or method is required to enable secure localization. Therefore, when designing/implementing trusted localization for a given IoT system, it is necessary to consider the potential attack vectors to select an appropriate localization technique.

Considering systems composed of devices whose objectives are to wirelessly obtain their correct distance from other devices/objects/people, the system model differs regarding the technology underlying the localization method. In the case of ranging-based localization, the system model consists of two or more devices. At least one of the devices denotes a verifier (or set of verifiers), which aims to estimate its distance to a prover using ranging methods. While the verifier is trusted, and its location is known this does not hold for the prover. If trilateration is used, at least three verifiers are needed to estimate the 2-D localization of a prover. In the case of LiDAR or camera-based localization, the system model consists of a single device, which aims to estimate its distance from an object/person/non-communicating device. In contrast to ranging, such methods do not require an explicit response to estimate the distance to other objects. In the case of GNSS (global navigation satellite system) the system model consists of a single device which aims for localizing itself.

When considering ranging measurements, many attacks are possible. Many of those were already mentioned and/or detailed in the Deliverable D3.3. The main technologies exploited were RFID, Wi-Fi, UWB and Bluetooth, which are key state-of-the-art technologies in the context of localization. Also, this deliverable introduces a new concept for addressing the Distance Enlargement Fraud (DEF), which was deemed to be unsolvable by the related literature. This concept uses the potential of coupling mechanisms for localization, more specifically for ranging between two devices. Similarly, to the basic idea behind distance bounding protocols, the proposed approach relies on the fact that electromagnetic fields propagate at the speed of light. The critical difference is that traditional two-way ranging of electromagnetic waves techniques use propagating waves, as in the proposed approach, the transmitted fields remain coupled to the transmitter/verifier, which can sense the moment in time when the transmitted field reaches the receiver/prover. In other words, the prover can only receive a signal if it is coupled to the verifier, thus disturbing the transmitted field. This disturbance can be sensed by the verifier and, therefore, used to detect possible frauds. Although coupling mechanisms have still a limited communication range, they have recently gained special attention, and their communication range is continuously increasing at a fast pace.

The work that has been done in our project illustrates a concept for the case of inductive coupling and evaluates it via numerical simulations. Deliverable D3.3 outlines further technical details and results. In parallel, we developed a method to localize a tag with a single anchor, namely E-SALDAT. Existing methods either require the specification of the surroundings of the indoor environment where the localization takes place, lack accuracy or lack efficiency. Those features are critical in a system that has to be implemented in industrial facilities and in Deliverable 3.4 we propose a module enabling trustworthiness among different stakeholders cooperating in a single task. For further details about this method, the interested reader may refer to Deliverable D3.4.

5.2. Scalable & Efficient Crypto algorithms

With the standardization of version 1.3 of the Transport Layer Security (TLS) protocol [TLS18], new features such as early data encryption were added to the protocol. Early data encryption enables clients and server to start encrypted application data transfer after the first message sent by the client. However, to achieve this feature, the client and server need to have a pre-shared key (PSK) which was either explicitly deployed or was generated during an earlier handshake and stored for later use. The use of PSKs, however, comes with the drawback that keys need to be stored securely. Especially in the context of constraint devices, securely storing these keys is non-trivial. Notably, with this approach one also loses forward-secrecy for the data transferred using early data encryption.

Recent work in the academic literature, such as the one by Derler et al. [BFE18], investigated a different approach to achieve the same features but without the need for PSKs and also without losing forward-secrecy concerning early data encryption. In [BFE18] the authors introduce the concept of Bloom filter encryption (BFE) which works like a typical public-key encryption scheme with the difference that the secret key is managed in a bloom filter. Whenever a ciphertext gets decrypted, the holder of the secret key punctures the key, meaning that the ability to decrypt this ciphertext afterwards is removed from the key.

