



D1.2

COLLABS System Architecture Definition

<i>Project number:</i>	871518
<i>Project acronym:</i>	COLLABS
<i>Project title:</i>	A COmprehensive cyber-intelligence framework for resilient coLLABorative manufacturing Systems
<i>Start date of the project:</i>	1 st January, 2020
<i>Duration:</i>	36 months
<i>Programme:</i>	ICT-08-2019

<i>Deliverable type:</i>	Report
<i>Deliverable reference number:</i>	DS-01-871518/ D1.2
<i>Work package contributing to the deliverable:</i>	WP 1
<i>Due date:</i>	JUN 2020 - M06
<i>Actual submission date:</i>	30/06/2020

<i>Responsible organisation:</i>	UNSPMF
<i>Editor:</i>	Dr. Srdjan Skrbic, Full professor
<i>Dissemination level:</i>	PUBLIC
<i>Revision:</i>	1.3

<i>Abstract:</i>	<i>This deliverable provides a specification of the conceptual architecture of the COLLABS platform. The COLLABS project aims at developing, demonstrating and supporting a comprehensive cyber-intelligence framework for collaborative manufacturing, which enables the secure data exchange across the digital supply chain while providing high degree of resilience, reliability, accountability, trustworthiness, and addresses threat prevention, detection, mitigation, and real-time response. These</i>
------------------	---

	<p><i>goals will be achieved using state-of-the-art technologies and making significant scientific and technological advances in several key relevant domains, including secure multi-party computations and homomorphic encryption, distributed deep learning and anomaly detection, distributed ledger technologies (blockchain) and smart contracts, and distributed remote software attestation.</i></p> <p><i>The specification of the architecture is based on a detailed analysis of reference architectures, state-of-the-art literature review, end-user requirement analysis, as well as general non-functional requirements and best practices.</i></p>
<p><i>Keywords:</i></p>	<p><i>Artificial Intelligence & Decision support; Information Security Technologies; Automation; Industrial Internet of Things (IIoT); Industry4.0; manufacturing; edge-to-cloud security; hardware-enabled security; machine learning; blockchain; behavioral analysis; accountability; trustworthiness</i></p>



The project COLLABS has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871518.

Editor

Srdjan Skrbic (UNSPMF)

Contributors (ordered according to beneficiary numbers)

Commissariat a L Energie Atomique et aux Energies Alternatives, CEA

Idryma Technologias Kai Erevnas, FORTH

Philips Consumer Lifestyle BV, PCL

Infineon Technologies Ag, IFAG

Advanced Laboratory on Embedded Systems SRL, ALES

University of Novi Sad Faculty of Sciences, UNSPMF

Sphynx Technology Solutions AG, STS

Thales Six GTS France SAS, TSG

Information Technology for Market Leadership, ITML

Universita Degli Studi Di Padova, UNIPD

Siemens AG, SAG

Renault SAS, REN

Harokopio University, HUA

Document Revisions & Quality Assurance

Internal Reviewers

1. ITML
2. REN

Revisions

<i>Version</i>	<i>Date</i>	<i>By</i>	<i>Overview</i>
1.3	11/05/2021	Natasa Vujnovic Sedlar, Srdjan Skrbic	Edited in accordance with the received internal reviews
1.2	29/04/2021	Natasa Vujnovic Sedlar, Srdjan Skrbic	Edited in accordance to reviews received during the technical review meeting in Feb 2021
1.1	30/06/2020	Srdjan Skrbic	Edited in accordance with the received reviews
1.0	09/06/2020	Srdjan Skrbic	Integrated minor inputs, abstract and executive summary written, references added
0.9	03/06/2020	Srdjan Skrbic	Integrated final inputs from partners, introduction and conclusion written.

D1.2 - System Architecture Definition

0.5	01/06/2020	Srdjan Skrbic	Integrated all section 2 inputs, section 3 content written, minor edits throughout the text
0.41	26/05/2020	Srdjan Skrbic	Integrated section 6 draft from ALES
0.4	26/05/2020	Srdjan Skrbic	Integrated partial third round inputs from ALES, FORTH, ITML, REN and PCL
0.3.1	05/05/2020	Srdjan Skrbic	Version of the document containing third round of requests for inputs
0.3	27/04/2020	Srdjan Skrbic	Version of the document containing second round of inputs
0.2	16/04/2020	Srdjan Skrbic	Version of the document containing first round of inputs
0.1	04/03/2020	Srdjan Skrbic, Zarko Bodroski	ToC.

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view - the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.



Executive Summary

This deliverable provides a specification of the conceptual architecture of the COLLABS platform. The COLLABS project aims at developing and demonstrating and supporting a comprehensive cyber-intelligence framework for collaborative manufacturing, which enables the secure data exchange across the digital supply chain while providing high degree of resilience, reliability, accountability and trustworthiness, and addresses threat prevention, detection, mitigation, and real-time response. These goals will be achieved using state-of-the-art technologies and making significant scientific and technological advances in several key relevant domains, including secure multi-party computations and homomorphic encryption, distributed deep learning and anomaly detection, distributed ledger technologies (blockchain) and smart contracts, and distributed remote software attestation.

The specification of the architecture is based on a detailed analysis of reference architectures, state-of-the-art literature review, end-user requirement analysis, as well as general non-functional requirements and best practices. Most of those review activities were performed within the deliverable 1.2 - positioning of COLLABS. Section 2 contains a summary of requirements specified in detail through use cases given by the three use case providers - ALES, PCL and REN and a high-level description of the infrastructure they possess. This document can be updated and refined during the project lifetime, as consortium members experience with the platform grows during the process of its implementation and integration.

In the next three sections, we first give description of four functional elements of the COLLABS framework: unified data exchange platform, data protection mechanisms, threat protection, detection and monitoring, and threat detection and response. After that, Section 4 presents a detailed description of COLLABS components provided by technology providers, divided into runtime components, and secure development and configuration components. Finally, Section 5 discusses how COLLABS components and technologies map to the four functional elements described in Section 3 by presenting three levels of security of the COLLABS framework.

A preliminary plan for demonstration, the experimentation protocol and pilot's execution with the evaluation guidelines are introduced in Section 6. Conclusions are drawn in the section 7. Information from this deliverable provides initial integration guidelines for the COLLABS Minimum Viable Product (MVP).



Contents

1. Introduction	10
1.1. Overview	10
1.2. Relation to other tasks and WPs	10
1.3. Contribution to the Scientific and Business Objectives	11
1.4. Structure of the document	12
2. COLLABS Requirements	13
2.1. COLLABS use cases	13
2.1.1. ALES	13
2.1.2. Philips	15
2.1.3. Renault	17
2.2. Requirements	21
2.2.1. Common Security Requirements	21
Identification and Authentication	21
Authorization	22
Logging, Monitoring and Accountability	22
Integrity Protection	23
Availability Protection	23
Confidentiality Protection	24
Deployment Qualities	24
2.2.2. Requirements Evaluation Strategy	25
2.2.3. Relationship between requirements and KPIs	25
2.3. Infrastructure	29
2.3.1. ALES	29
2.3.2. PCL	30
2.3.3. REN	32
Architecture overview	32
Industrial network security concepts	33
3. Functional elements	36
3.1. Unified data exchange platform	38
3.2. Data protection mechanisms	38



3.3. Threat Protection, Prevention and Monitoring.....	39
3.4. Threat Detection and Response	39
4. System Components	39
4.1. Runtime components	40
4.1.1. Andromeda Trusted Execution Environment	40
4.1.2. Traffic Analysis Component	41
4.1.3. Hardware Security Component	42
4.1.4. Fine-grained authorization	43
4.1.5. Distributed anomaly detection.....	44
4.1.6. Security infusion.....	45
4.1.7. 3ACEs	47
4.1.8. IoT secure wireless fingerprinting.....	48
4.1.9. ML structured (non)convex optimization and graphical models-based tools	49
4.1.10. Workflow-Driven Security Framework	50
4.1.11. Infrastructure to identify user	51
4.1.12. Infrastructure for remote attestation	52
4.1.13. Security assurance platform.....	54
4.2. Secure development and configuration components	56
4.2.1. Honeypot.....	57
4.2.2. DESYRE	58
4.2.3. FSV.....	59
4.2.4. Interactive visualization	60
5. Integration of Security Aspects.....	62
5.1. Hardware-enabled and device-level security (Level-1)	62
5.2. Inter-device level security based on distributed ledger technologies (Level-2) ..	63
5.3. Machine learning-based cognitive security level (Level-3)	63
5.3.1. Security of machine learning based models.....	63
5.3.2. Machine learning-based device fingerprinting and anomaly detection.....	64
5.4. End-to-end security aspects	65
6. Real-life industrial demonstration - pilots	67
7. Summary and Conclusion	70
References	71



List of Figures

Figure 1. The COLLABS architecture as seen in the proposal. 11

Figure 2. The PW4000 94-inch fan engine. 13

Figure 3. Reference Architecture. 14

Figure 4. Location of Drachten site in the Netherlands. 15

Figure 5. Example of mass-produced consumer goods at the Drachten site. 16

Figure 6. Global overview factory infrastructure. 16

Figure 7. Line control PC overview. 17

Figure 8. Renault in figures at the end of 2019. 18

Figure 9. Automated Guided Vehicules in Renault. 21

Figure 10 - Reference architecture 31

Figure 11. Renault corporate architecture. 32

Figure 12. Communication between levels. 33

Figure 13. Remote access use case. 34

Figure 14. Monitoring and threats detection. 35

Figure 15. COLLABS functional elements. 36

Figure 16. Runtime components 40

Figure 17. distributed and parallel computation testbed. 49

Figure 18. Secure development and configuration components. 57

Figure 19 DESYRE link to ALES pilot and interaction with other components 58

Figure 20. Cyber-Intelligence manufacturing framework for digital collaboration 62

1. Introduction

1.1. Overview

The goal of this deliverable is to provide a conceptual definition of the COLLABS framework architecture through multiple viewpoints: requirements (including use-case and infrastructural), functional components (data exchange; data protection; threat protection, prevention, and monitoring; threat detection and response), system components (runtime components; secure development and configuration components), and integration of security aspects (levels 1, 2, 3; end-to-end). The conceptual definition of the COLLABS framework architecture has been established having in mind the key industrial security needs and potential technology improvements that could be provided by technical partners, overall in order to meet targeted KPIs defined in the GA.

A key concern in COLLABS architecture design is communication between individual components at various levels. The somewhat outdated Purdue model [1] of control hierarchy, still in use today, stipulates rather strict division of components into zones: the enterprise zone (the business planning and logistics network), manufacturing and cell/area zone, and the safety zone. The zones (and levels within: level 0 - physical process; level 1 - intelligent devices; level 2 - control systems; level 3 - manufacturing operations systems; level 4 - business logistics systems; level 5 - enterprise network, possibly including the “outside” world line the World Wide Web) represent points of separation with rigid control of communication, to the point of complete lack of connections for security reasons. With the proliferation of IIoT and the ongoing merger of information technology (IT) and operational technology (OT), the Purdue model is being challenged in the sense that communication between levels and zones needs to be increased both quantitatively and qualitatively. COLLABS will take special precautions in this regard to enable secure communication and data exchange across levels, making an effort to operate directly on encrypted data wherever possible.

The system specification is based on functional and non-functional requirements, as well as use cases (including reference architectures) provided by members of the consortium. Runtime components are classified in two dimensions: by security level (level 1 - hardware-enabled; level 2 - inter-device; level 3 - machine learning and cognitive) and element of the smart manufacturing environment they belong to (digital supply network, smart factory, connected objects). We describe the foreseen interaction between the runtime components, as well as the runtime components themselves, the secure development and configuration components. Integration of security aspects throughout the three aforementioned security levels is also described.

1.2. Relation to other tasks and WPs

This deliverable is part of Work Package 1 (namely, “Setting the Scene: Project Set Up”). Work Package 1 consists of four tasks that examine and discuss the critical roles of security and resilience for collaborative manufacturing environments (Task 1.1), identifying security threats and adapting security components to real-life industrial manufacturing environments (Task 1.2), experimentation protocol - real life industrial pilots (Task 1.4), while Task 1.3 connects directly to this deliverable through analysis of technology convergence - COLLABS architecture revision and tools specifications.

Task 1.3 will propose a refined specification for COLLABS end-to-end architecture provided in the proposal (Figure 1) based on a thorough understanding of the industrial IoT challenges, cybersecurity requirements and innovative COLLABS technological offerings introduced in the previous tasks. The goal of the task is to set up the convergence of all needed technologies, namely cyber assurance and protection, IoT, machine (deep) learning, edge/cloud computing, blockchain and smart contract technologies, to ensure that COLLABS will reach its objectives. The outcome of Task 1.3 will be the direct starting point of Task 6.2, as well as the basis for virtually all forthcoming tasks. COLLABS technical specifications and architecture will

be continuously updated following the technical and business achievements of the project and will built on top of the latest version of Reference Architectures proposed by ECSO (RAMI4.0 and IIRA) for Industry 4.0.

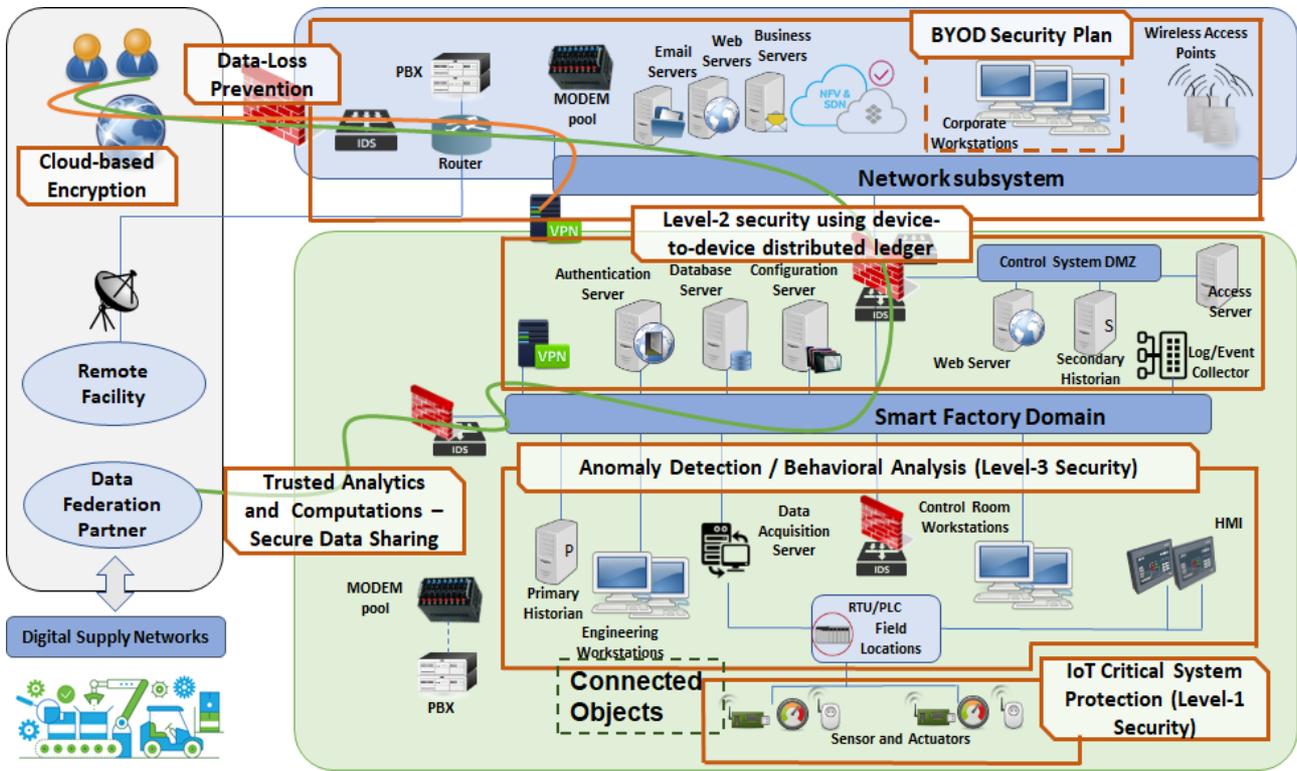


Figure 1. The COLLABS architecture as seen in the proposal.

1.3. Contribution to the Scientific and Business Objectives

This deliverable represents an important foundation for fulfilling all project objectives, directly or indirectly. Most notably, for Specific Objective #1, to develop and support a *comprehensive cyber-intelligence framework for collaborative manufacturing* that supports data exchange across the digital supply chain, threat prevention, detection, mitigation, and real-time response, the deliverable sets the groundwork by describing requirements, use cases, functional elements, components (and their interaction), and plan for demonstration.

Regarding Specific Objective #2, to provide scientific and technological advances in IIoT-based digital collaboration and security in the context of Industry 4.0, the deliverable describes how relevant technologies, such as cybersecurity and protection, secure multi-party computation and homomorphic encryption, (distributed) machine (deep) learning and anomaly detection, and distributed ledger technologies (blockchain) are orchestrated to work together within the framework.

The deliverable also directly contributes towards achieving Specific Objective #3, to provide novel tools and services for enabling collaborative manufacturing, by describing the ways how to leverage innovative secure execution environments, mechanisms related to security, privacy, accountability, trustworthiness, etc.

Specific Objective #4 will be addressed in this deliverable by describing a preliminary plan for real-life industrial demonstration and evaluation. Its purpose is to facilitate a secure exploration of IIoT's full potential in collaborative manufacturing environments and realize societal and industrial opportunities by

validating COLLABS framework in real-world settings via complementary use cases driven by large industries,

By establishing the groundwork for COLLABS framework implementation and contributing to the objectives described above, the deliverable will indirectly contribute to the remaining Specific Objectives: #5 consolidating international and European links, raising awareness, collaborating with standardizations bodies and ensuring the technology transfer of project's results, and #6 boosting the effectiveness of the European Security Union in the domains of secure collaborative manufacturing, by offering high TRL solutions (TRL 6-7), and by ensuring business continuity and long-term sustainability, during and after the project lifetime.

1.4. Structure of the document

The rest of the deliverable is structured as follows.

Section 2 focuses on COLLABS requirements, starting with concrete use cases from three consortium partners (ALES, Philips and Renault), followed by the requirements themselves in areas from identification and authentication, to deployment qualities. The section concludes with infrastructure descriptions from the same three partners.

In Section 3, we provide the description of four functional elements of the COLLABS framework: unified data exchange platform, data protection mechanisms, threat protection, detection and monitoring, and threat detection and response.

Section 4 gives a detailed description of all components and technologies provided by the project partners, divided into runtime components, and secure development and configuration components.

Section 5 discusses how COLLABS components and technologies map to the four functional elements described in Section 3 by presenting three levels of security of the COLLABS framework.