Technically, this feature is achieved by mapping the ciphertext to indices in the Bloom filter, adding them to the bloom filter, and keys of the newly set indices are removed. If one tries to decrypt the same ciphertext again, the bloom filter will already contain it and the keys to decrypt no longer exist. As the Bloom filter inherently has a (controllable) false positive rate, this means that some ciphertexts cannot be decrypted. Bloom filter encryption can be transformed into a secure puncturable key exchange mechanism (PKEM). The puncturing mechanism achieves two features in this context: first, it provides forward-secrecy and second, it is already replay-attack resistant. Contrary to typical key exchange as performed in TLS, by using a PKEM the client does not need to wait for the server's answer before being able to encrypt application data. As long as the client knows the server's public key, the client can use the early data encryption, but instead of using a PSK, the key exchanged with the PKEM is used as the basis to derive the necessary key material. Therefore, it is no longer necessary to securely store PSKs on both sides.

The code necessary to deploy this feature is developed and presented in the Deliverables D3.6.1 and D3.6.2. The first Deliverable is concerned with the implementation of the BFE and PKEM scheme. In the Deliverable D3.6.2, the library developed in D3.6.1 will be integrated into a TLS library such as OpenSSL. Also, Deliverable D3.5 provides detailed descriptions of the cryptographic schemes such as signature schemes, public-key encryption, key exchange as well as authenticated encryption schemes. The TLS operates on the network layer and adds an overhead that needs to be taken into consideration in data transmission.

Additionally, Deliverable D3.4 elaborates on the functioning of the watermarking technique for its usage in industrial field-level sensors. Authentication and provenance of data are of utmost importance for reliable communication. Watermarking technique provides a lightweight stamp without additional data volume as required by cryptographic schemes. The lightweight security stamp feature makes it applicable for data authentication at the field level (sensor) networks. As described in Deliverable D3.4, Watermarks can be an alternative lightweight security measure ensuring authenticity and data ownership. Therefore it is increasing trust, which simplifies applications and in particular without additional data volume as required by message authentication codes or digital signature.

Watermarking has been widely used in digital multimedia to prevent copyrights of pictures and images and has evolved to be an efficient way to use in lightweight field-level sensors. The field-level sensors have different data types depending upon the type of data transmitted: Sequence data, Spatial Data, Spatiotemporal Data and Streaming data. The watermarks add information to the data payload and the addition is based on the amount of noisy environment the data channel is likely to be. The watermark is additionally inscribed to the least significant bit on the payload (or) on a side-channel where the alteration of data is not possible.

6. STRATEGIC SECURITY ASSURANCE

6.1. Threat Modelling

STRIDE threat modelling is an approach aiming to identify threats and vulnerabilities within the IT system architectures and was originally introduced by Microsoft as part of their Security Development Lifecycle (SDL) concept. Within IoT4CPS, the corresponding modelling tool was selected to model the main industrial use case and perform a security analysis process for self-awareness of the persistent threats observed in data transmission. The methodology is divided into six categories that are defined in the model such as Spoofing Identity, Tampering of data, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege. D4.2 explains in detail each of the identified threats and models a pattern structure to identify them.

6.2. Penetration Testing

Penetration testing is the process of testing computer systems as well as human resources (social engineering) to identify security threats and possible vulnerabilities. These tests can be performed from the inside and from the outside of the systems under test to ensure that all possible options of an attacker are covered. To perform more effective penetration testing and to keep the costs down, the IoT4CPS project pursued a strategy to perform a kind of grey-box penetration test obtained by the threats identified via the threat modelling process. More detailed information about this process including the comprehensive list of threats is covered by Deliverable D4.2.

7. ANALYTICAL TOOLBOX

7.1. Anomaly Detection

The analytical toolbox provides a set of tools to support anomaly detection for IoT-enabled CPS systems. It consists of a framework that allows training, evaluating and deploying anomaly detectors on data streams. The proposed stream analytics framework in the IoT4CPS use case has four main components: a streaming platform, a model server, a stream model executor, and a training environment.