In section 6 we define a preliminary plan for demonstration: the experimentation protocol, the outlines COLLABS demonstration and pilot's execution, and the evaluation guidelines.

Finally, Section 7 closes the deliverable with a short summary and conclusion.

2. COLLABS Requirements

2.1. COLLABS use cases

2.1.1. ALES

In the following we introduce a use case developed in collaboration with and based on needs obtained from Pratt & Whitney Kalisz (PWK), Poland. Pratt & Whitney (P&W) is a world leader in the design, manufacture and service of aircraft engines and auxiliary power units. P&W employs state-of-the-art intelligent technologies and innovative manufacturing lines to produce the world's most advanced engine parts and deliver products more quickly and with higher quality. In particular in Kalisz (Poland) Pratt & Whitney owns the largest production factory in the aviation industry in greater Poland with more than 1500 employees. In those plants components and parts for aircraft engines are created and in particular this factory is the main supplier for UTC in complex gears, steering devices and engine main shafts. The factory is featuring its entrance in the industry 4.0, however not all the plants are at the same level: some plants are way more interconnected and advanced than the other, therefore this factory provides a good coverage for different levels exposing both legacy and current systems. One of the goals of this project is to better connect all the plants that compose Pratt & Whitney in order to exploit the data collected in each site to fine tune the overall management. Moreover increased data exchange between different Pratt & Whitney factories or between PW and suppliers/customer is also seen as a desirable improvement whenever it happens securely.



Figure 2. The PW4000 94-inch fan engine.

We use as starting reference the Purdue model, which we use to relate our reference architecture (presented in Figure 3Figure 1) with the other use case providers. Additional details and an extended presentation are available in Deliverable 1.2. Our reference architecture can be divided in Shop Floor (which represents Purdue layers PL 0,1,2), Manufacturing Zone (PL 3,4) and Enterprise (PL 5), which can be connected to cloud-based services through internet. Purdue layers 0,1,2 provide direct control of the manufacturing process and collection of production data (process data, product compliance), hosting the endpoint devices enabling smart manufacturing (smart sensors and actuators, PLCs, I-IoT controllers, local HMIs). The Manufacturing Zone is dedicated to process control by hosting SCADA and engineering workstations to control the products manufacturing stages and optimization. Finally, the Enterprise level contains all the services needed: managing orders, stock and deliveries, as well as collaboration with remote facilities and external parties (suppliers or maintenance providers).

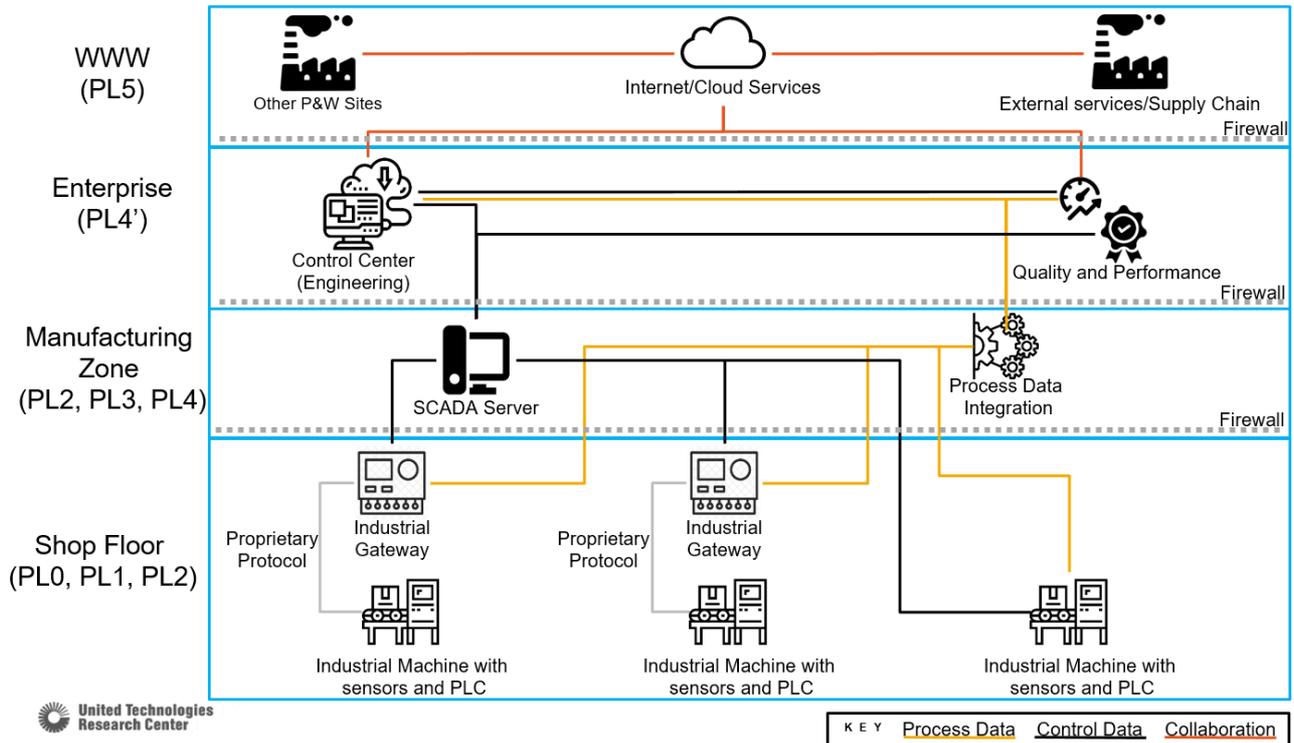


Figure 3. Reference Architecture.

Overview: the proposed scenarios describe the need of silos’ breaking across manufacturing sites to facilitate integration and collaboration at several levels, while keeping data security and confidentiality: (1) at shop floor level, to improve production KPIs (e.g. OEE) by collection of process data across multiple sites and more effective maintenance, (2) at process control level, to be able to reconfigure production more globally and manage stocks, and (3) at the Enterprise level, to facilitate data sharing across factories in the same group or partners in the supply chain or customers, inventory management, improved documentation of product compliance.

In the context of the described environment, we propose four specific scenarios and related challenges that are essential to realize the Industry 4.0 roadmap.

Scenario 1 (Controlled and secure remote maintenance): equipment maintenance shall be executed remotely, whenever possible, exploiting local employees support. This scenario requires external/third-party services to access the network and equipment, which guarantees strong segregation with respect to existing functions and data. During the execution of maintenance routines, design and process data shall be provably isolated to ensure protection of IP-sensitive information and integrity of the production process data. Any software/firmware updates shall be validated with fine-grained control and capability to remotely assess that the software stack integrity has not be compromised.

Scenario 2 (Controlled share of compliance data): compliance data is collected from the manufacturing process and is used as evidence of part manufacturing quality such as inspection of parts images and analysis of multiple parts measures against blueprints. Quality checks may be computationally expensive and require involvement of internal and external experts for improved assessment. Compliance data may be shared in a controlled manner within the enterprise and externally (potentially leveraging Cloud-based services), ensuring fine-grained control on authorized access to the information. When hosted on Cloud based services, design data shall be granted to not be leaked to other ongoing computations and, whenever possible, it would be preferable to guarantee data encryption while at rest and under analysis to avoid intellectual property or technical data loss.

Scenario 3 (Trusted compliance data share across the supply chain): the manufacturing of a complex and safety-critical system such a jet engine requires manufacturing, transfer, integration, and testing of a myriad mechanical and electronic parts. The manufacturing ecosystem collaborates in the supply chain to realize this coordination. Safety guarantees are provided by adherence of all parties to the highest standards of production and requires appropriate justification of due diligence from all parties. Compliance data and its traceability is essential and the interaction between supply chain parties is greatly facilitated by digital means. Automatization of these complex information flows requires to establish trust, guarantee integrity, and support traceability and accountability, potentially without relying on a single central authority.

Scenario 4 (Analysis of manufacturing performance at global scale): process data is collected from the shop floor and used for performance analysis and optimization at the Enterprise layer 5, closing the feedback loop onto the local factory. Extending this scenario across multiple factories and considering geographical distribution would enable several additional scenarios such as improving inventory/stock and ability to reconfigure production according to market. This scenario would leverage the enterprise network infrastructure. There are several security challenges, related to guaranteeing the flow of carefully selected data from shop floor to the external network, without disclosing sensitive information that would be bound to specific sites or national borders and guaranteeing not to enable attacks that may affect local networks to propagate globally or vice-versa.

2.1.2. Philips

Company context

What started in 1950 as a small shaver factory is now one of Philips' largest innovation and production sites in Europe. The Drachten site has a surface area of 280,000 square meters with approximately 2100 employees consisting of more than 40 nationalities.



Figure 4. Location of Drachten site in the Netherlands.

The site is very important for the future of personal health, driving key innovations. Highly advanced automated production methods are used to manufacture at low cost and stay competitive. Development departments also guide and steer the operations at production and supply centers across the world.

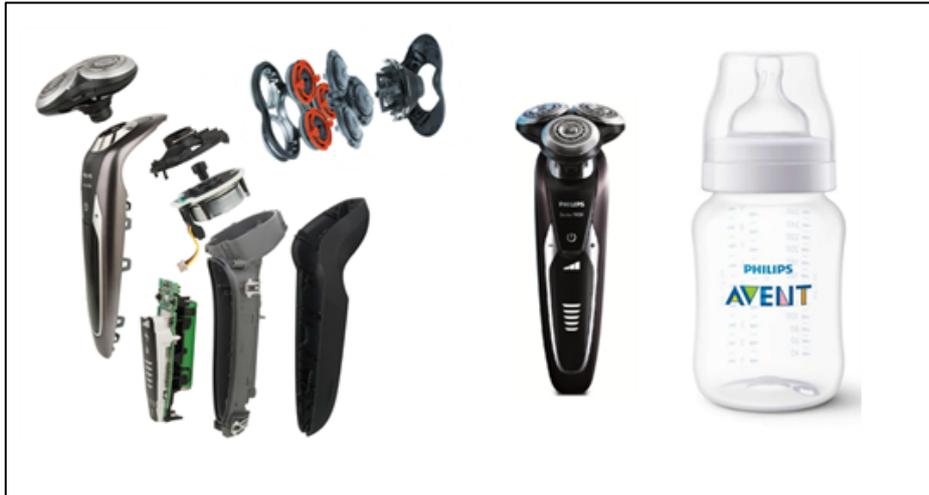


Figure 5. Example of mass-produced consumer goods at the Drachten site.

There is a dedicated factory infrastructure which facilitates the operation of a large and diverse amount of IT and OT equipment connecting over 1500 devices. A dedicated manufacturing IT department manages all these assets and services providing 24/7 support and maintenance.

Challenge number 1

The implementation scope for COLLABS is the area of the infrastructure referred to as machine networks; see Figure 6 to understand the positioning of a machine network. There are approximately 70 of these networks that exist in the environment.

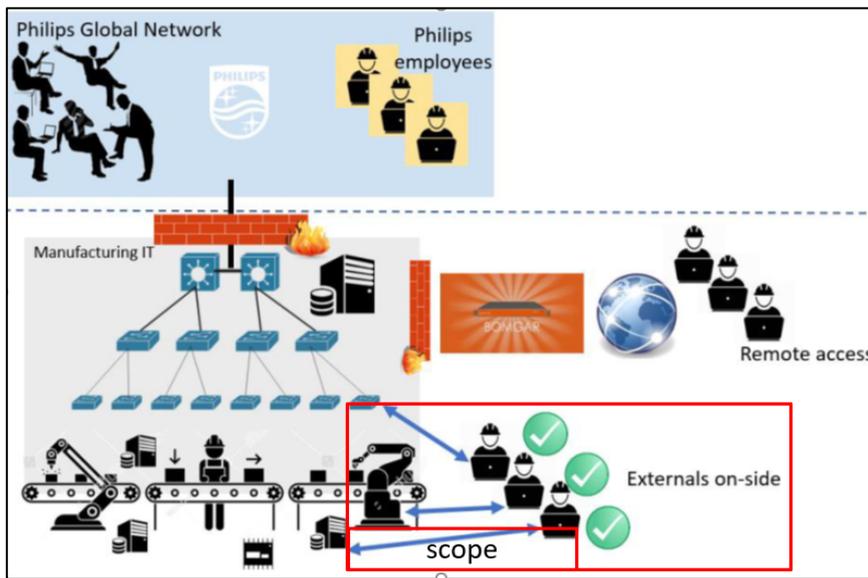


Figure 6. Global overview factory infrastructure.

Purchased production lines come with supplier operated integrated networking solutions. To separate these networks from the rest of the infrastructure, a multi-homed “line control PC” is used. This control PC connects to both the machine network and the factory infrastructure, which is illustrated in Figure 6 where the scope of control for manufacturing IT is outlined in red. The network in this overview is not managed by the manufacturing IT department due to organizational reasons. Because machine networks introduce a

level of high-risk situations, firewalls (including UTM and industrial protocol support) have been implemented.

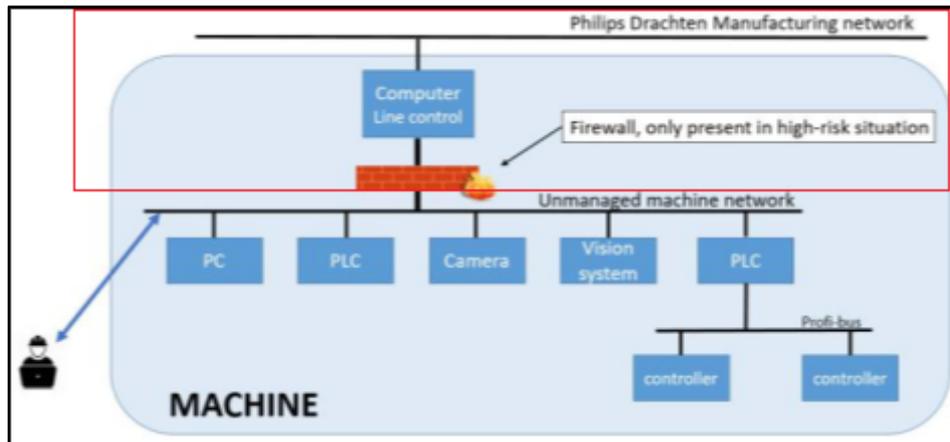


Figure 7. Line control PC overview.

Machine networks are varied by nature but generally contain a mixture of both IT and OT devices to be protected. The IT devices tend to be running (legacy) Windows operating systems. OT devices include PLCs, HMIs, SCADA, high performance imaging systems, presses, injection moulding devices et cetera.

The use case objective is the development of an easy to configure and low maintenance threat prevention/detection solution. This solution should be intelligent and self-learning to reduce the impact on IT operations. If the IT security provided is comparable or better than current solutions with lower required effort and cost, it will be considered a success.

Challenge number 2

Philips works closely together with equipment and tool suppliers to develop new manufacturing processes. As part of these collaborative activities, relevant data must be shared with partners. Besides suppliers, Philips often collaborates with consortium partners in European, national, as well as regional innovation projects. As part of these innovation projects, partners need (near real-time) process and equipment data from the shop floor. This type of collaboration requires a secure data exchange solution, for confidential and business critical data, which is flexible, works bidirectional and can deal with all sorts of (near real-time) machine and process data.

2.1.3. Renault

Company context

RENAULT Group, as a French multinational automobile manufacturer established in 1899, has known many of the industrial revolutions and had to reinvent itself to face the new challenges.

RENAULT represents 40 plants and 13 logistics sites over the world (Figure 8). All these sites are concerned by the COLLABS security challenges.

Since the rise of cybersecurity attacks and especially ransomware targeting industrial environments, RENAULT started a global program to upgrade all its plant to the state of the art of cyber security. COLLABS program will focus on the next steps.



Figure 8. Renault in figures at the end of 2019.

In the context of a highly connected industrial environment, driven by the new usage of the industry 4.0, digital collaboration enables new business opportunities, better data collection and better collaborations with external providers to always improve performance and enhance productivity. Several new initiatives are driven by the Industry 4.0 revolution, at each step of the supply chain and manufacturing process. These innovations involve new uses like inter-connection of billions of devices embedded in industrial systems, integration of new kind of IoT devices, new kinds of digital workstations, inter-connection of traditionally segregated systems and networks (OT/IT).

Use cases include different types of scenarios where the industrial network needs to interconnect with external suppliers, entities, or environments. This use case breaks one of the fundamentals of the industrial network security: the isolation, the segregation from external, Internet based networks.

All these new usages lead to an exponential increase in security risks and attack surface which are critical for productivity. Any interruption of the chain has a major financial impact. The risk can also be approached from the point of view of confidentiality but mainly from the point of view of the integrity and the availability.

Cybersecurity teams cannot prevent the deployment of these new initiatives which are necessary to improve the production process. Cybersecurity must find solutions to maintain the good level of security regarding the integration of many new IoT and IIoT devices, the interconnections with automatons and the multiplication of peer-to-peer connections that makes segmentation complicated.

The integration of more and more devices must also take into accounts the human organization to manage it. Plants have less and less people, devices must be secured by design, plug and work this means without complex configuration and security maintenance automated, such as the measures to simplify PKI management for billions of IoT devices.

Challenges

The different scenarios cover all the levels of the RENAULT infrastructure, from the OT/IoT/IIoT equipment's connected to the shop floor to the interconnection with external partners or cloud-based services.

Scenario 1 - Controlled and secured remote maintenance

RENAULT plants are scattered all over the world as well as the suppliers for industrial equipment. Maintenance operations, setting up production chains and supervision of industrial process shall be executed remotely:

- because plants have less and less local employees specialized for that,
- because suppliers do not have enough resources to send employees in plants,
- provide easy access to suppliers to perform maintenance operations,
- better reactivity to operate maintenance,
- and reduce presence in plants, reduce travel costs.

This scenario requires that an external supplier can have access, deep in the industrial network, to his equipment and only his equipment.

The solution shall permit a quick intervention of an external supplier with an efficient and fast validation process compatible with the mobility of the maintenance teams on large sites. The solution shall also limit the dependency of external suppliers to specific software or hardware components.

The objective is to cover all limitation of the current deployed solution.

Scenario 2 - Cloud-based architecture for industrial process

This scenario is probably the most disruptive scenario corresponding to the cloud-based smart factory of Industry 4.0 paradigm. It describes how the production process could be modified to use a cloud-based agent approach to create intelligent, collaborative, and more flexible industrial environment.

It covers many use cases where resources and services are progressively hosted externally in private/public cloud providers.

Industrial environment, processes, automatons and protocols have specific constraints related to network topology and efficiency. An industrial process requires a high level of availability, any interruption or delay could have critical impact on the production. For these reasons, cloud hosting for some parts of the industrial equipment does not seem applicable to the context and we will prefer local deployment of cloud-based technologies (virtualization).

Industry 4.0 concept also increases the need to collect more and more data from the manufacturing process. Data is collected for different domains of the industrial process regarding maintenance, performance, production, quality, and compliance. Domains collect data to allow predictive maintenance, to improve processes, to check parts compliance, etc.

The two main challenges of this scenario are:

- Virtualization of IT shop floor equipment, industrial PC desks, SCADA PC, etc.
- How to securely interconnect shop floor environment with cloud services considering the multiplicity of the cloud environment providers, the segregation between each infrastructure and the fined-grain control on the shop floor. And how to securely host sensitive services, applications, and data in public-cloud.

Scenario 3 - Assets management, conformity assessment and threat detection

Asset management refers to the identification and the cartography of all IT, OT and IoT devices present in the plant. Asset management is mandatory to evaluate the security level of the industrial network and to deploy an efficient threat detection architecture.

Asset management allows to identify the security level and the risk associated to each device and to identify their level of conformity defined in the corporate security policy.

In RENAULT plants, asset management and cartography are done with different tools and techniques that present limitations:

- An organizational process where each new device should be declared in a database with all associated data. Unfortunately, process is not always respected by misunderstanding, by lack of resources or sometimes because what started as a proof of concept, as a test that should disappear becomes a project deployed in production.*
- An agent deployed necessarily on new devices, mainly PC, and when possible on old ones, Installation of agent device by device requires human resources not available, sometimes the agent cannot be installed because there are not enough hardware resources or sometimes because the operating system is not supported anymore.*
- By using security appliances that try to deduct, monitoring the traffic on distribution switches, the inventory of the assets (protocols, MAC addresses...). Monitoring the traffic gives a limited view of the assets (limited to Purdue level 2) and require manual processing to sort, merge and analyse the results.*

This scenario requires new methods to automatically generate an inventory, to build a cartography of a whole industrial environment including its specificities. Solution shall include all levels of the Purdue model, from the OT devices (robots, automatons...) to IT and IoT devices.

Scenario 4 - Security of connected devices

Today's industrial environment is composed of OT devices, which are not designed to face cybersecurity threats, IoT devices, which present very weak security properties and IT devices that are more and more protected against cybersecurity threats.

The objective of this scenario is to globally increase the security of the industrial environment, providing security to low cost IoT (sensors, actuators, etc.) and industrial automation devices.

Identify the hardware security components required to ensure embedded trusted execution environments for connected devices, identify the cryptographic mechanisms and protocols depending on the constraints of each device, identify the software stacks ...

A typical use case of connected devices that are more and more deployed in plants are AGV (Automated Guided Vehicles) (Figure 9).



Figure 9. Automated Guided Vehicules in Renault.

The autonomous devices are critical for the production, because they are used to bring parts in the production line. Based on wireless connections they communicate with the industrial process and they are sensible to radiofrequency attacks and most of the time are not secured by design.

Another typical use case is the security of the PLC. Today, most security mechanism deployed in industrial devices (PLC, automatons...) are based on password for access control. Password management is a nightmare for local teams. Passwords should be different for each device, for each plant ... Security based on passwords ends with default passwords for all the devices.

The important topics of the scenario:

- Provide security by design capabilities to devices and make the devices easy to use, plug and work.
- Provide an effective convergence between OT and IT, with adapted protocols.
- Provides distributed, collaborative protocols with mutual authentication mechanisms between devices to make automated segmentation based on devices security policies.
- Security management of IT/OT devices during the whole lifecycle with a specific focus on automatic patching without disturbing production process.

2.2. Requirements

For the three demonstrators ALES (section 2.1.1), PCL (section 2.1.2), and REN (section 2.1.3) threat and risk analysis workshops have been conducted. The identified risks have been mapped to the common security requirements (CSR). Details on this process are provided in deliverable COLLABS D1.2 section 2.f.

In addition, deliverable COLLABS D1.2 provides further details for the requirements and highlights the references to the NIST SP800-171 Rev 2 [2] and IEC 62443 standards. This section provides a summary that points out the relevance to the respective demonstrator scenarios.

In the tables below, S1, S2, S3, S4 refer to use cases' scenarios (i.e., scenario 1, 2, 3, and 4) of the demonstrators introduced above.

The following requirements will guide technologies development in WPs 2,3,4 and their integration in WP5. In particular, an outcome of WP5 will be a mapping of technologies to the satisfied requirements, which will be useful to assess coverage and to drive the experimentation activities in WP6.

2.2.1. Common Security Requirements

Identification and Authentication

Identification and authentication of users is a key requirement of any system or framework. Concerning users, we refer to human users, technical (service) users, and devices. Please note that in many traditional OT environments, the authentication of users is often not enforced, as access to the cyber-physical systems

demands for access to the physical environment or restricted network zone. That means, access to systems here is often realised through restricted access to the overall environment. The convergence of IT and OT domains - e.g., in the case of a remote maintenance use case - is a game changer in this regard as closed and strictly controlled network zones must be made accessible to external partners. This demands for consolidating IT and OT security approaches. Hence, the following requirements CSR-01 and CSR-02 are crucial security concerns in a collaborative scenario (such as remote maintenance).

ID	Description	ALES	PCL	REN
CSR-01	Access to the system shall be authenticated and shall be granted strictly to the required machine/data. That demands for identification and authentication of users (humans, software processes and devices) prior to granting access.	S1	S1, S2	S1, S2, S3, S4
CSR-02	The system shall support state-of-the-art cryptography and management capabilities for protecting credentials.	S1	S1, S2	S1, S2, S4

Authorization

The following common security requirements address access control for components at all layers of the Purdue architecture. Though these requirements are quite common for IT domains, their implementation and enforcement in OT domains (and therewith at lower levels of the Purdue architecture) are challenging. In addition, the goal is to implement these requirements consistently across all levels, again, facing handovers between IT and OT domains. This demands for protocols and solutions that span all layers of the architecture.

ID	Description	ALES	PCL	REN
CSR-03	Timed Access: external (and if required also internal) access shall be restricted to the least-required time necessary to perform the required task.	S1	S1, S2	S1, S4
CSR-04	Least Privilege: any access is granted the minimum system authorizations and resources needed to perform its function.	S1, S2	S1, S2	S1, S2, S4
CSR-05	The system / components shall provide the capability to support the management of accounts and access control policies. Furthermore, they shall provide the capability to integrate into IAM (identity and access management) systems that allow the management of identifiers and policies.	S1, S2	S1, S2	S1, S2, S4
CSR-06	The system shall provide support for fine-grained access control (e.g., via attribute-based access control).	S1, S3	S1, S2	S1, S2, S4

Logging, Monitoring and Accountability

In case of collaborative manufacturing use cases with access to components at the lower levels of the Purdue architecture (i.e., at the layers of Connected Objects and Smart Factory), concise logging and monitoring needs to be in place. This is important for being able to provide evidence of actions so that root causes of potential incidents can be identified and analysed - on the fly or at retrospect. This is addressed by CSR-07. CSR-08 addresses the need of online monitoring for being able to trigger immediate actions and therewith to ensure robustness and availability of the overall system. CSR-09 addresses non-repudiation which is of particular importance for collaborative use cases: with different actors being engaged at the same time, it is not only necessary to being able to track and trace actions, but, also to provide proof for the originators of respective actions so that they can be hold accountable for. This is a key requirement for collaborative use cases that demand for a shared responsibilities-approach.

ID	Description	ALES	PCL	REN
CSR-07	Logging: Activities, i.e., access to assets in particular by externals and/or administrative users, shall be tracked and logged. In particular security relevant audit logs shall be created and maintained.	S1	S1, S2	S1, S3, S4
CSR-08	Monitoring: Activities (in particular security relevant activities, e.g., of human or technical users) shall be monitored and the system shall provide capabilities to identify security relevant events (e.g., out of log data and online user monitoring). It shall support alerting and proactive measures.	S1	S1, S2	S1, S3, S4
CSR-09	Accountability and non-repudiation: Activities shall be traceable and auditable so that users cannot successfully dispute the origin of their actions.	S3	S1, S2	S1

Integrity Protection

The following data and system integrity protection requirements address the specific needs of operational environments. For OT systems, it is necessary to always be able to determine and to specify a stable, well-defined state. For example, a production processes that must ensure that the manufactured goods have a fixed quality. This also holds true for all use cases that are analysed in the context of the COLLABS project. CSR-10 and CSR-12 focus on the integrity of the overall system / environment while CSR-11 is concerned with data integrity protection. The latter one applies to both, data used or produced by the system (like configuration settings, recipes, or the like) as well as security relevant information like log data. Hence, CSR-11 is also closely related to logging, monitoring and accountability requirements presented in the previous section.

ID	Description	ALES	PCL	REN
CSR-10	System integrity protection: the system shall protect against unauthorized manipulation or modification, e.g., modification of the equipment, software, user sessions, or network topology	S1	S1, S2	S1, S4
CSR-11	Data integrity protection: the system shall protect against unauthorized manipulation or modification of data, e.g., audit log information, production data, component configuration data, control data (recipes)	S1	S1, S2	S1, S2, S4
CSR-12	System integrity protection: the system shall be based on baseline security configurations for components (including hardware, software, firmware).			S3, S4

Availability Protection

Through collaborative manufacturing use cases, new attack vectors and therewith risks for existing OT environments arise. The following common security requirements highlight the importance of ensuring availability of the overall system even when new access patterns (like remote maintenance) shall be supported. CSR-15 not only defines a security requirement but also, implicitly, introduces an additional use case that shall be supported: remote patching and firmware updates of components. This requirement is relevant in online scenarios for making sure systems are kept up-to-date and security vulnerabilities are fixed as early as possible to mitigate the risk of an extended attack surface.

ID	Description	ALES	PCL	REN
CSR-13	The system shall be protected against system/service degradation (e.g., individual components); e.g., protection against denial-of-service.	S2, S3	S1, S2	S1, S2, S4

CSR-14	Data availability shall be ensured, e.g. protecting against loss of access to production data, component configuration data, control data and audit log information.	S2, S3, S4	S1, S2	S1, S2, S4
CSR-15	The system shall support online patching and update capabilities.			S4
CSR-16	The system shall provide a fail-safe configuration. I.e., in case of an unexpected event or error, the system shall go to a safe state (provide resilience).			S2, S4
CSR-17	Security functionality needs to be self-contained and free from side-effects on the production. That is: any failure in security mechanisms shall not have adverse effect on availability and/or performance (e.g., with regard to real-time requirements).			S2, S4

Confidentiality Protection

The following requirement CSR-18 addresses the need to protect data confidentiality, both, at rest and in transit. Again, likewise to the previous requirements, it shows that implementing the requirement across the different network zones of the Purdue architecture represents a challenging task which COLLABS aims at providing answers for (e.g., refer to task T2.2).

ID	Description	ALES	PCL	REN
CSR-18	Protection of confidentiality of data in transit and at rest shall be supported. In particular, confidentiality of data transferred to and managed in the Cloud should be protected.	S2, S3, S4	S1, S2	S1, S2

Deployment Qualities

The following common security requirements address security of operational qualities. That is, how COLLABS components and the overall framework can be deployed and integrated into collaborative use cases that span multiple organisations. Hence, requirements like CSR-21 (multi-tenancy) represent a crucial need to support COLLABS use cases.

ID	Description	ALES	PCL	REN
CSR-19	The system / components shall provide the capability to enforce mutual compliance with other system / components, based on shared security policies. In order to comply to a specific security policy, systems/components' capabilities need to fulfil the security rules and requirements specified by the respective policy.	S3		S3, S4
CSR-20	System shall provide plug-and-work security configuration based on collaborative and baseline security policies, thus limiting manual and recurrent configurations (e.g. certificate updates) reducing the risk of security threats cause of (e.g., manual) misconfiguration.	S3		S4
CSR-21	Multi-tenancy: When integrating resources that are used by multiple tenants/users (e.g., cloud environments), those shared resources shall support tenant separation / process isolation.	S2, S4	S2	S2
CSR-22	Network Segregation: The system's network topology shall support network segregation to limit the attack	S1, S3	S1	S1, S2, S4

surface by providing network segmentation and zone boundary protection.
 Reusable baseline security configurations supporting automated deployments and network topology hardening shall be provided (infrastructure-as-code).

The CSRS listed in this section have been inferred based on the results of a threat and risk analysis that was conducted for the three industrial COLLABS use cases. Though at the first glance these requirements seem to be quite common security requirements which apply to most applications - e.g., referring to data security and authentication and authorization- addressing them in the context of an integrated but at the same time highly distributed and in particular cross-organizational system architecture is quite specific and has not been sufficiently solved so far. That is, COLLABS not only aims at the security of individual, stand-alone components. Instead, providing a security framework for collaborative use cases is what determines the research direction of COLLABS. Hence, solving these requirements will support users in

- securely connecting objects at the shop floor level,
- ensuring secure information flow across the different (network) layers of an industrial site
- implementing a holistic security approach for industrial use cases, and even
- securing collaborative use cases across organizational boundaries.

2.2.2. Requirements Evaluation Strategy

COLLABS aims at providing technical components and a framework to address the requirements of the representative industrial use cases. That means that COLLABS components presented in this document contribute to fulfilling the introduced common security requirements (CSRs). In general, the evaluation of CSRs is handled by the experimentation protocol that evaluates the achievement of the overall objectives that are represented by key performance indicators (KPIs), impact key performance indicators (iKPIs), and common security requirements (CSRs). The experimentation protocol was introduced in deliverable D1.2, section 3 (“Experimentation Protocol”) and is refined in deliverable D6.1 (named “Demonstration - initial execution and evaluation”) with a detailed assessment process being introduced, there. As will be shown in D6.1, we will map COLLABS’ components to CSRs and describe individual evaluation strategies to prove their validity. Furthermore, to demonstrate the validity of CSRs for the overall COLLABS framework, framework and use cases represent additional evaluation scopes that are taken into consideration. KPIs, iKPIs, and CSRs will be continuously monitored, and the achievements be documented as part of WP6 deliverables. We refer to deliverable D6.1 for details on the defined experimentation protocol.

2.2.3. Relationship between requirements and KPIs

After the tasks related to the definition of CSR, the further course of thinking went in the direction of mapping the components provided by technology providers to the defined CSRs. On the one hand, this mapping is a continuous process, and on the other hand, the system architecture itself, as well as the list of components, is subject to changes during the project. The first table shows the mapping of CSRs to the system components provided and described in this deliverable that are related to fulfilling requirements defined by a specific CSR.

A detailed analysis shows that there is a good match between the components and the CSRs, so that all CSRs are covered with at least one component, and often with several, with the exception of CSR-22. CSR-22 remains defined as a requirement, but the components that implement the appropriate functionalities will be defined in later stages of the project, so that some of the existing components will take over this function or additional components will be defined for that purpose.

A much more detailed description of the relationship between CSR, components and KPIs will be defined in the deliverables of work package 6. Defined documentation approach implies that for each individual CSR, additional mappings to components are defined and updated with a description of how the defined components meet the prescribed requirements, including defining measurement points for monitoring progress, strategies, and evaluation criteria, as well as a baseline for comparison and testing.

Table - Mapping between CSRs and components.

CSR	Component name
CSR-01	Interactive visualization Workflow-driven security framework (WDSF) Hardware security component Fine-grained authorization IoT Wireless fingerprinting ML S(N)C and GMS tools
CSR-02	Interactive visualization Hardware security component Fine-grained authorization
CSR-03	Workflow-driven security framework (WDSF) Infrastructure to identify user
CSR-04	3ACEs Workflow-driven security framework (WDSF)
CSR-05	Workflow-driven security framework (WDSF) Hardware security component Security Assurance Platform Fine-grained authorization
CSR-06	Fine-grained authorization
CSR-07	Workflow-driven security framework (WDSF) Security Assurance Platform Infrastructure to identify user
CSR-08	Security Infusion 3ACEs Security Assurance Platform IoT Wireless fingerprinting ML S(N)C and GMS tools Distributed Anomaly Detection Traffic Analysis Infrastructure to identify user
CSR-09	Security Infusion Workflow-driven security framework (WDSF)
CSR-10	3ACEs Hardware security component Infrastructure for remote attestation Security Assurance Platform Distributed Anomaly Detection FSV Andromeda
CSR-11	3ACEs Hardware security component Infrastructure for remote attestation Fine-grained authorization FSV Andromeda
CSR-12	Hardware security component Infrastructure for remote attestation Andromeda
CSR-13	Hardware security component Infrastructure for remote attestation Security Assurance Platform Fine-grained authorization
CSR-14	3ACEs Infrastructure for remote attestation Fine-grained authorization
CSR-15	Security Infusion Security Assurance Platform

	Fine-grained authorization Andromeda
CSR-16	Infrastructure for remote attestation
CSR-17	Security Assurance Platform Fine-grained authorization
CSR-18	3ACEs Hardware security component Fine-grained authorization Traffic Analysis
CSR-19	Workflow-driven security framework (WDSF) Hardware security component Fine-grained authorization FSV
CSR-20	Workflow-driven security framework (WDSF) Hardware security component
CSR-21	Interactive visualization Fine-grained authorization FSV Andromeda
CSR-22	None

In addition to the mapping shown, it is worth noting that the component DESYRE is a component that has been proposed by ALES for their internal use only. It supports the setup and execution of the demonstration as well as the configuration of the different scenarios. It does not address any CSR nor KPIs.

The connection between CSRs and KPIs is defined through the system components. The following table shows the mapping between components and CSRs, the same that is shown in the previous table, but so that the table is now sorted by components. Another column has been added to the table defined in this way, showing mappings of the appropriate row to KPIs. Analysis of KPIs has shown that there are KPIs that cannot be mapped to a particular set of CSRs or components because they relate to the system as a whole. These are the following KPIs: iKPI-1.1, iKPI-1.2, iKPI-2.1, KPI-1.1, KPI-3.1, KPI-4.3, KPI-4.5, KPI-5.1. They are not shown in the table below.

In this way, this key table connects CSRs, KPIs that are affected by each individual CSR and components that on the one hand fulfill the requirements prescribed by CSRs, and on the other hand affect the fulfillment of the corresponding KPIs.

As before, a much more detailed description of KPIs and their relation to components will be defined in the deliverables of work package 6. Defined documentation approach envisages that for each individual KPI we provide updated mapping to components, description of this connection between them, strategy, and criteria for KPI evaluation, measurement points for monitoring progress, etc.