The streaming platform (e.g. Kafka) serves as the central data hub. It enables the analytical models to consume data from data streams and make the result of the analysis available to other applications. A model server (e.g. mlflow) supports the administration of the analytical models, by tracking model configuration parameters and evaluation metrics in a traceable way, and allow the versioning, comparison and deployment of models. In the proposed framework, the analytical models (i.e. anomaly detectors) are deployed to a REST API, which will be used by the stream model executor to analyze the consumed data from the data streams. Finally, the training environment e.g. Python or R) is used for visualizing the data, as well as for training and evaluating analytical models. Training and evaluation may be performed on batch datasets or by replaying historical data streams.

The analytical toolbox distinguishes between three levels of data sources for anomaly detection: data from network traffic, data from operating systems and data from the hardware. At the network level, the data consists of aggregated TCP/IP information, like IP addresses or the number of packets sent, etc. At the operating system level, the data is mostly comprised of logs and application events. Finally, at the hardware level, the communication behaviour of hardware components and physical measurements, like e.g. the power consumption, are used as a data source to detect anomalies.

A demonstration of the analytical toolbox in the context of the Industry 4.0 use-case is using the following two datasets for anomaly detection: IoT4CPS main Industrial Demonstrator and Test case generation for MQTT brokers from a Research partner. For datasets that contain no anomalies (attacks or outliers), these are inserted manually. A detailed description of the developed methods is provided in Deliverable D4.2.

7.2. Automated test-case generation

Security testing in the area of IoT-based CPS is heavily influenced by the decentralized architecture used to implement the system under test as well as its interfaces and the communication protocols supported by individual connected cyber-physical objects. Testing, thus, has to target interaction and integration aspects. Approaches for automated test generation at this testing level range from generating random input (fuzzing) to model-based testing (MBT).

The work in IoT4CPS focuses on the generation of interaction sequences according to protocols used in IoT systems, which is a typical domain of MBT. However, instead of developing full models as a basis for testing, our approach experiments with a reduced interface model that can be integrated as a test driver. The driver provides a list of commands (e.g., protocol messages) that can be processed by established test case generators from functional testing to create interaction sequences. Applicable methods for generating sequences are based on random approaches, search-based strategies, genetic algorithms, reinforcement learning. Online feedback-directed testing determines viable sequences and avoids generating illegal sequences violating protocol constraints. It also creates sequences by executing each selected command during test generation and evaluating the feedback (response of the tested system) before adding them to the sequence. Thus, the approach can generate long valid sequences (positive tests) that achieve a deep coverage of internal states as well as sequences that lead to an invalid command call after some valid interactions (negative tests). Security issues are addressed in automated testing by augmenting the list of regular commands with the implementation of attack patterns obtained from publicly available catalogues like CERT or CVE (Common Vulnerabilities and Exposures). Implemented examples are the injection of potentially harmful input using malformed encodings, e.g. incorrectly UTF-8 encoded strings, to bypass validation logic. Other examples include illegal command sequences, invalid length specifications for payload data, or message flooding. Each implemented attack pattern can be directly triggered via the test driver.

A first version of the demonstrator for automated security testing has been built for secure data exchange for distributed connected devices in an untrusted environment. Test case generation is shown for data hubs using the MQTT messaging protocol in the setting of the Industry 4.0 use case. Security testing has been aligned with potential threats identified in a security risk assessment-based threat model, which may be used to control the selection and prioritization of the attacks applied in test generation. For example, an attack pattern is selected for inclusion in testing if a corresponding vulnerability has been specified in the model. The goal of the first version of the demonstrator has been to confirm the technical feasibility of the approach and to explore new opportunities for automation, such as the integration of threat modelling and security testing. The detailed approach of the developed techniques is provided into Deliverable D4.4.