Table - mapping between components and KPIs

#	Component Name	Partner	CSRs	KPIs
1	Andromeda	FORTH	CSR-10 CSR-11 CSR-12 CSR-15 CSR-21	KPI-3.1 KPI-4.1
2	Traffic Analysis	FORTH	CSR-08 CSR-18	KPI-2.2 KPI-4.1
3	Hardware security component	IFAG	CSR-01 CSR-02 CSR-05 CSR-10 CSR-11 CSR-12 CSR-13	KPI-1.6 KPI-2.3 KPI-4.1 KPI-4.5 iKPI-5.1 iKPI-5.2

			CSR-18 CSR-19 CSR-20	
4	Fine-grained authorization	TSG	CSR-01 CSR-02 CSR-05 CSR-06 CSR-11 CSR-13 CSR-14 CSR-15 CSR-17 CSR-18 CSR-19 CSR-21	KPI-1.6 KPI-2.3 KPI-4.5 iKPI-1.5 iKPI-5.1 iKPI-5.2
5	Distributed Anomaly Detection	TSG	CSR-08 CSR-10	KPI-1.3 KPI-2.3 KPI-3.3
6	Security Infusion	ITML	CSR-08 CSR-09 CSR-15	KPI-1.3 KPI-1.4 KPI-1.6 KPI-3.3 KPI-4.1 KPI-4.5 KPI-4.6 KPI-6.2 iKPI-5.1 iKPI-5.2
7	3ACEs	ITML	CSR-04 CSR-08 CSR-10 CSR-11 CSR-14 CSR-18	KPI-1.3 KPI-4.5 iKPI-5.1 iKPI-5.2
8	IoT Wireless fingerprinting	UNSPMF	CSR-01 CSR-08	KPI-2.2 KPI-3.3 KPI-4.1
9	ML S(N)C and GMS tools	UNSPMF	CSR-01 CSR-08	KPI-1.3 KPI-1.4 KPI-2.2 KPI-2.3 KPI-3.3
10	Workflow-driven security framework (WDSF)	SAG	CSR-01 CSR-03 CSR-04 CSR-05 CSR-07 CSR-09 CSR-19 CSR-20	KPI-1.6 KPI-4.5 iKPI-1.5 iKPI-5.1 iKPI-5.2

11	Infrastructure to identify user	UniPD	CSR-03 CSR-07 CSR-08	KPI5.2 KPI2.1 KPI3.2 KPI4.6
12	Infrastructure for remote attestation	UniPD	CSR-10 CSR-11 CSR-12 CSR-13 CSR-14 CSR-16	KPI-1.6 KPI-4.5 (KPI-4.6) iKPI-5.1 iKPI-5.2
13	Security Assurance Platform	STS	CSR-05 CSR-07 CSR-08 CSR-10 CSR-13 CSR-15 CSR-17	KPI-1.6 KPI-4.1 KPI-4.5 KPI-4.6 iKPI-5.1 iKPI-5.2
14	Honeypot	FORTH	CSR-08	
15	FSV	ALES	CSR-10 CSR-11 CSR-19 CSR-21	
16	Interactive visualization	ITML	CSR-01 CSR-02 CSR-21	KPI-1.6 KPI-4.1 KPI-4.5 KPI-4.6 iKPI-5.1 iKPI-5.2

2.3. Infrastructure

2.3.1. ALES

The reference architecture validated with Pratt & Whitney Kalisz (PWK) is shown in Figure 3 and represents the high-level data flows required by PWK to fully transit to the Industry4.0 interconnection model. Here, follows a division in zones of the architecture and its mapping to the corresponding level(s) in the Purdue model [3].

Zone Name	Description	Purdue Level
Shop floor	This zone, where programmable logic controller (PLC) and industrial equipment are placed, is dedicated to direct control and sensing. Equipment can communicate with the manufacturing control layer through industrial gateways, if they support ICS/SCADA protocols (e.g. BACnet, Profibus), or be directly connected to the manufacturing layer, if they support industrial TCP/IP communications (e.g. Industrial Ethernet, ModBus/TCP).	PL0, PL1, PL2
Manufacturing zone	This zone, where supervisory control and data acquisition (SCADA) servers are placed, is dedicated to control and coordination of all the shop floor equipment. Through human machine interfaces (HMI) it is possible to monitor production and provide input for local control of the shop machines. Besides, this layer is responsible to collect, integrate and share process data from shop floor equipment to upper layers.	PL2, PL3, PL4
Enterprise	This zone hosts functions controlling the entire production at a higher level of abstraction, such as the engineering functions and	PL4'

	<i>the quality & performance control functions leveraging process data incoming from the manufacturing zone. Notice this level is not shared across different production sites which are instead connected with each other using cloud services through the world wide web.</i>	
<i>World Wide Web</i>	<i>This zone is outside the enterprise and supports connectivity with other manufacturing sites as well as partners in the supply chain. Through the corresponding infrastructure, it is possible to connect and share data across manufacturing sites or request external services such as maintenance or supplies.</i>	PL5

Notice that each zone is isolated from the other by firewalls that are set to avoid unauthorized information flows.

2.3.2. PCL

The Philips Drachten architecture can be mapped to the following zones.

Zone #1: Shop floor (Purdue level 0,1,2): this zone, where programmable logic controller (PLC) and industrial equipment are placed, is dedicated to direct control and sensing. Equipment can communicate to and from the manufacturing zone through a “line control pc” (see scenario 1) which is further secured using an industrial firewall (including UTM and industrial protocol support). Through human machine interfaces (HMI), it is possible to monitor production and provide input for local control of the shop machines

Zone #2: Manufacturing zone (Purdue level 3,4): this zone is dedicated to control and coordination of all of the shop floor equipment. This zone is also responsible for collecting, integrating, and sharing process data from shop floor to upper layers. All centralized IT systems supporting the production process in the plant are found in this zone.

Zone #3: Enterprise (Purdue level 5): this zone hosts functions controlling the entire production at a higher level of abstraction, such as the engineering functions and the quality & performance control functions leveraging process data incoming from the manufacturing zone. The plant office network as well as interconnections with other corporate sites are found here.

Zone #4: Internet (DMZ) (Purdue level 5): this zone is outside the enterprise and supports connectivity with other manufacturing sites as well as partners in the supply chain. Through the corresponding infrastructure, it is possible to connect and share data across manufacturing sites or request external services such as maintenance or supplies.

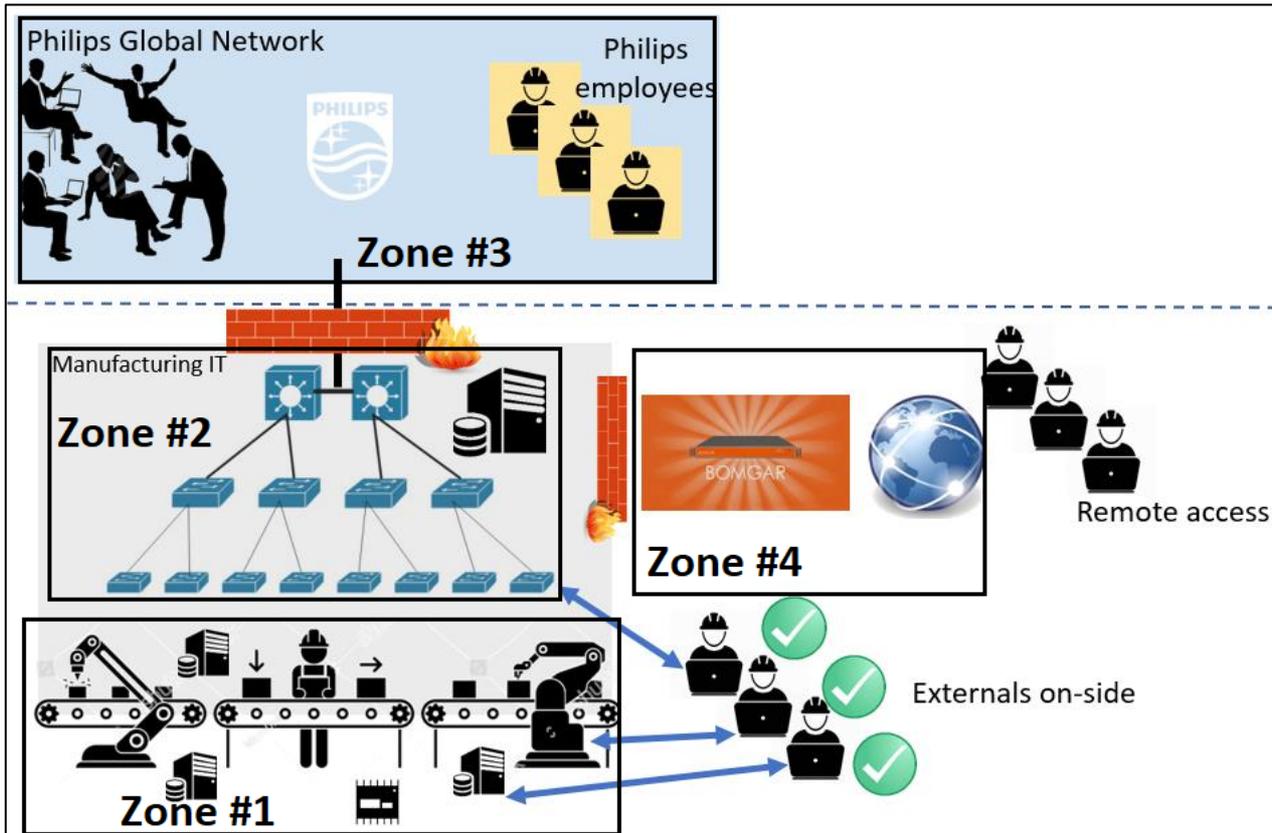


Figure 10 - Reference architecture

Security concepts

Zone #1: Shop Floor

There is a limited overview and insight of the assets in this zone. Networking is managed through vendors through connections to the manufacturing zone, which is managed through PCL. Assets are not centrally managed and are generally not patched

Connections between zone #1 Shop Floor and zone #2 manufacturing zone

In high-risk situations, a firewall (including UTM and industrial protocol support) is used between zone #1 and zone #2 to strictly control access using the principle of least privilege.

Zone #2: Manufacturing zone

Central management is used where possible to manage these assets. The IT network is segmented using VLANs where all intra-network traffic must pass through a central firewall cluster (including UTM). The use of segmentation limits the attack surface and prevents the lateral movement of any possible attacks or malware in the network. The usage of dangerous protocols is blocked wherever possible (e.g. SMB, RDP).

Connections between zone #2 manufacturing and zone #4 Internet (DMZ)

No internet access is allowed from within the shop floor. Some internet access is granted in the manufacturing zone using an explicit proxy. All traffic between these zones passes through firewalls (including UTM) where access is strictly controlled using the principle of least privilege.

Zone #4: Internet (DMZ)

Access to this zone from the internet is protected through firewalls (including UTM) and geo-IP filtering further limiting the scope of attack. Some resources are hosted in the DMZ e.g. remote access solutions

2.3.3. REN

Architecture overview

All plants of the RENAULT group share the same architecture.

Levels 0 to 4 are local to a plant. Each RENAULT plant is composed of an office network isolated from an industrial network:

- **Level 0** links machine by machine the shop floor operational technologies and equipment (PLC, Robots, monitoring, input output units) ... Level 0 is composed of local fieldbus physically segmented.
- **Level 1** is dedicated to Ethernet TCP IP communication between PC and production displays and robots for programs backup.
- **Level 2** is the area supervisory control (SCADA). This level is a kind of the frontier between the OT and the IT world.

It is composed of standardized industrial desks (PC), which interact with industrial controllers to collect data and provide orders. These industrial desks provide local HMI for control and supervision but also remote access.

On level 2, on the IT network, there are also deployed IT/IOT devices used to collect data from the production level (sensors ...) and human oriented devices to provide local information regarding the production (shop floor screens, tablets ...).

RENAULT corporate architecture can be represented as a traditional Purdue Model.

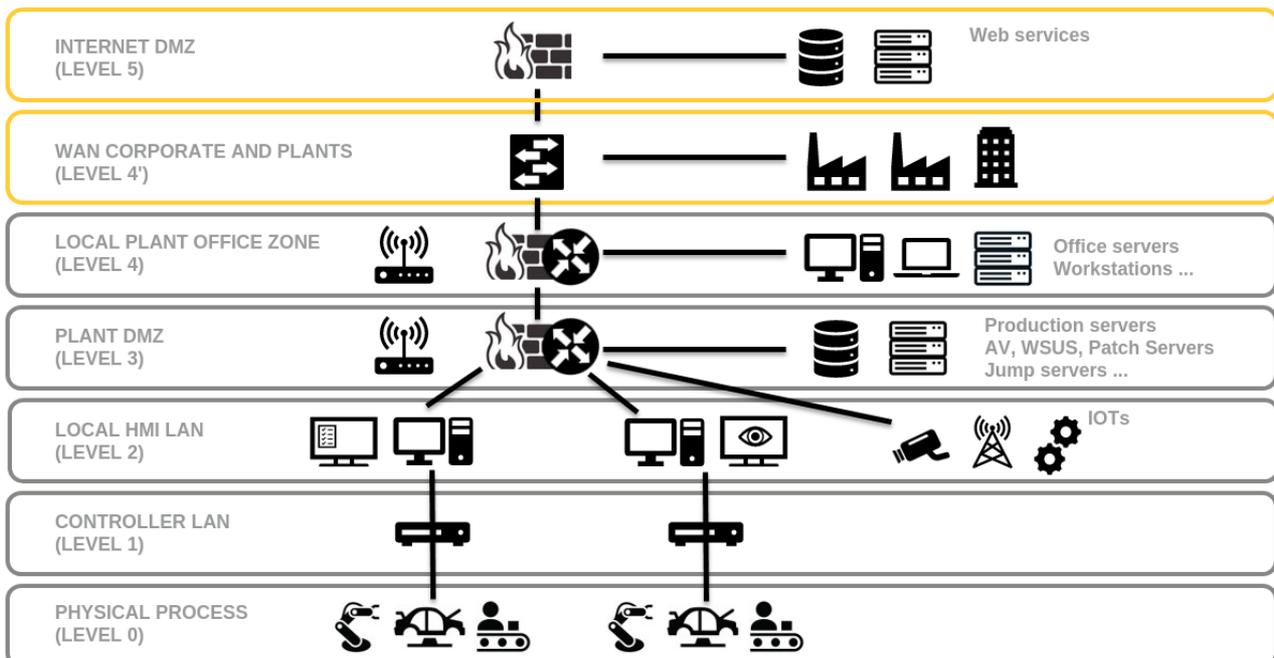


Figure 11. Renault corporate architecture.

- **Level 3** is the industrial DMZ zone. This zone contains industrial services exposed to the local office and corporate network. Any direct traffic to industrial network is forbidden and must be relayed by a service in the DMZ (for example jump servers).
- **Level 4** is dedicated to plant office network and interconnexion with RENAULT corporate WAN. Each plant is protected by next generation firewall.

Level 4' is the WAN zone which interconnect each plant, each RENAULT site as well as RENAULT data center.

Level 5 is the corporate internet DMZ with external web services.

Industrial network security concepts

There is no direct communication between **level 0** and **Level 1**, communications between these two levels are realized through the industrial controllers (PLC, automatons). There is no cartography of the assets in levels 0 and 1, which are not centrally managed and not patched (or almost).

On **levels 0 and 1**, devices are not managed and for most not patched. These levels do not provide any security mechanism (authentication, access control...).

On **level 2**, industrial desks are all managed (central management tool, WSUS) and protected against malwares (antivirus, whitelist...).

Level 2 IT network is segmented based on VLAN and access control lists. Segmentation is based on different criteria (industrial process, IOT...) based on the criticality of each zone to limit the spread of an attack or a malware to the whole network. Segmentation is enforced by a next generation firewall with IPS capabilities. Security policy is based on a least privilege principle, default policy is to block every traffic not explicitly authorized.

Moreover, the default policy is to block any Internet access. Only specific services are whitelisted and authorized through corporate Internet proxies (e.g., antivirus updates...).

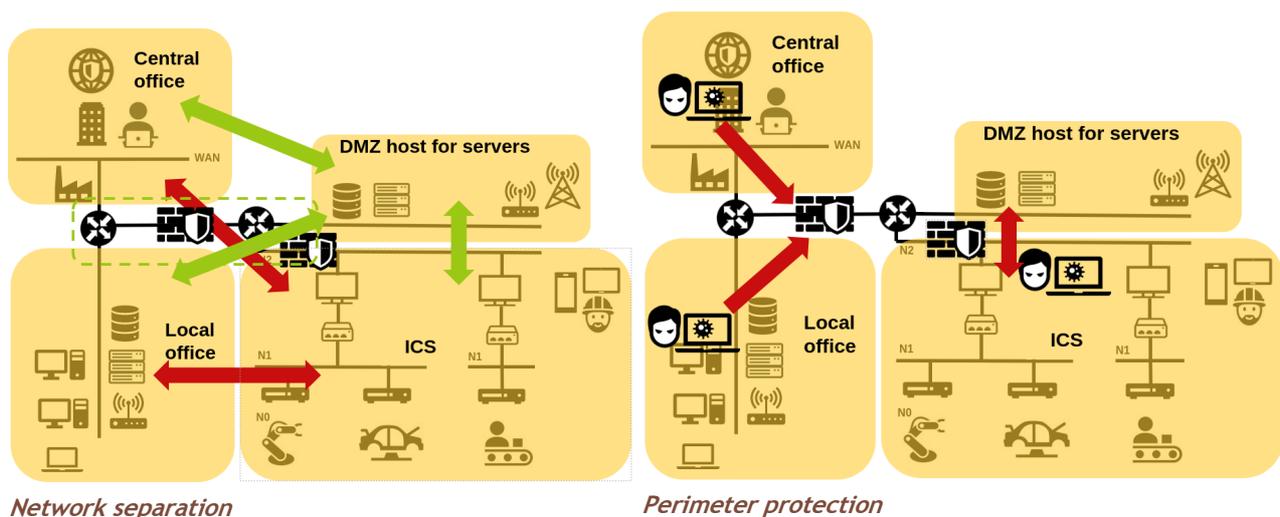


Figure 12. Communication between levels.

Level 2 implements network access control mechanism. Upon connection, a device is automatically affected to the right VLAN according to its rights and privileges. It removes human errors in attributing

VLAN to switch ports. It increases network flexibility, VLAN definition is given according to the device and not to the switch. Devices are affected to VLAN according to their MAC.

Levels 3 and 4, enforce the network separation and the perimeter protection. Firewalls enforce those policies:

- Direct traffic with industrial network, from local or central office networks forbidden;
- Traffic between central or local office networks and industrial network authorized through DMZ or protected zones filtered;
- Dangerous protocols blocked from central or local office networks to industrial network (for example SMB, RDP...);
- Network traffic protected against well-known attacks (IPS...).

The remote access use case (Figure 13. Remote access use case.) (SSH, RDP, VNC...) is a good example that illustrates the different levels of protection:

- VLAN isolate assets in dedicated zones depending on their security level and criticality;
- firewalls block any direct access to these assets except from a specific service hosted in a protected zone (DMZ);
- a security service for secure remote access (bastion or “jump server”) centralize all remote administration protocols from local and central networks;
- access to bastion from Internet (for internal staff or suppliers) is authorized through the setup of a VPN. Internal staff uses hardware token as MFA, external suppliers request for an access code generated by RENAULT teams using an OTP hardware device.

Another aspect of the cybersecurity strategy in the industrial network is the **monitoring and the threat detection**.

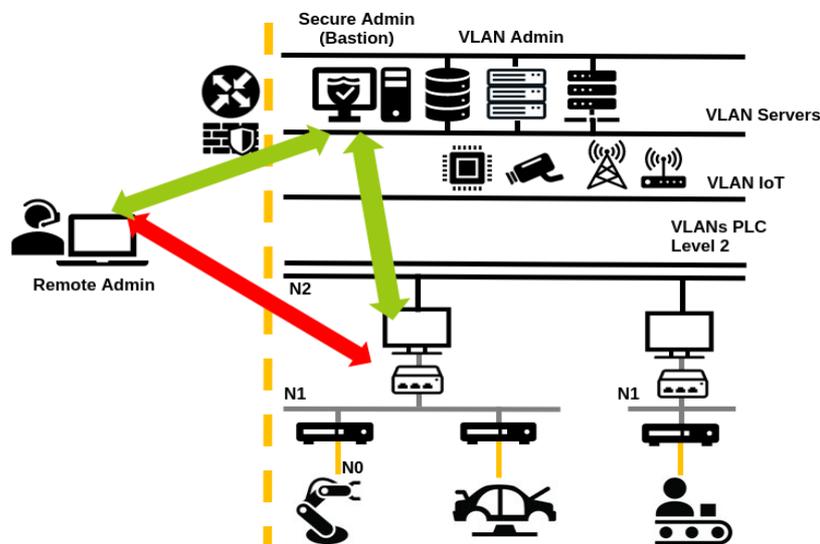


Figure 13. Remote access use case.

Each plant is equipped with a threat detection appliance which monitors traffic on the main distribution routers. This appliance can detect abnormal behaviour (asset, traffic...) and generate security events. Main security events are sent to the central RENAULT Security Operation Center (SOC).

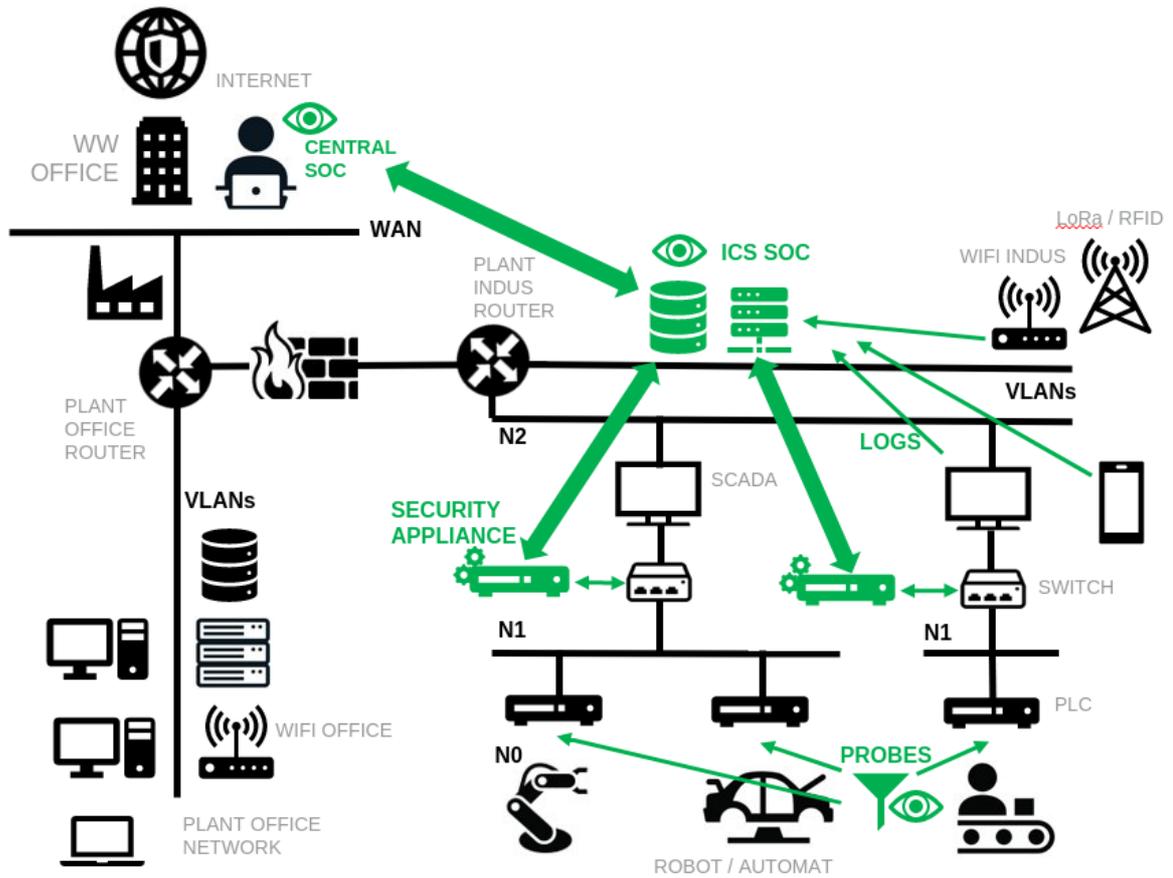


Figure 14. Monitoring and threats detection.

3. Functional elements

COLLABS tools and technologies provided by the project partners are mapped to the four COLLABS functional elements.

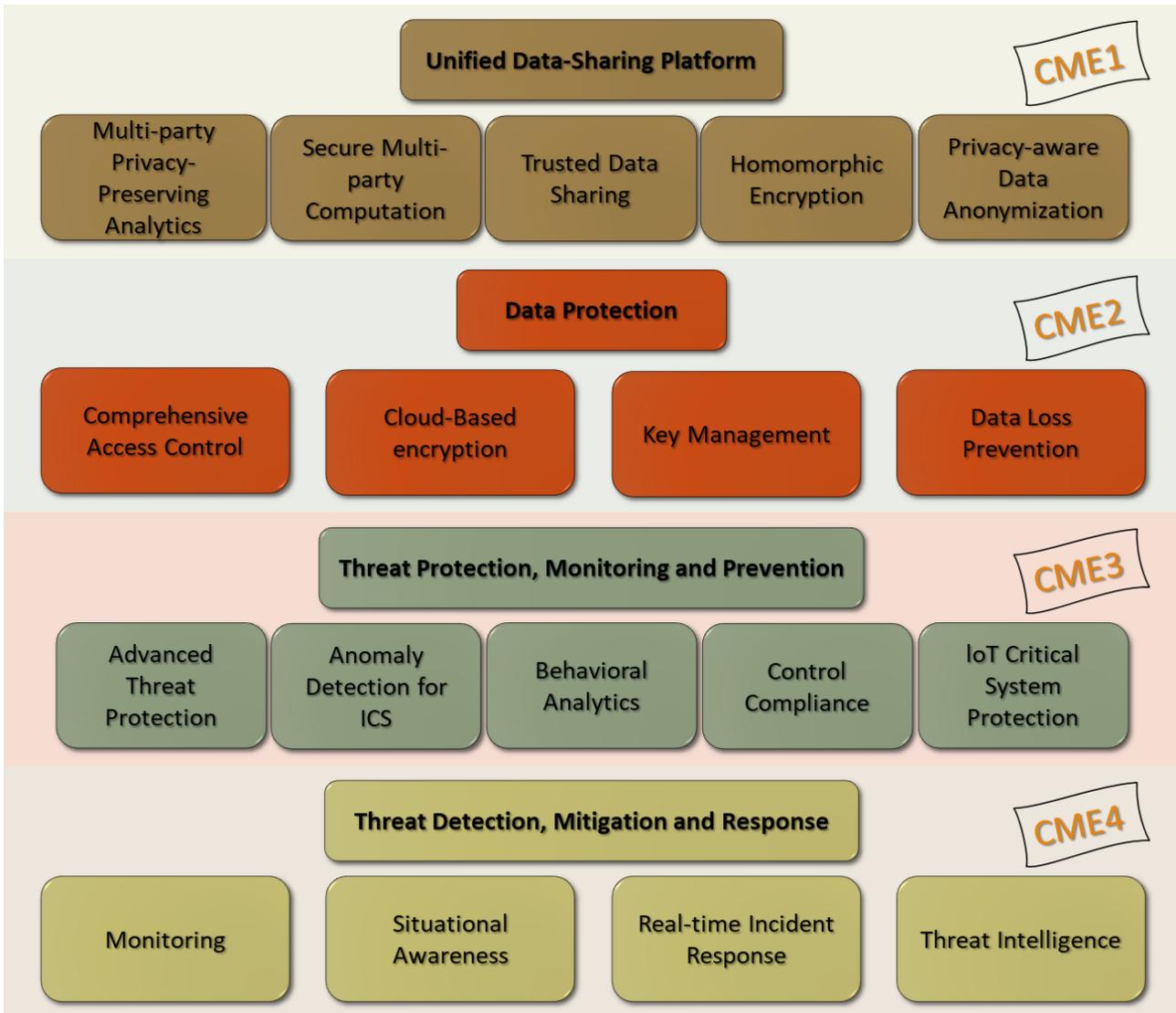


Figure 15. COLLABS functional elements.

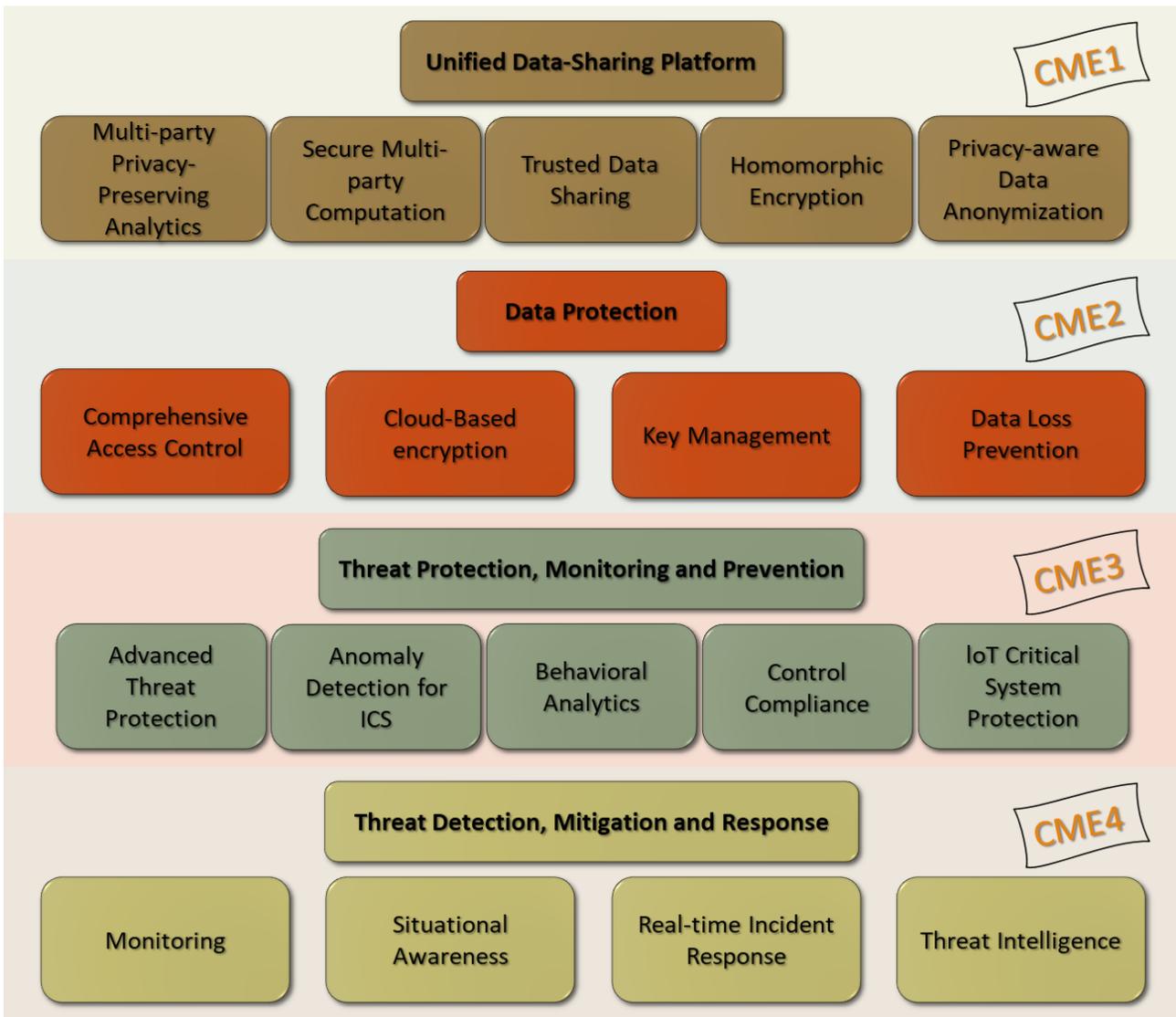


Figure 15 shows the high-level functional organization of COLLABS framework. The framework consists of four elements that target characteristics of Industry 4.0 environment, equipment and devices and cloud-based infrastructure.

Unified Data-Sharing Platform (Collaborative Manufacturing Element 1 - CME1) digitally connects external partners with manufacturing facilities to create a value chain. This CME includes practically usable solutions that can guarantee an adequate level of security without limiting the possibility of exchanging data and information on the factory floor and outside the factory. Data Protection Element (CME2) rounds up solutions for efficient data protection. The third element, Threat Protection Monitoring and Prevention (CME3) is responsible for threat protection. Threat Detection Mitigation and Response is the fourth cybersecurity element (CME4). It provides threat detection and implementation of countermeasures. Additionally, this functional element is addressing evolution of the system and real-time responses.

COLLABS will provide a data exchange platform based on secure multi-party computation, homomorphic encryption, differential privacy, and zk-SNARKs [4] based on distributed ledger. Several mechanisms for data protection will be provided, including comprehensive access control and data loss prevention. Threat protection and monitoring will be done using remote attestation schemes and usage of deep learning and machine learning to monitor a wider range of evolving threats. The COLLABS framework also includes mitigation and real-time response to detected risks. The IoT devices response measures include firmware

and software updates, while at the factory level, the measures include filtering traffic or limiting traffic which contains malicious or suspicious packets.

3.1. Unified data exchange platform

Secure multi-party computation and homomorphic encryption allow computation on sensitive data without disclosing the values themselves. One of the goals of COLLABS is to utilize secure multi-party computation and homomorphic encryption in statistical analysis, machine learning and deep learning in order to protect sensitive data from unauthorized access by partners, untrusted infrastructure or cyberattacks. Efforts will be focused to a set of algorithms which will be selected in the requirements analysis process. Solutions developed within the project will allow multiple parties to process sensitive data jointly without revealing sensitive and confidential information to anyone outside and ensuring the compliance to data access criteria and privacy.

The COLLABS framework will include an implementation of secure data exchange in industrial scenarios using zk-SNARKs and distributed ledger - blockchain. The solution will be based on combination of hardware trust and cryptographic schemes to be able to provide secure self-attestation based on industrial IoT data. Information obtained in this way might be used to prove compliance to security policies in manufacturing while observing privacy and protecting sensitive data from data producer. This will facilitate the exchange of highly critical data.

In addition, we will use methods based on differential privacy to support data analysis and exchange in industrial use cases. Differential privacy introduces the epsilon factor, or privacy cost as a parameter to existing machine learning and deep learning algorithms. This method introduces a trade-off between the level of privacy of the exchanged or processed data and the performance of data analysis.

3.2. Data protection mechanisms

Data protection mechanisms include comprehensive access control and data loss prevention mechanisms.

Comprehensive access control includes security services based on trust to authenticate IoT and insuring communication only between trusted components. COLLABS framework will use identity based and context-based access control when managing communication between cloud-based applications and web applications. It includes the use of distributed PKI for authentication of users and devices to remove the need to use passwords for users and devices whenever possible. Management of certificates will be done using blockchain to provide immutability and prevent forgery attempts. Moreover, we are planning to use Attribute-Based Access Control (ABAC) that will allow precise and flexible definition of access rules using XACML standard. Access rules are administered and managed in a centralized way, in a Policy Decision Point (PDP). Since IoT devices with low processing power and low memory capacity are not suitable to act as servers, Attribute-Based Encryption (ABE) will be used to ensure trust between the sensor and end user. In that case the IoT device only encrypts the data it sends, and PDP sends decryption key to the end user, ensuring the communications adheres to rules described there. COLLABS framework will also include IoT device fingerprinting methods to detect of anomalous behavior and signaling received from edge devices. Combination of specified concepts will enable COLLABS to provide additional level of security and confidence in industrial scenarios.

Data loss prevention element within the COLLABS framework consists of a set of solutions to protect confidential data using content detection and context signatures in industrial use cases. Data stored across all layers of the manufacturing industry environment requires portable solutions to prevent data losses and leaks. Considering the size of datasets in such scenarios, using high-performance computing environments that include GPUs for data processing is a must. Regular expressions provide a flexible solution for representing patterns, including personal, financial, or secret information. Within the COLLABS framework, a mechanism that includes specialized regular expression matching implementations running

on HPC hardware will be used. To automate classification, monitoring and detection of sensitive data, we will use deep learning methods - predictive models suitable to identify any sensitive information and track unusual activities or new access patterns.

3.3. Threat Protection, Prevention and Monitoring

Threat protection, prevention, and monitoring functions of the COLLABS framework have two main pillars - remote attestation and advanced threat protection.

Remote attestation is a security mechanism that provides evidence of device reliability. An attacker with physical access to an IoT device can attack the device by updating the device's firmware and endanger privacy and security of the whole system by doing so. Such attacks can be prevented and detected using remote attestation - a software that remotely checks integrity of IoT device firmware and guarantees its integrity. Remote attestation is a protocol that allows proving of software integrity to a remote verifier, which provides evidence that the software has not been modified. This is accomplished by signing protected memory regions. There are some challenges that need to be resolved before remote attestation is included to COLLABS framework. For instance, current remote authentication schemes do not take into account the interaction between devices, then there is the question of scalability in case we use large number of devices and applying remote attestation schemes without degrading performance of the system.

In addition, COLLABS framework will include advanced threat protection, i.e. mechanisms that rely on deep learning and machine learning methods used to detect and prevent wide range of threats using complex analytics. ML and DL methods will be used to track anomalous behavior and introduce predictive analysis of threats and attacks. Using historical data and labeled datasets, ML and DL algorithms can be trained to detect threats automatically and trigger mitigation actions or signal system administrators so that they can respond to the security threats manually.