8. OPERATIONAL SECURITY ASSURANCE

8.1. Reliable IoT Discovery and Classification

The Internet of Things (IoT) connects millions of devices of different cyber-physical systems (CPSs) providing the CPSs additional (implicit) redundancy during runtime. However, the increasing level of dynamics, heterogeneity, and complexity increases the system‘s vulnerability and challenges its ability to react to faults. Based on enhanced scanning algorithms for safe and reliable detection and classification of IoT devices and network topologies, the appropriate analytic steps to monitor and verify security and trust are performed, including processing the IoT data streams.

The IoT discovery and classification approach demonstrates that automated network mapping of a production site can contribute to obtain an authentic view of the actual network structure and connected equipment at any time. Up-to-date reports on the network topology help in administrating cyber-physical systems and provide the responsible CISO with the opportunity to easily check how the results align with the intended structure, which is very beneficial for an audit process. At the moment the IoT Discovery tool supports setups with Ethernet (IPv4 and IPv6), LoRa, and Bluetooth based communication by default, but due to its flexible architecture additional scanner and analyzer modules can be added very easily. Deliverable D4.5 provide a detailed description of the developed technical solutions for IoT discovery and classification.

9. PRODUCT LIFECYCLE MANAGEMENT AND DIGITAL TWIN

IoT4CPS addresses two aspects of IoT lifecycle data management: multi-stakeholder issues and cybersecurity (including privacy aspects of stakeholders). The tasks target the design and implementation of a research prototype and the definition of guidelines on what needs to be accounted for, at data level for "digital twinning" of cybersecurity and privacy features for future Connected and Automated Mobility and Smart Manufacturing applications, to offer preventive security measures and reduce safety accidents.

9.1. Identity, Security & Safety in Product Life-Cycle Data Management (PLCDM)

The autonomous CPSs of connected vehicles and industrial ecosystems need to operate in highly dynamic cloud environments, and when one component changes its behaviour or breaks down (e.g. due network problems or security attacks), the system should expose "smart" behaviour by recognizing the faulty situations and returning to its normal processing with minimum damage. Identity, security and safety, in the Automotive Industry have always been a concern for authorities, governance bodies, manufacturers and the public alike. However, a common standard allowing a complete integration of safety and security measures in the connected car's PLCDM is still missing [ENISA16].

Deliverable D5.4.1 "Identity, Security and Safety in Product Lifecycle Data Management" captures identity, security and safety aspects of two automotive manufacturing and automotive driving scenarios, towards the definition of an extended data model related to the entire lifecycle of connected vehicles. The data model presented in D5.4.1 integrates the security and safety features based on the use cases (as described in D5.2 "Product Lifecycle Data Management (PLCDM) Stakeholder Perspectives") and threats identified in the D4.1 "Automotive Ethernet Protection Profile" of IoT4CPS WP4 "Security Verification and Analysis". The resulting, extended data model ensures the inclusion of both multi-stakeholder and IoT-/ CPS-based assets (and their services) in the lifecycle of connected vehicles and adds the third cybersecurity perspective to it. With such a model, the aim is to enable "digital twinning" of the real-world situations and processes related to lifecycle phases in the Automotive Driving and automotive Smart Manufacturing sectors, while emphasizing the importance of a range of automotive safety and security indicators.

9.2. Digital Twin Concepts, Data Models and Prototype

To enable data acquisition, exchange and processing in IoT4CPS, we use the concept of a Digital Twin to model the data management architecture and employ data analytics to proactively address data security, privacy and safety of connected vehicles applications. This Digital Twin is designed to provide both monitoring capabilities of the connected vehicle's ecosystem, and reasoning over a diverse body of knowledge and data in order to enable adaptive behaviour for mitigating cybersecurity and safety-critical situations.