3.4. Threat Detection and Response

Threat detection and response functionalities within the COLLABS framework leverage model checking and attribution mechanisms as base methods to identify abnormal or malicious events and behavior. These functional elements will be organized as a collaborative threat intelligence that will allow participants, third parties and external security experts to access and contribute to the threat intelligence. This will be accomplished by using distributed ledger technologies. The platform will also include security certification mechanisms responsible for monitoring, assessing, validating, and certifying the proper execution of the framework and monitoring the delivery of the desired levels of security and privacy.

Beside the set components dedicated to detecting anomalous behavior and unwanted events, COLLABS framework also includes components dedicated to response and mitigation of detected threats. At the edge, on IoT devices, those measures include firmware and software updates based and technologies that allow execution of code in isolated areas of memory - memory enclaves. At the level of smart factory's communication infrastructure, the measures include filtering traffic or limiting traffic that contains suspicious content. At the same time, at the system level, through all layers, access control, policies and trusted execution are monitored continuously.

4. System Components

The system components that make up the COLLABS framework architecture have been divided to runtime components and secure development and configuration components. This section contains a detailed description of those two types of components as well as their interaction. Interaction between components represents the initial version and might change during the project.

4.1. Runtime components

COLLABS runtime components and their interaction is shown at Figure 16. Runtime components horizontally, the components are divided to the three main elements of the smart manufacturing environment - digital supply network, smart factory, and connected objects. The digital supply network refers corresponds to external entities within the supply chain with which a smart factory exchanges information. The smart factory itself is a middle element of the system, and finally, the connected objects are the lowest scale of the system consisting of individual devices (IIoT, sensors, etc.) interconnected within the smart manufacturing ecosystem.

Vertically, the components are divided to three security levels - Hardware-enabled and device-level security, Inter-device level security based on distributed ledger technologies and Machine learning-based cognitive security level. Section 5 describes the three security levels in detail.

Finally, every component has one or two colors that position them to appropriate collaboration manufacturing elements described in the previous section.

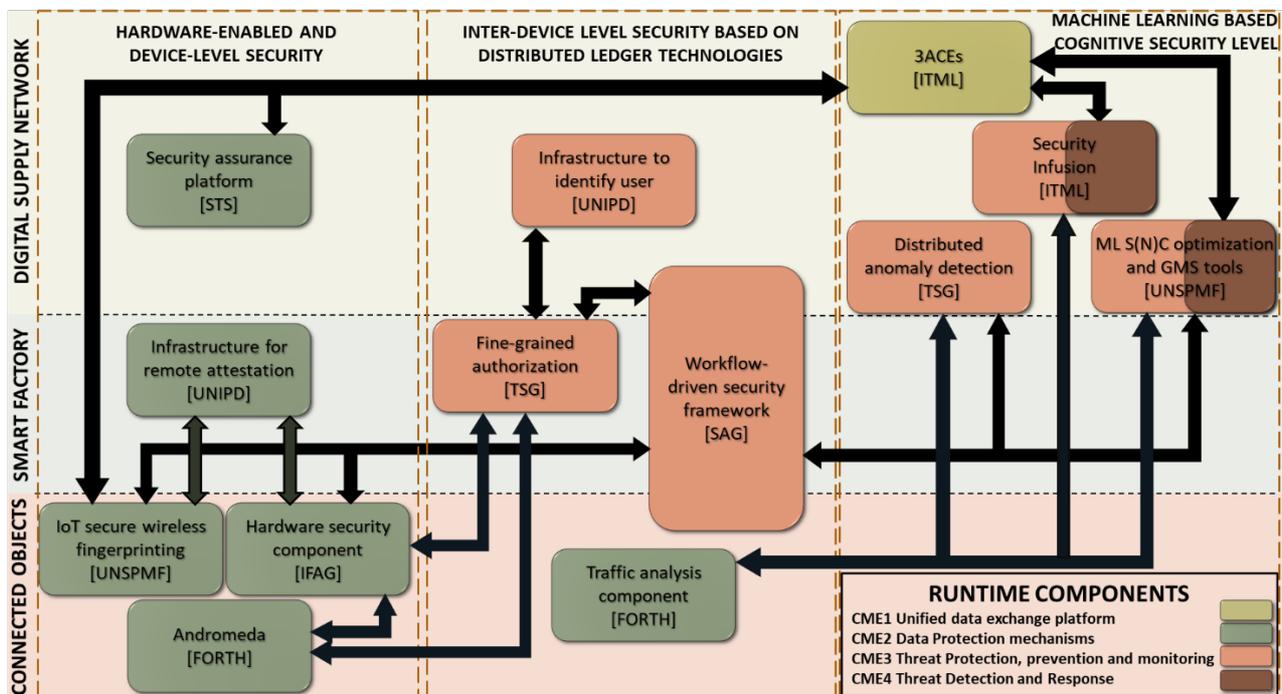


Figure 16. Runtime components

4.1.1. Andromeda Trusted Execution Environment

Brief description

FORTH's Andromeda tool, leverages hardware trusted execution environments such as SGX and TrustZone to provide hardware-secured code and data enclaves.

Objectives

- Authenticity: proof of genuine entities in a dedicated computing network. Typical use for it is for device-to-device authentication, however it can also be used to prove users' genuine identity.
- Physical (hardware) isolation: comparing to software-based Trusted Execution Environments (TEEs), the biggest advantage is the physical separation so that remote attacks are immensely hardened. Via

predefined interfaces it will still be possible to be connected but only after schemes like mutual authentication, etc.

In general, a secure element based on the Andromeda tool can be considered as the root of the trust before any communication starts. The secure element can undertake this role by being responsible for security decisions, e.g., deciding whether an entity is authentic and whether a user's identity is real and their privileges are proper. If these turn out to be true, then the system can consider that the entity can be trusted and allow further execution from that entity and its computing environment.

In COLLABS, the focus is on edge devices security, but the principle is universally applicable also for any critical infrastructure like router/gateway and server/cloud.

Interactions with other components

Andromeda TEE will interact with the authorization modules through proper interfaces defined according to the deployment scenarios.

Technical pre-requisites and requirements

The most common security decision is based on mutual authentication. Devices secured through Andromeda and any other devices can establish a challenge-response procedure. The mostly one used is the symmetric cryptographic function, like AES. Both entities keep a master key securely. Using this shared secret to encrypt random numbers as challenge, the signed challenge can be verified by other entity based on the same key.

After mutual authentication, the entities usually derive keys for further communication. The essential rule is never exposing master key, but to use derived keys for communication. These derived keys are usually called session keys because they exist temporarily only in a certain communication session.

Intel SGX must be provided in the machines that will run the Andromeda module. FORTH will also work towards implementing Andromeda on top of ARM's TrustZone technology.

Potential benefits for the future users

The advancements in collaborative manufacturing can only be realized to their full potential if certain primitives central to the security of the IT systems, such as authentication procedures and cryptographic functions, can be considered trustworthy, even in the events of attacks. Hardware-based trusted execution environments are key technologies in that direction and their adoption is rapid among the industry. The Andromeda TEE leverages the hardware capabilities of the Intel SGX and ARM Trustzone technologies in order to provide secure and unmodifiable critical code storage and execution as well as protection of critical data (e.g., master encryption keys), even in the case of compromised systems (hardware and software components included). The technology provides both the ability to protect central infrastructure (server or cloud systems based on high-end x86 systems) as well as edge devices, built on more resource-constrained compute elements.

4.1.2. Traffic Analysis Component

Brief description

FORTH will contribute to a traffic analysis module which will provide signature-based detection on packet metadata to perform detection of attacks.

Objectives

The goal of the module is the use of multiple datasets of malicious traffic for signature generation to cover a large area of threats. Also, by using packet metadata such as packet payload length and the order the packets arrive at as variables and the traffic analysis module will be able to detect attacks in encrypted traffic.

Interactions with other components

The traffic analysis module will receive network traffic and send alerts of attacks to the anomaly detection modules.

Technical pre-requisites and requirements

Datasets of malicious traffic are needed for the generation of the signatures and python support has to be installed in the machine where the module will run.

Potential benefits for the future users

The traffic analysis component can be placed in a central gateway and monitor traffic both from the cloud and the edge devices. It can serve the end-users as a security mechanism that detects attacks by analyzing encrypted network traffic. Its purpose is to trigger alerts to the corresponding modules which will inform the end users of malicious actions inside their network. The module will provide vital information concerning malicious actions inside the network using state-of-the art techniques which work in encrypted traffic.

4.1.3. Hardware Security Component

Brief description

IFAG provides a family of Hardware Security Modules (HSM) whose name is Optiga Trust.

These components can make all the cryptography tasks that derive from others generic modules. These tasks may include sign, verification, encryption, decryption, true random number generator (TRNG), secure store of valuable data, IP protection, secure updates, key provisioning, and others. These modules are protected against eavesdropping, tampering and message forgery.

Objectives

The goal of using HSMs in the COLLABS framework is to provide a secure execution environment to allow even very low computational capacity edge devices to:

- Perform secure crypto processing of input data directly from the edge.
- Send data-packets with an identity-certification.
- Be analyzed as part of a remote attestation process.

Receive firmware and software updates in a secure and remote way.

Interactions with other components

Hardware security component may interact with:

- Those components that read or interact in some way with the data generated by the edge devices. This data could have been signed and encrypted by an HSM, so these components will have an indirect interaction with the Hardware Security Component.
- IoT secure wireless fingerprinting because this component needs to interact directly with the IoT device to gather IoT device data in real-time.

- *Andromeda TEE in those devices that use this component together with Hardware Security Component.*
- *Fine-grained authorization for device authentication.*
- *Infrastructure for remote attestation in order to collaborate in the remote attestation process.*

Technical pre-requisites and requirements

It is important to have access to the source code of the edge device to have the possibility of integrating the software stack libraries of the HSM that is required to use.

Additional information

In the case of the use of an Ethereum-based blockchain network, the use of Blockchain2go shield is recommended, as this product is focused on carrying out cryptographic operations of this type of blockchain which are uncommon and not supported by other HSMs.

Potential benefits for the future users

Users will benefit from the confidence of employing state-of-the-art security devices communally reserved for personal uses in their industrial IoT (IIoT) devices. The use of these hardware security devices in IIoT devices with a non-cybersecurity-oriented design greatly reduces the risks of cyberattacks, saving not only the repairing and / or replacement costs, but also the much higher costs associated with denial of service in the industry. At the same time, it produces an increase in security and confidence in the IIoT nodes, which offers the opportunity to delegate more and new industrial functionalities, increasing productivity and reducing costs. In short, hardware security modules are a fundamental enabler step for the development of Industry 4.0 [5].

4.1.4. Fine-grained authorization

Brief description

Fine-grained authorization component is a 5G-enabled asset, which enables flexibility and dynamicity of attribute-based access control (ABAC), governed by a central policy, for devices with restricted computing or network capabilities, relying on existing IT security standards.

It contains a XACML 3.0 authorization engine with policy management service, OAuth2/CWT access tokens generation service and enforcement modules for gateway-level authorization, and attribute-based encryption (ABE) key management service and encryption/decryption modules for sensor-level authorization.

The component supports OpenID Connect authentication, enabling identity federation for secure & multi-tenant data sharing.

Objectives

*In the scope of the COLLABS project, fine-grained authorization component provides **flexible and end-to-end access control** of the data produced by the smart factory, allowing secure data exchange within the factory or between different stakeholders. In order to carry data exchange across existing systems boundaries, the solution enables the multi-tenancy of authorization system, allowing partners in collaborative manufacturing to share data in a secure and trustful manner.*

According to the COLLABS project assets and requirements, the component may be further progressed to meet specific needs of Industry 4.0, evolution of relevant standards (i.e., IETF WG on ACE Authentication and Authorization in Constrained Environments), and meet specific needs of the surrounding components such as:

- supporting a blockchain-based architecture for authentication and access delegation, to allow interaction between the different stakeholders not accepting to depend on a single authority
- complying with privacy measures, regarding the disclosure of information required to grant access

Interactions with other components

The fine-grained authorization component may interact with:

- **Hardware Security Component / Trusted Execution Environment:**
 - for device authentication,
 - for access token proof-of-possession resolution.
- **Blockchain:**
 - for authentication using specific PKI,
 - for access rights definition/delegation.

Technical pre-requisites and requirements

The authorization method may vary according to the environment capabilities (computing resources or networking connectivity):

- **Attribute-based encryption method:** for “greenfield” systems or for devices that are more constrained in computing resources than network connectivity (e.g., a sensor)
 - should be able to execute encryption module (in C)
- **Self-contained access token method:** for “brownfield” systems (with a gateway) or for devices that are more constrained in network connectivity than computing resource (e.g., a moving engine)
 - should be able to host a token enforcement agent (in java or python)

Additional information

For authentication, and for data flow using an access token, communication channels should be secured in confidentiality and integrity (e.g., using TLS/DTLS).

Potential benefits for the future users

Users with the Fine-Grained Authorization system can benefit the granularity and the flexibility of ABAC rules definition, without the heaviness of the infrastructure it traditionally requires. The usage of ABE ensures end-to-end confidentiality of the data from the Shop Floor to the Cloud with no need of intermediate circles of trust. Data can be encrypted independently of who it is intended for, and new accesses can be dynamically granted after its production and encryption, even to new tenants in the system, but always in accordance with the access control policy.

4.1.5. Distributed anomaly detection

Brief description

This component provides a distributed anomaly detection in Industrial IoT networks. Existing approaches rely on analyzing single network packets or clustering large numbers of packets to detect intrusions or compromised services. The choice of the ML model depends on parameters such as data that are massively distributed, so that there is a large number of clients each having a small amount of data. IoT devices typically generate little traffic, which means only little data can be provided by each client alone.

Objectives

This component is based on the work done in T2.5. It is able to detect specific security threats and identify malicious behaviours. This component will be based on innovative distributed ML techniques.

Interactions with other components

To be defined later with other components in WP2/WP3/WP4.

It might interact with distributed remote attestation component (if it exists) before ensuring that all devices are running the correct code.

Technical pre-requisites and requirements

To be fixed when defining relations (INPUT/OUTPUT) to other COLLABS components. The approach will depend also on the type of data, the frequency of data, the amount of data collected, and the use cases requirements.

Potential benefits for the future users

Our framework provides solution for learning from both “very large” data sets and naturally distributed data sets. It avoids the necessity of gathering data into a single workstation for central processing. It also provides a scalable learning solution since the growing volume of data may be offset by increasing the number of learning sites. Our framework will enable to detect anomalies on encrypted and unencrypted communications.

4.1.6. Security infusion

Brief description

Security Infusion is an agent-based software solution that collects, analyzes, visualizes, and presents data concerning the operations and security status of an organization’s IT resources. In order to enable retrospective forensic analysis, the program stores data related with past logs and events, so that they can be retrieved when necessary. Furthermore, the application has the ability to perform regular or on-demand, agent-independent scans on the managed infrastructure, namely port scanning, and vulnerability assessment, providing reports and remedy proposals for issues it might detect. The application realizes its functions through the following components:

- Infusion Agents: Windows & Linux Systems.
- Infusion Manager.
- Infusion Web Interface.

While the agents reside in the systems (hosts) they monitor, the manager can be deployed either at the edge of the infrastructure or through the cloud.

The **Agents** run seamlessly on the hosts, collecting data on every operational aspect of the system. Two types of host agents are available: **Windows Agent** and **Linux Agent** for systems running the corresponding OS. Infusion agents can also be installed on systems that take the role of a Log Server, in order to monitor and collect network-related operational information.

The collected data are accumulated on the **Infusion Manager** where they are processed and transformed into exploitable information. Machine learning algorithms are applied to the datasets created, so with time, the precision of the analysis increases. Besides the objective of accurately detecting anomalies and risks, a threat response framework is also realized-through reports and remedy proposals. The Infusion Manager environment can be installed on a virtual or a physical machine, residing either at the logical edge of the monitored infrastructure (Edge Manager) or in the cloud (Cloud Manager).

The **Web User Interface** is a simple, intuitive administration environment that visualizes the operational information as processed, analyzed and aggregated by the Edge Manager. The information and action proposals are presented and administered through seven functions plus a central Dashboard that aggregates important information elements. Eight application tabs correspond to these functions: Dashboard, Inventory, Port Scanning, Monitoring, Vulnerability Assessment, Analytics, Event Analyzer, Forensic Analysis, and the admin panel with the relative settings options.

Objectives

ITML developed Security Infusion to be an application for IT operations monitoring with elements of cyber security management, designed to run and operate in a simple and intuitive manner.

The main objective of this deployment is to ensure that ICT resources, services running on them, network and computing events, are monitored, reviewed, and analyzed in real time, while relative data are collected and stored for further classification and forensic purposes, using data analytics and machine learning algorithms.

Security Infusion can be deployed either through the cloud or at the edge of an organization's infrastructure, without overloading the network with unnecessary traffic and chatter. The application's architecture ensures that vital information is collected, processed, measured, and presented in a timely and compact fashion, when needed, as needed.

Eventually, built-in machine learning makes time and data growth an ally for better situational awareness and response; the more data it collects the more effective it becomes.

Technical pre-requisites and requirements

Infusion Edge Manager

	< 20 Agents	< 100 Agents
Platform	AMD64	AMD64
CPU	2 CPUS	2 CPUS
Memory	4GB	6GB
Disk space	Fully configurable per agent. 75KB per snapshot of the system. Example: Keeping 1 month of data, for five servers with one snapshot per minute: 30 days x 5 agents x 24 hours x 60 min x 75Kb = 16GB	

Infusion Windows Agent

	Minimum	Recommended
OS	Windows 7	Windows 7
Platform	32bit/64bit	32bit/64bit
CPU	Intel i3	Intel i5
Memory	2GB	4GB

Infusion Linux Agent

	Minimum	Recommended
OS	N/A	N/A
Platform	32bit/64bit	32bit/64bit
CPU	Intel i3	Intel i5
Memory	2GB	4GB

Potential benefits for the future users

In COLLABS, Security Infusion is a tool responsible for monitoring and securing network devices in infrastructures across all different use case scenarios. Considering that it offers real-time and historical data access concerning the security posture of the users' enterprises, it reduces users' inconvenience when attempting to retrieve collected and analyzed security data in a written or visualized form, without compromising its integrity or accuracy. The users can also benefit from the flexibility of options when deploying the solution, for it can be deployed at the edge, on a cloud instance, or a hybrid of both options, depending on the users' legal and operational requirements. Moreover, the platform will also be creating alerts when a certain threat or anomaly is detected, allowing users to act rapidly in the case of a potential network threat to resolve or avoid certain issues. The solution in itself is cost-effective, user intuitive, and adaptable to several versions of predominant operating systems (Linux and Windows) that are currently used in manufacturing environments.

4.1.7. 3ACEs

Brief description

The **3ACEs bot**, which is an embedded assistant that acts as a data analyst, hides the complexity of blending heterogeneous data streams and provides an automated preliminary analysis on the raw data. This allows the tech-savvy business user to **formulate their high-level business requirements**.

The first step for any business entity that wants to extract business value from their existing digital footprint is to **review the currently available data**. Examples of such data include but are not limited to online sales data, web usage, site analytics, production line sensors, logistics and warehouse data or existing market analysis.

The second step is to **collect the data**, starting with a small representative sample and feed it to the **3ACEs bot**. A data scientist can optionally assist in this process in cases of enterprises that have vast amount of data, from heterogeneous sources.

Following the engagement of 3ACEs bot the data is processed and analyzed, in order to provide on-demand, self-service analytics. This is achieved with the **3ACEs analytics engine** that allows for an iterative data analysis process to take place, based on multiple advanced Machine Learning (ML) algorithms that make the most out the existing data.

Finally, the insights produced are presented through an advanced visualization interface, that constitutes the **3ACEs business intelligence provider** aiming to assist the tech-savvy business user in taking action into strategic and/or business decisions - or simply identify malfunctions in existing processes.

Objectives

3ACEs is an Analytics as a Service platform that delivers data insights as a service. Users and companies can benefit from any kind of data they already produce and get valuable business feedback about their existing processes, production line and / or customers' habits.

3ACEs delivers the essence of data business analytics solutions to SMEs in order to help those companies optimize **decision-making** at the tactical, operational, and strategic levels. The product is configurable, scalable and can be adopted and operated by **non-experts**.

Interactions with other components

The component receives data from edge devices and provides classified data to higher layers.

Potential benefits for the future users

3ACES - Analytics as A Service - role in COLLABS is to provide ideal decision support for the users' businesses throughout the data it collects across different domains and use cases. When combined with the Data Fusion Bus, it constitutes the data integration layer of the solution. The benefit it brings to future users lays within optimizing their decision support through data analytics, thus serving in the clustering, classification, regression, and anomaly detection of the data presented; at the same time, the tool is customizable to a high extent, which makes it both efficient and flexible to adapt in any use case. It also delivers a convenient solution to instances where noisy data ought to be processed. Cost reduction is another major aspect which 3ACES offers, whereas knowing the reoccurring anomalies and security issues allows enterprises to solve them before having catastrophic implications; on the other hand, the solution itself is quite affordable compared to similar ones that are currently available in the market.

4.1.8. IoT secure wireless fingerprinting

Brief description

Gathering IoT device data in real-time, ranging from channel state information and radio reception quality metrics, device activity patterns and connection quality, may provide a wealth of information for device behavior modelling and characterization. We aim to develop dynamic behavioral models, where data coming from each end device will be continuously inspected and preprocessed for device identification and verification, anomaly detection, etc. Most importantly, the indoor public space (a building at UNS campus) will be fine grain fingerprinted by pre-collecting data set of end device signals. We will develop a new deep learning models to empower efficient fingerprinting-based device identification. Finally, we aim to develop a novel method for fast and efficient training of a deep learning model by using established indoor channel models, ray tracing tools, and 3D-modelling of objects under consideration. Development of such training methods is a critical enabler for development of value-added security and ambient intelligence services and its deployment into real world Wi-Fi IoT systems. From the algorithmic perspective, structured (non)convex optimization and neural network-based methods will be used for training and inference. In order to accommodate potentially low processing and low storage requirements at the devices, lightweight to moderate complexity machine learning methods will be considered, such as lightweight autoencoders with a low number of hidden layers or online stochastic first order methods. Depending on the device requirements, different implementations will be considered, including 1) C/C++ based and 2) Python based, using, e.g., Tensorflow2, scikit-learn and PyOD libraries.

Objectives

Different IoT devices behave in a different way. Observing specific physical (PHY), medium access control layer (MAC) or network flow data features, which are already collected to optimize communication system performance, can provide discrimination among devices. Furthermore, the same data can identify if any of the devices is behaving "normally", or anomalous behavior is present, which may be result of device malfunction, but also, security threat. Device identification and profiling, besides its location, is the critical input to device identification, threat detection and context recognition.

Technical pre-requisites and requirements

Technical results, implementations and demonstrations will be performed in several stages. MATLAB simulated environment with realistic standard-based physical layer implementation of IEEE 802.11ah HaLow IoT standard will be used for initial investigation and data set generation. From this stage, we will move to real-world testing and deployment, where we will use FPGA-based boards with IEEE 802.11ah implementation. Finally, we will also use commercial off-the-shelf IEEE 802.11 devices, in particular, access points with specific hardware chipsets that allow access to lower-layer data extracted about each connected device such as channel state information. The setup will also require usage of servers and GPU cards for training and deployment of machine learning algorithms.

Potential benefits for the future users

Usage of wireless IoT nodes will grow exponentially in the future with billions of nodes being connected to different industrial and infrastructure systems. Monitoring IoT devices at such a massive scale is only possible using scalable and efficient automated methods. Data-centric machine and deep learning approaches are ideal choice, but they require abundance of specific device data. IoT wireless fingerprinting tool is designed and developed to identify and generate such data, and present it in the most efficient form to the subsequent processing by machine learning tools in order to achieve desired accuracy while taking into account specific constraints of state-of-the-art wireless IoT interfaces.

4.1.9. ML structured (non)convex optimization and graphical models-based tools

Brief description

This module will contain a pool of ML algorithmic implementations for carrying out anomalous pattern detection, identification, and tracking. The pool is mainly based on a framework wherein a problem at hand is modelled via structured (non)-convex optimization or graphical models' approach. For example, in anomaly detection, the normal plus anomalous data pattern can be modeled via a sparsity plus low rank-enhancing optimization model. The problem at hand is then solved via parallel and distributed optimization algorithms or belief propagation-like methods. The framework is very generic and can accommodate various ML and analytics tasks. Current pool of methods includes sparse regression, clustering, classification, alternating direction method of multipliers (ADMM), belief propagation, as well as supervised and unsupervised anomaly detection methods based on autoencoders, support vector machines, local outlier factor, isolation forest, etc. The pool is implemented in several packages including C/C++, Python and PyCOMPSs; all supported through message passing interface (MPI) library and is applied in various applications including distributed state estimation, localization, and synchronization. Further advances will be primarily based on the MPI library-based and Python-based implementations and will focus on supervised and unsupervised anomaly identification, detection, and tracking tasks. This includes, e.g., anomaly detection based on the fingerprint data at edge devices and anomalous traffic flow analysis.

Objectives

Develop and optimize large-scale distributed ML structured (non)-convex optimization methods and graphical models-based methods on an in-house distributed and parallel computation testbed containing 40 or more Raspberry Pi 4 quad-core platforms and on in-house 100-core mini cluster computer.

Message passing interface (MPI) library and C++ will be used to develop distributed algorithms in real-world testbed environment where their performance and convergence can be tested against delays in inter-node communications, data losses, and various problems related to asynchronous node operation.

Large-scale probabilistic graphical models in the form of factor graphs empowered with Belief Propagation (BP) methods for distributed inference will be developed in C++ and run using message passing interface (MPI) library on an RPi cluster.

Technical pre-requisites and requirements

Distributed and parallel computation testbed containing 40 or more Raspberry Pi 4 quad-core platforms. Mini cluster consisting of 16 nodes with 6-core i7 CPUs, 8 NVidia GTX960 GPUs, 304GB RAM, 36TB storage and 10Gbit/s network.

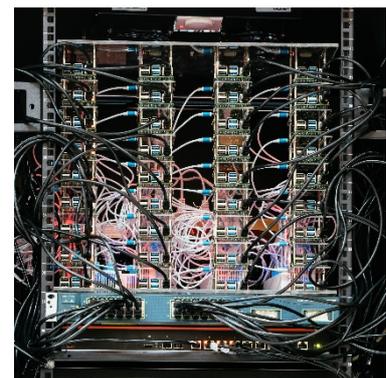


Figure 17. distributed and parallel computation testbed.

Potential benefits for the future users

Improve security of (wireless, IoT) network systems through application of the models to device identification, anomalous device detection, secure data sharing, and possibly other problems related to COLLABS use cases and beyond. The applications will provide additional support to standard methods for (user and device) authentication and detection of security-related events such as potentially malicious or defective behavior of users and devices, resulting in more secure and robust systems, and mitigating the risks of losses associated with security breaches and malfunctioning hardware. The module will also be used as a component in potentially novel approaches to device identification and anomalous device detection based on wireless fingerprinting.

4.1.10. Workflow-Driven Security Framework

Brief description

In collaborative manufacturing systems, different stakeholders such as the manufacturers, suppliers, system-integrators, and customers are involved. These stakeholders have their own goals, but they agree on a common workflow i.e., a set of tasks that are to be done in a predefined order. On a high-level, the common workflow may compose several individual sub-workflows. For example, manufacturers want their product to be compliant with required regulations and manufactured and assembled with certain quality. The workflow-Driven Security Framework (WDSF) provides a set of tools to enforce the rules and conditions specified by the involved stakeholders in a collaborative way (see [6]).

Objectives

In the scope of the COLLABS project, WDSF is used to ensure supply chain integrity, confidentiality, and compliance to required regulations in manufacturing. In addition, a special focus on privacy will be explored i.e., WDSF will be extended to protect the disclosure of sensitive private information i.e., any information that may link directly or indirectly to the identity of a person or the organization involved in collaborative manufacturing environments. Furthermore, how resilience in collaborative manufacturing can be achieved will be investigated.

Interactions with other components

The following COLLABS components may potentially interact with WDSF, these are initial ideas and may be updated during the course of the project:

- Trustworthy edge devices and sensors component (e.g., see sections 4.1.3 and 4.1.8):
 - o WDSF can leverage on this component to collect reliable trustworthy data.
- Potential interaction with DESYRE to virtualize devices and gather data for WDSF (e.g., section 4.2.2).
- High-level Anomaly detection/behavioral analysis based on different entities' workflow execution information (e.g., sections 4.1.5, 4.1.6, and 4.1.9):
 - o WDSF can provide workflow information to behavioral analysis component.
 - o Potential interaction with ML structured (non)convex optimization and graphical models-based tools to get insights on workflow execution anomalies.
- Workflows modelled needs to be verified before deployment (e.g., section 4.2.3):
 - o Potential interaction with Formal Specs Verifier (FSV) which could support in formal verification of workflows. WDSF could provide Petri Net models to FSV for verification.

Technical pre-requisites and requirements

WDSF relies on standard REST APIs to communicate with other components. Both basic authentication and advanced authorization such as OAuth 2.0 protocols are supported. To interact with WDSF other components should expose REST APIs.

- Petri Nets (PN) are used for modeling and specifying the workflows and WDSF uses standardized Petri Nets Markup Language (PNML) to import or export Petri Nets workflows.
- WDSF relies on Blockchain infrastructure to record workflow events for accountability and traceability purposes, therefore, a blockchain framework like Hyperledger Fabric will be used.

To read workflow events e.g., the anomaly detection components can develop tools that can read data from the blockchain infrastructure.

Additional information

WDSF relies on trustworthy sensors and edge devices to produce or collect data. The identification of and the establishment of trust to such sensors and devices are crucial necessities for ensuring accountability of actions and for being able to trace the origin and integrity of data. Furthermore, WDSF instruments blockchain technologies in order to provide transparency, integrity, and accountability in distributed workflow scenarios.

Potential benefits for the future users

WDSF is used in COLLABS to realise secure maintenance use cases where for instance maintenance providers need to be granted access to resources such as devices that are owned and operated by other organisations. In general, organisations taking part in distributed use cases that span multiple domains can take advantage of the trust model provided by WDSF: Instead of having to trust selected organisations (usually called trusted Third Parties) that run a kind of central infrastructure, a shared responsibility model can be applied. That means that all organisations have the same level of access to and control of information managed by WDSF. Referring to the example of a remote maintenance use case, both, device owner as well as service provider have access to the audit log. That means, they can both check and provide proof about which partner was responsible for which action in the distributed process. By that, balanced relations of trust exist. What is more, because of the Petri Nets based workflow engine, WDSF eases the implementation of cross-organisational business processes and the realisation of a shared infrastructure.

4.1.11. Infrastructure to identify user

Brief description

In the context of COLLABS framework, the control of the access of external users is fundamental for ensuring the security of the whole system. Moreover, the access should be guaranteed for the strictly required time needed. Based on this requirement, this module contains a set of methods based on ML and AI for user authentication and de-authentication.

In particular, the component provides a user-friendly authentication method based on an assessment of the ear channel movement (called as E-authentication) during chewing. This method is based on a behavioral assessment of the user and can be applied as a continuous authentication solution.

An additional layer of behavioral authentication, without any prior knowledge of the user, can be applied using keyboard dynamics and lie detection techniques.

Finally, to ensure the proper log-out to the system, different de-authentication methods can be applied. In the COLLAB scenario, de-authentication is crucial for mitigating intrusions through Lunchtime Attacks, whereby an insider adversary takes possession of the user workstation before any inactivity log-out.

Objectives

User authentication.

Interactions with other components

Our authentication infrastructure integrates with the Fine-grained authorization component (TSG). In general, the requirements provided by the infrastructure could serve as authentication process along with authorization component

In particular, the first method (E-authentication) uses a proximity sensor in a modified earphone. Possible application includes the possibility to unlock a computer without the need to interact with the device physically.

Keyboard dynamics and lie detection requires an ad-hoc form to assess the identity of the user.

The de-authentication method may require an NFC reader, a Bluetooth connection, a WebCam or a proximity sensor.

Technical pre-requisites and requirements

To implement these projects, knowledge of machine learning, features extraction, and video processing are needed.

Potential benefits for the future users

IIoT scenarios deal with various stakeholders locally and remotely. Therefore the infrastructure for user identity is beneficial for the identification or authentication of the legitimate users. As these users control the operations of IIoT machines, it is required to have a strict identity verification system. Moreover, the behavior of the users can be analyzed with their system interactions and this analysis is beneficial for detecting any compromised user. Similarly, the de-authentication process helps in proper logging out of the system; thus it provides no scope of misusing the system in absence of system activity by the legitimate users. In a word, this infrastructure helps in detecting and mitigation of anomaly risks.

4.1.12. Infrastructure for remote attestation

Brief description

Remote Attestation (RA) component serves as a suitable security protocol to provide evidence about the integrity of individual devices (e.g., IoT, IIoT, MIIoT). In particular, RA protocol runs between two parties: a trusted party called Verifier and an untrusted party called Prover. At the attestation time, the Prover sends evidence about the current content of its memory to the Verifier, whereas the Verifier checks the information, and establishes whether a Prover is trustworthy. The execution of RA is typically uninterrupted, enabling the detection of mobile adversaries which try to evade detection by getting relocated during the attestation. Thus, the RA component in COLLABS executes a novel protocol for secure asynchronous remote attestation of a group of devices that communicate among themselves by publish/subscribe paradigm to provide distributed IoT services.

Different from the aforementioned swarm attestation protocols that aim to aggregate efficiently the individual attestation results of a group of devices, our RA module also considers the communication data exchanged among devices. Additionally, each device that completes the attestation resumes immediately its regular operation even though the attestation may progress on the other devices, unlike swarm attestation schemes which attest devices synchronously. Finally, the RA module attests a group of devices that interact asynchronously, and each device keeps a historical evidence of these asynchronous interactions.

In particular, the RA module consists of three main phases: (1) Deployment and measurement, (2) Attestation, and (3) Verification.

Deployment and measurement: deployment and measurement is an offline phase that is performed to guarantee a secure setup of the devices on an IoT system before the attestation procedure. A network operator (OP) is responsible for deploying the devices in a secure manner. Moreover, OP is responsible for the key management (i.e., uses an asymmetric key-pair to communicate to each Prover) of the network and the installation of the secure applications on the device. A trusted external party knows the installed version of the applications on the devices and has access to the device binaries. During The measurement, it measures all the legitimate states of each service running on a device. In addition, the Verifier knows the services that are publishers and subscribers and the legitimate interactions among them.

Attestation: to describe the attestation protocol, we assume that an asynchronous distributed IoT service is composed of two services: a publisher and a subscriber. RA protocol exploits asynchronous communication capabilities among IoT devices in order to attest a distributed IoT service executed by them. RA verifies both that each IoT device is not compromised (device trustworthiness), and that the exchanged communication data have not maliciously influenced the communicating devices (legitimate operations). By tracing the execution order of each service invocation of an asynchronous distributed service, RA allows each service to collect accurate historical data of its interactions and transmits asynchronously such historical data to other interacting services.

Verification: starts when the Verifier retrieves the attestation result (e.g., GHVs) from service (S) which acts as a Prover. Along with the timestamped attestation result of S, GHV also contains the timestamp attestation result of previous interacting services i.e., P. The Verifier verifies the checksum of each service P and S that has been included in the evidence GHVs and checks the exchanged data among these services.

Objectives

In the scope of COLLABS framework, RA aims at innovative security objectives, such as SW integrity verification and secure SW updates that would be efficient and interoperable to cope with IoT complexity, heterogeneity, and dynamicity in different industrial settings. In summary, the objectives of RA under the framework of COLLABS are as follows:

- An efficient and effective remote attestation protocol that performs attestation over a potentially large number of resource constrained IoT/IIoT/MIoT devices in a distributed Industrial system.
- Guarantee the integrity of a software running on a single device.
- Protocols that aim to attest a large number of devices in scalable manner (i.e., swarm).
- Performs the attestation of a group of IoT devices without interrupting the normal operation of all the devices at the same time.

Interactions with other components

The following COLLABS components may potentially interact with the RA:

- Hardware Security Component (IFAG- Hardware Security Modules (HSM) whose name is Optiga Trust). The goal of using HSMs is to provide a secure execution environment to allow even very low computational capacity edge devices to perform secure crypto processing and Receive firmware and software updates in a secure and remote way.
- IoT secure wireless fingerprinting (UNSPMF) can gather IoT device data in real-time, ranging from channel state information and radio reception quality metrics, device activity patterns, connection quality, may provide a wealth of information for device behavior modelling and characterization.
- Trusted Execution Environment (TEE) which can act as hardware-protected memory. During RA, TEE loads the code of attestation protocol along with the attestation-related details. It can also act as a memory region that stores keys and is read-accessed only by RA.

Technical pre-requisites and requirements

Device Trust Assumptions: following common assumptions reported in the literature, we assume the presence of three trusted components that reside on a device:

- *Read-Only Memory (ROM): Memory region in ROM where the code of attestation protocol is loaded along with the attestation-related details.*
- *Secure Key Storage: Memory region that stores keys and is read-accessed only by RA. This memory region is generally not updated during attestation.*

Secure writable memory: Memory region that can be read-write accessed only by RA and is used to securely store the vector clock value. The aforementioned memory regions are secure and can be accessed only by authorized entities

Additional information

For attesting potentially large networks of smart devices with unstructured or dynamic topologies additional modules of RA can be integrated, named as PADS: Practical Attestation for Highly Dynamic Swarm Topologies. In particular, PADS builds upon the recent concept of non-interactive attestation, by reducing the collective attestation problem into a minimum consensus one.