Deliverable D5.5.1 “Lifecycle Data Management Prototype I”, presents the conceptual model of the Digital Twin prototype and designs the architecture of the first Digital Twin prototype and a conceptual environment for testing the Digital Twin prototype as a virtual honeypot. After identifying stakeholders and IoT/CPS assets (devices and their services) in the system, the approach defines the data strategy to acquire a variety of datasets (“data in motion” collected from industrial and operational lifecycle phases and interaction within the connected car ecosystem, and “data at rest” with historical logs and static data and measurement). The design of such a prototype requires an effective data strategy to be put in place, and in parallel, it requires knowledge and understanding of policy and regulatory issues at national and international levels regarding smart vehicles, cybersecurity and safety.

The next step requires to perform relevant security and safety assessments and to prioritize tests, based on potential risks related to both stakeholders and assets, and criticality of services in the lifecycle. For example, it makes sense to start with security and safety assessment of those assets with the highest vulnerability (e.g. network exposure) or largest potential risk (e.g. drive control). The objective of such assessments is to examine all assets involved in corporate processes, gather detailed information about them and eventually, find associated vulnerabilities. The identified vulnerabilities need to be mitigated, which includes configuring and updating assets to strengthen their security and comply with corporate governance models and security standards. Once the proper security measures are established, relevant monitoring procedures need to be in place to ensure that the desired security and safety posture of the system remains in achieved. Furthermore, the system needs to be monitored for intruders through an IDS system or monitored for changes to identify any new vulnerabilities caused by newly introduced applications or missing security patches, or monitored to ensure that the integrity of the system is maintained even when it is used by the authorized users. These all are envisioned functionalities of the Digital Twin prototype.

The implementation details of the current, second Digital Twin research prototype in IoT4CPS are provided in “D5.5.2 “Lifecycle Data Management Prototype II”. The prototype is created to connect “loosely coupled” components (client applications) to share data with third parties, keeping stakeholder control over subsets of the data by the clients. It enables “data publishers” and “data subscribers” to connect through Kafka Streaming Applications, in order to exchange contractually agreed data streams. The source code of the prototype is released under a permissive open source license and can be found on the IoT4CPS internal GitLab instance. A fork on public GitHub has also been created with intention of providing access to the open-source code.

10. APPLICATION

One of the main objectives of IoT4CPS is to provide industrial demonstrators to showcase the integration of security concepts along the product life-cycle and across the value chain. Our industrial prototypes will provide guidance and inspiration by raising the awareness of the security issues arising over the lifecycle of the products, showing the applicability of the project findings and how these can tackle the challenges in the industrial domain and finally, by generating experience regarding sustainable real-world applications.

10.1. Bidirectional Connectivity for Vehicle Industrial Testing, Monitoring and Device Flashing/ Calibration (AVL)

Industrial automation also enhances its use-case to vehicular production units that provide monitoring and controlling of the basic vehicle sensors through the production plant. This facilitates the manufacturing process in terms of process automation, productivity optimization and predictive maintenance. The connectivity is done in an AVL demonstrator Device.CONNECT. The vehicular sensors connect to a smart hub placed inside the car that integrates all the different sensors to an integrated framework. The smart hub connects to a MQTT broker through either Cellular (or) Internet transferring information from the hub to a subscribed client. The client is a database server present in the production plant and is used to receive data from the broker and display it at the remote monitoring unit called Device.CONNECT Framework (DCF). The entire network provides a bi-directional communication for the production plant to effectively communicate and control the in-vehicle sensors.

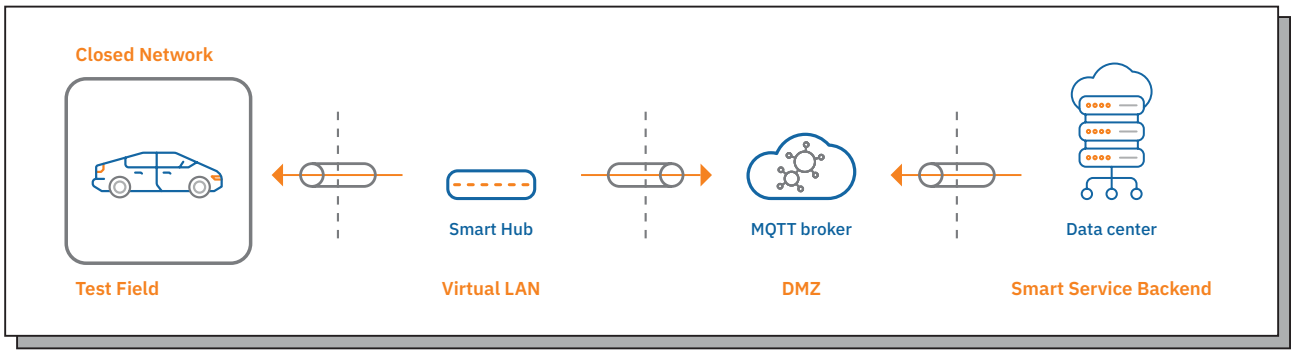

Figure 4: IoT4CPS AVL Device.CONNECT Architecture, in D 7.1

Figure 4 shows the data flow between the vehicle and the production plant. This is elaborated in D 7.1 under AVL's Device Connect Framework that provides a secure IoT platform for communication. The test-field is described as a vehicular component connected to a virtual LAN. The sensor data communicates to a broker through a DMZ firewall or X.509 certification for authentication purposes.

10.2. Benefits of Integration of WP3/WP4 into Device Connect Use-Case

Crypto Library

Cryptography has been considered the most secure way of data communication to date. One of the major protocols that provide a secure communication channel such that both authenticity and confidentiality of the transferred data can be ensured is Transport Layer Security (TLS). Cryptographic libraries are used to secure data over TLS communication. The TLS operates on the network layer and adds an overhead that needs to be taken into consideration in data transmission. Data communication encryption requires TLS to secure the transmission payload to prevent eves-dropping and system-level attacks.

Watermarking Technique

This technique has been used predominantly in digital multimedia to maintain their authenticity and copyrights. The same can be applied to sensor data to authenticate its real-time availability. The watermark feature can be added in the data payload to inform the receiver of the data authenticity.

Threat Modelling

Threat modelling is a software architectural level task under the strategic security assurance model that incorporates various methods of security. It is a technique for the security analysis process and self-awareness of the persistent threats observed in data transmission. A threat modelling tool identifies the threats and vulnerabilities within the IT system. The methodology is divided into six categories that are defined in the model such as: Spoofing Identity, Tampering of data, Repudiation, Information disclosure, Denial of Service, Elevation of privilege. The integrated solution analyses the traffic behaviour to predict any threats or vulnerabilities that could affect the system.

Penetration Testing

Penetration testing is used to generate test cases from the previously defined threat modelling. It is the process of testing computer systems as well as human resources (social engineering) to identify security threats and possible vulnerabilities. These tests can be performed from the inside and from the outside of the systems under test to ensure that all possible options of an attacker are covered. To perform a more effective and to keep the costs down for penetration testing, the IoT4CPS project pursues the strategy to perform a kind of grey-box penetration test obtained by the threats identified via the threat modelling process. The penetration test aims to specify guidelines and recommendations, that address the identified issues.

Automated Test-Case Generation

Building upon the penetration testing, the automated test case generation automates the reporting of security vulnerabilities thus automating the process. Applicable methods for generating sequences are based on random approaches, search-based strategies, genetic algorithms, reinforcement learning. The attack pattern is recognized by training datasets of the corresponding vulnerabilities and testing them through test datasets. Security issues are addressed in automated testing by augmenting the list of regular commands with the implementation of attack patterns obtained from publicly available catalogues like CERT or CVE (Common Vulnerabilities and Exposures).

Anomaly Detection in Network Traffic

This solution detects any unusual activities as anomalies with auto-encoder datasets to manage and deploy analytical models in an I4.0 environment.

10.3. SBI-based Virtual Factory for Secure Connection of Machinery, Robots, and Product Lines (X-NET)

Virtualization technologies offer ease of access through remote connections that connects multiple devices on the go. Large Industrial equipment is a combination of multiple devices connected and integrated. These devices can be specific to different vendors. Provisioning, maintaining and configuration should be efficient and remotely available. This is possible by isolating the devices specific to a vendor from the entire equipment through remote VPN connections without any interference to other parts of the machine. This virtualization through VPN's requires secure connections to prevent mishandling. This leads to a concept of Security by Isolation (SBI) for a Virtual Factory.

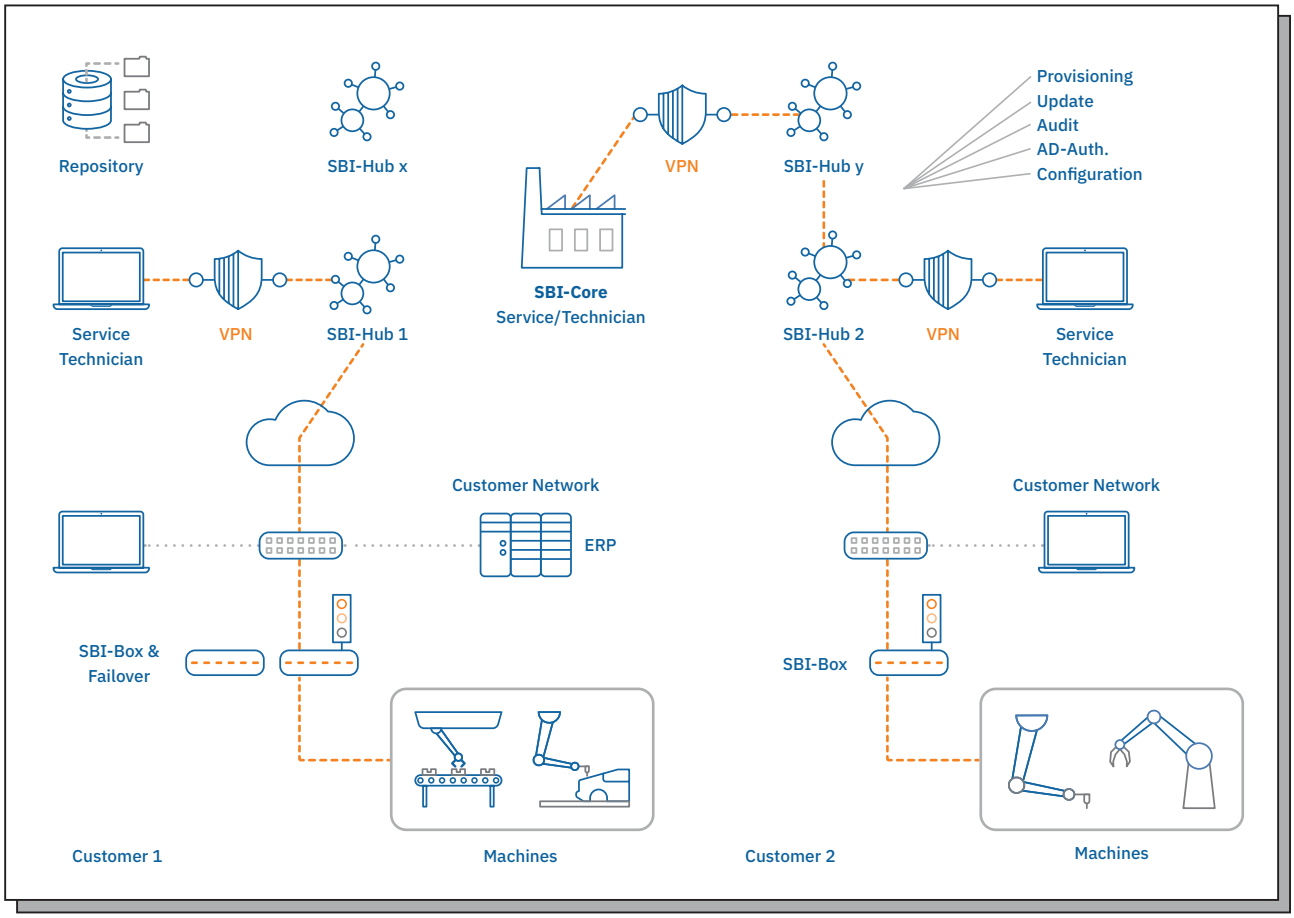

Figure 5: IoT4CPS Overview SBI-Concept, in D 7.1

Figure 5 shows the SBI-concept consisting of SBI-Core, SBI-Hubs, SBI-Boxes and the technicians to coordinate the whole process. The detailed elaboration of the architecture is presented in D 7.1. The main idea of the demonstrator is to show the virtualization in different work areas of a company. Furthermore, the process of IoT device components successfully isolated from one another to enable secure remote mainte-

nance of the component, with only access to their component and not the complete cyber-physical system is also considered This concept provides a roadmap to reduce the failure downtimes by a redundant design and virtual maintenance. Furthermore, standardized protocols like TLDP, VNC or X11 get converted into bidirectional video streams. This media discontinuity raises security and allows secure auditing.

10.4. Benefits of Integration of WP3/WP5 into SBI Virtual Factory Use-Case

The concept of SBI-Virtual factory has security and redundancy as the main prerequisites for its functionality. X-Net SBI-demonstrator will incorporate the solutions from WP3 and WP5 to achieve this.

Crypto Library

As described in Sec.4, it uses TLS 1.3 library to provide secure communication of the data payload being transmitted. The SBI-Core integrates this library into its data transmission mechanism and provides encryption through PSK's (private shared keys).

Digital Twin

The Digital Twin provides redundancy in data analysis through remote connections. It implements isolation and data sharing feasibility from a single machine to different stakeholders wherein each one has their own view on data, without the need to provide full access to the machine for all parties. It will be shown how to filter (and maybe combine) the live data streams for the different stakeholders - with the possibility to also access historical data stored within the messaging layer (up to some predefined storage duration, depending on the hardware capabilities).

REFERENCES

[SME18] Federal Ministry for Digitization and Business Location, SMEs Report 2018. Online available: https://www.bmdw.gv.at/WirtschaftsstandortInnovationInternationalisierung/Wirtschaftsstandort/KMU_Politik/Documents/Mittelstandsbericht%202018_barrierefrei_FINAL.pdf

[STAT18] Statista Austria: Survey on planned investments in IT security in Austria 2018. Online available: https://de.statista.com/statistik/daten/studie/979768/umfrage/umfrage-zu-investitionen-in-it-sicherheit-in-oesterreich/

[TLS18] Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC No. 8446). Internet Engineering Task Force. Internet Requests for Comments.

[BFE18] Derler, D., Jager, T., Slamanig, D., & Striecks, C. (2018, April). Bloom filter encryption and applications to efficient forward-secret 0-RTT key exchange. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 425-455). Springer, Cham.

[RPGB19] D. Ratasich, M. Platzer, R. Grosu and E. Bartocci, „Adaptive Fault Detection Exploiting Redundancy with Uncertainties in Space and Time," 2019 IEEE 13th International Conference on Self-Adaptive and Self-Organizing Systems (SASO), Umea, Sweden, 2019, pp. 23-32, doi: 10.1109/SASO.2019.00013.

[ENISA16] Cyber Security and Resilience of Smart Cars: Good Practices and Recommendations. Online available: https://bit.ly/2C3PLEb, Last accessed: November 02, 2019

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.