Potential benefits for the future users

IIoT comprises a collaborative manufacturing process. Different infrastructural components run with various remote services. The authenticity of the services must be confirmed before they actually execute. Therefore, the remote attestation process helps in this process of authentication. It helps the users to remotely verify the service with hash, failing with the corresponding service can be stopped immediately to investigate further. Without remote attestation, any malicious service can make a trapdoor or backdoor to the system leading to severe security breach or malfunctioning of the industrial outputs. Thus, remote attestation is beneficial for the IIoT users.

4.1.13. Security assurance platform

Brief description

The Assurance Platform is an integrated framework of models, processes, and tools to enable the certification of security properties of services. It uses different types of evidence to demonstrate the support for the required properties and award the corresponding certificate. The types of evidence, which have been envisaged for our framework, include monitoring data and testing data. The security assurance platform will be used for monitoring, testing, and assessing the COLLABS framework.

Lastly, the security assurance platform:

- *Combines runtime monitoring and dynamic runtime testing to ensure correct and effective operation of security controls.*
- *Can be hooked to different systems programmatically through appropriate probes (e.g., event captors, test tools) in order to obtain the monitoring and/or test evidence required for assurance and/or certification assessments.*
- *Operates based on models that determine the operational evidence that should be captured from systems and how it should be assessed (e.g., what conditions it should satisfy) in order to assess the correctness and effectiveness of implemented system security controls.*
- *Enables the runtime assessment of temporal event patterns and rules that can express signature or anomaly-based patterns.*

Objectives

The integration of the SPHYNX Security Assurance Platform is aligned with the 1st of the project's objectives (i.e., "Develop and support a comprehensive cyber-intelligence framework with threat prevention, detection, mitigation and real-time response").

In the context of COLLABS, the main functions of the security assurance platform will be further expanded to meet the security requirements of COLLABS. The platform will be expanded and modified based on the needs of the IIoT environment requirements and Industry 4.0 procedures.

More specifically, and in the context of WP5/Task 5.1, the platform will be extended in ways that allow it to be responsible for monitoring the execution times and accuracy of each and every component of the platform, ensuring and assuring the proper functioning of the whole COLLABS framework.

Interactions with other components

The main functional components of the COLLABS framework that could be taken into account from the Assurance Platform involve those which are related with:

- Data protection
- Threat protection, monitoring and prevention
- Threat-detection and real-time response

A variety of external and/or partners' tools could be also programmatically integrated, in order to expand platform's capabilities on the IIoT 4.0 domain.

The exact interactions and the associated workflows involving the Assurance Platform will be specified once the detailed static and dynamic architecture of the COLLABS framework are defined.

Technical pre-requisites and requirements

The main components of the Assurance Platform are the following:

- **Security Assurance Loader:** The component responsible for receiving the security assurance model for the target organization. This model includes the assets of the organization, security properties for these assets, threats that may violate these properties and the security controls that protect the assets.
- **Monitoring Controller (docker):** The component responsible for initiating, coordinating, and reporting the results of the monitoring process.
- **Testing Controller:** The component responsible for initiating the testing and report the results to the assurance database.
- **Certification Controller:** The component that offers the means for getting the generated certification, via the Retrieval API, for both the service consumer and the CA/Cloud Service Provider.
- **Vulnerability Loader:** The component responsible to load the known vulnerabilities (of the identified assets) and updates the assurance platform depending on the organization's assets included in the assurance model.

Databases:

- **Monitoring Database (included in the Docker),** that holds the monitoring results, the monitoring certificates and the overall process done by the Monitor.
- **Security Assurance Database** that holds the security assurance model and its components.

- **Vulnerabilities database** that holds the known vulnerabilities from NVD.

External components utilized by the Assurance Tool are the following:

- **Monitoring Module** (docker compose) is a runtime monitoring engine built in Java that offers an API for establishing monitoring rules to be checked. The module is made of three submodules: a monitor manager, a monitor, and an event collector. The role of the module is to forward the runtime events from application's monitored properties and finally obtain the monitoring results. This module is offered as a docker component.
- **Virtual Machines (VM)** and other cyber infrastructures, to enable the continuous assessment of the security of cyber systems through the combination of runtime monitoring and dynamic testing.
- **Message Broker (RabbitMQ)** is a messaging bus that allows communication between the external components and the assurance platform.
- **OpenVas** is a software framework of several services and tools offering vulnerability scanning and vulnerability management. The tool is used as part of the dynamic testing offered by the assurance platform.

Potential benefits for the future users

Since that the Security Assurance tool assess the execution and accuracy of each component of the COLLABS platform, it ensures and assures the proper functioning of the whole platform. Thus, the benefit for future users is indirect as it reduces the operational risk of the COLLABS platform in the case of a cyber-attack, avoiding the exploitation of known or unknown vulnerabilities and providing assessments on its total security posture. The un-affected operation of COLLABS solution enables the secure data exchange across the digital supply chain with a high degree of trust enforcing a high degree of resilience, reliability, and accountability. Thus, the Security Assurance can offer a unique selling point towards COLLABS adoption as the security assurance for on the proper operation of the COLLABS platform assures that the platform operation it does not interfere with the supply chain's day to day processes.

4.2. Secure development and configuration components

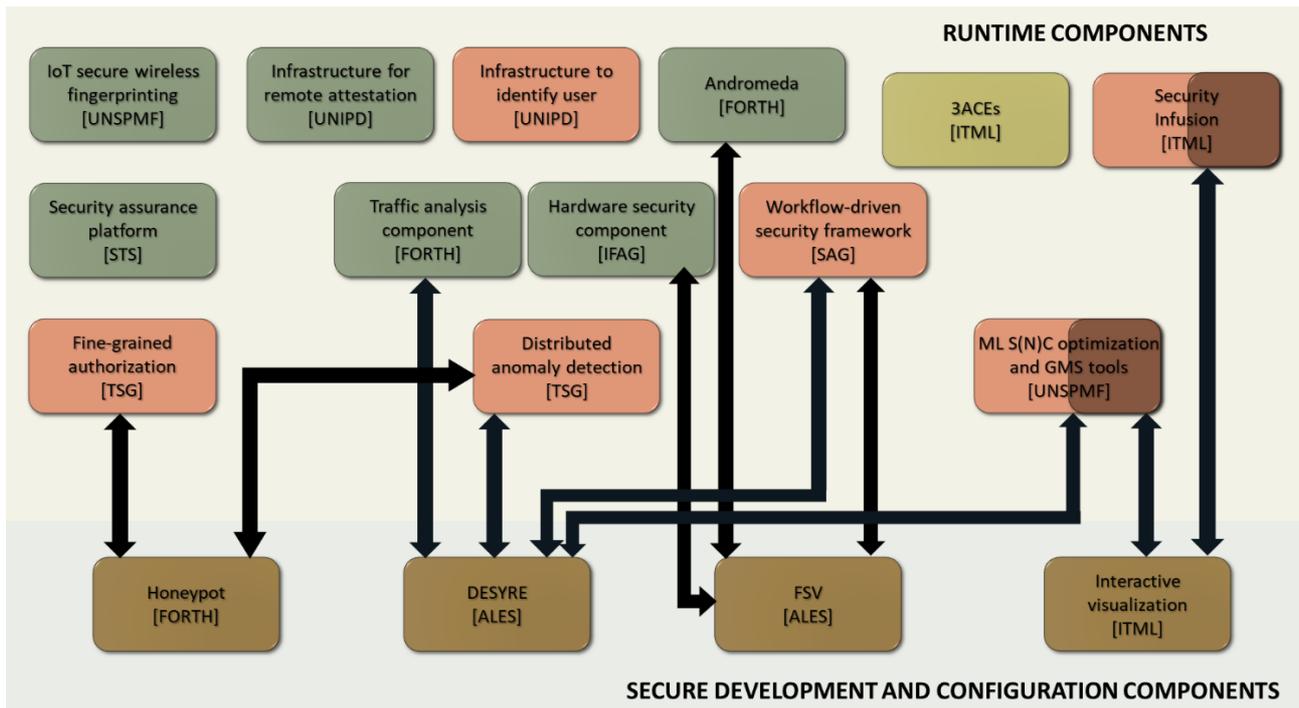


Figure 18. Secure development and configuration components.

4.2.1. Honeypot

Brief description

Our Honeypot implementation will emulate working systems in an industrial setting and will be able to attract traffic from malicious actors.

Objectives

Our objective for this module is to act as an extra line of defense against attacks in an OT environment. Our honeypot will be able to attract the attention of attackers by blending in the environment and running services sought by the attackers.

Interactions with other components

Our module will report alerts to anomaly detection modules.

Technical pre-requisites and requirements

6-8 GB of RAM, 128 GB SSD.

Potential benefits for the future users

The OT-Honeypot will pose as a vulnerable OT device and will attract the attention of an attacker by emulating old and vulnerable services. Any information about scanning or attempting to exploit the honeypot will be immediately sent to the end-users. This will provide the end-users with an extra defense mechanism which can inform them of attackers trying to pivot inside their network. The information provided will assist to determine valuable intelligence on the attack taking place such as its origin and lower its impact by producing immediate alerts.

4.2.2. DESYRE

Brief description

The DESYRE framework is a virtual prototyping environment. The simulation engine enables the simulation of the specified system architecture at multiple levels of abstraction. In the simulation environment, the computation, networking, and physical aspects of the system are co-simulated together for fast and accurate design exploration, verification, and performance evaluation. Based on SystemC, the simulation engine leverages coordination of heterogeneous Models of Computation (MoC) required today to model and simulate complex Cyber-Physical Systems (CPS). Besides SIL, DESYRE offers also Virtual-Processor-in-the-Loop capabilities via the integration of QEmu ISS (Instruction Set Simulator). QEmu is a generic and open-source machine simulator and virtualiser allowing the execution of target software binaries including operating systems and applications on a host computer.

Objectives

ALES plans to use DESYRE within COLLABS for extending ALES physical pilot/demonstrator setup with a virtual environment to support validation of COLLABS platform components. The virtual environment will be completely transparent to the consortium and will be used only for extension of the physical pilot if necessary. DESYRE tool can support virtualization of Collaborative Manufacturing scenarios, including simulation of domain-specific protocols (such as IEEE 802.3/802.11/800.15.4, CAN 2.0, MQTT and TCP/IP-based communication stacks).

Interactions with other components

DESYRE virtualization does not add an extra security functionality but it can add more degrees of freedom in COLLABS technologies experimentation to what the physical pilot can provide. We envision the following technologies to possibly benefit from a virtual extension of the pilot environment:

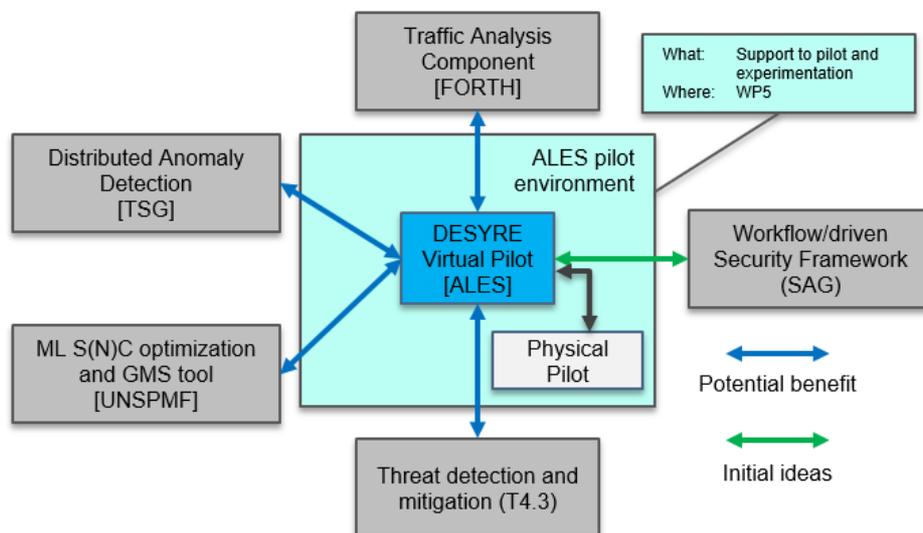


Figure 19 DESYRE link to ALES pilot and interaction with other components

Note: other components may benefit from application of DESYRE to assess their integration into COLLABS through ALES laboratory.

Technical pre-requisites and requirements

FW/SW to be simulated should be available (this may not be the case for industrial PLC/II-IoT devices and for MES/ERP or similar applications) and compatible with supported HW platforms in the simulation environment built-in model library. Communication stacks should be supported in simulation or freely

available for download and compatible with supported HW platforms. ALES does not plan to develop ad hoc models for COLLABS demonstration.

Additional information

DESYRE will be used only by ALES to extend ALES pilot in COLLABS

Potential benefits for the future users

DESYRE is used in COLLABS to extend ALES physical pilot/demonstrator setup with a virtual environment. The ability to add virtual components and thus to create a hybrid laboratory allows ALES to easily adapt the environment to various type of requests by reconfiguring via software the network architecture. The virtualization software allows the user to emulate a hardware component at a deep level (it models the entire protocol stack up to physical level). This provides the ability of testing and evaluating very specific hardware (and its scalability) without actually buying it. This provides a cost/effective way of exploring new technologies with large-scale testing.

4.2.3. FSV

Brief description

Formal Specs Verifier (FSV) is an industrial-strength formal verification framework, providing an environment for analysis of complex systems designs against functional, safety and security requirements. The framework is structured into: (1) a translation layer, supporting automated and formal transformation from a system design language to a mathematical model including formal requirements specifications, (2) an algorithmic layer, where the various verification objectives are addressed by specific verification algorithms, (3) an analytic layer, where computational tasks generated by verification conditions are discharged by backend engines, such as SAT/SMT/OMT solvers, industrial and academic model checking tools, internally developed analytics for specific verification tasks. The platform has a high-maturity core, developed across years, and currently adopted in multiple industrial programs, and it can be extended with more explorative/research tools/analyses by leveraging its layered architecture. Extensions can include design and specification languages, new verification tasks and related algorithms, novel analysis back-ends.

Objectives

In the scope of COLLABS, the FSV tool is used to evaluate cybersecurity of existing architectures and validate (by formal verification) designs based on high assurance security components.

In particular, we foresee these potential applications:

- Verifications are employed to formally analyze security of core components and their interactions, to provide trust in COLLABS security building blocks, considering:
 - o HW security elements' interaction with SW/OS.
 - o Communication and coordination mechanisms.
 - o Isolation and segregation of information flows
- Analysis of cybersecurity risks of Industry 4.0 infrastructures to support COLLABS solution deployment.

Existing verification algorithms and analytical back-ends will be evaluated to support the different verification and analysis needs. Potential integration of external academic tools will be evaluated on the basis of partners' feedback.

Interactions with other components

As an example, we envision to use FSV tool in the design and integration of the following components:

- *Workflow driven Security Framework (4.1.10): in task 2.6 we anticipate a collaboration with SAG to verify security properties of workflows and smart contracts generated by their framework with FSV*
- *Trusted Execution Environments (4.1.1): in task 2.1 we aim to define an approach to formally validate information flow policies implemented by TEEs, with specific reference to ARM TrustZone and Intel SGX approaches.*
- *Hardware security component (4.1.3) & Trusted Execution Environments (4.1.1): in tasks 4.1 and 4.2 we envision the definition of a combination of TEE and HW security component, and the formal validation of their interaction to guarantee security properties at design time.*
- *Hardware security component (4.1.3): in task 3.2 and 3.3 we consider a TPM that can support a PKI and blockchain infrastructure. In this context a potential application of formal verification can be evaluated to establish correct integration patterns and communication.*

Note: other components may benefit from application of FSV to assess their design and/or integration architecture into COLLABS.

Technical pre-requisites and requirements

Cybersecurity evaluation of architectures and validation of designs by formal verification requires a description of the architecture and data flows that will require modeling. Verification is performed against requirements that are agreed with technology providers and users. Formal modeling of architecture, data flows and requirements will be agreed with technology providers and customers.

Additional information

FSV will be used by ALES to support design and validation of COLLABS solutions.

Potential benefits for the future users

FSV can be used to provide formal guarantees about specific properties. This means that once a design/architecture gets properly modeled is possible to prove some (security) properties in it. This opens to various benefits: the project under analysis receives formal correctness guarantees that can help for certification purposes. Formal property checking provides stronger requirement satisfaction guarantees compared to usual testing/simulation and therefore is a great improvement for safety critical systems. Furthermore, formal verification provides a higher degree of confidence that bugs or attacks will not disrupt the product, and this reduces risk of incidents and thus mitigate the derived risk of economic and branding loss.

4.2.4. Interactive visualization

Brief description

A collection of visualization elements that can receive data in multiple formats and formulate dynamic multi-targeted dashboards for users of different level of IT expertise.

Objectives

The Interactive visualization module offers interconnected and interactive visualizations of captured security events and operational metrics. It enables situational awareness of end users and helps them identify patterns or correlations among events which can foster the decision-making process. Moreover,

users can check to see if any abnormal situation seems to be about to happen (or already took place) and generally search for patterns in events and metric values that can reveal correlations and help them decide on appropriate actions.

Interactions with other components

The module will interact with other components in terms of receiving their output as the information to be visualized. This can be achieved via provided APIs or other access method, e.g., direct access to the relevant data, message-based communication (MQTT), etc.

The module can be also adapted to serve as an entry point for available user actions. Visualizations can be connected to interfaces of other components and therefore allow users to navigate seamlessly among them.

Technical pre-requisites and requirements

The module is deployed as a web application together with an optional accompanying backend sub-module for advanced data import capabilities.

Potential benefits for the future users

Considering that it offers interconnected and interactive visualizations of captured security events and operational metrics, it reduces users' inconvenience when attempting to interact with component or when receiving output for visualized information. To that extent, users can take advantage of the tool's flexibility of deployment and access acquisition, because it performs under a plethora of various conditions, which facilitates the operational processes for the users. At the same time, the tool provides a seamless navigation experience among different interfaces of deployed components, due to its adaptability, which can reduce the cost of having to deploy a different solution at each of the individual modules.

5. Integration of Security Aspects

In this section we describe multiple-levels security mechanism that consists of three security levels. The first level consists of hardware-enabled and device-level security mechanisms, the second level includes security-enabling functionalities based on distributed ledger technologies (blockchain). The third level of security corresponds to applying system-wide machine learning-based techniques to provide contextual awareness and deliver cognitive security-enabling mechanisms. Levels 2 and 3 correspond to information exchange between the devices either within the boundaries of the smart factory, or external partners within the digital supply network.

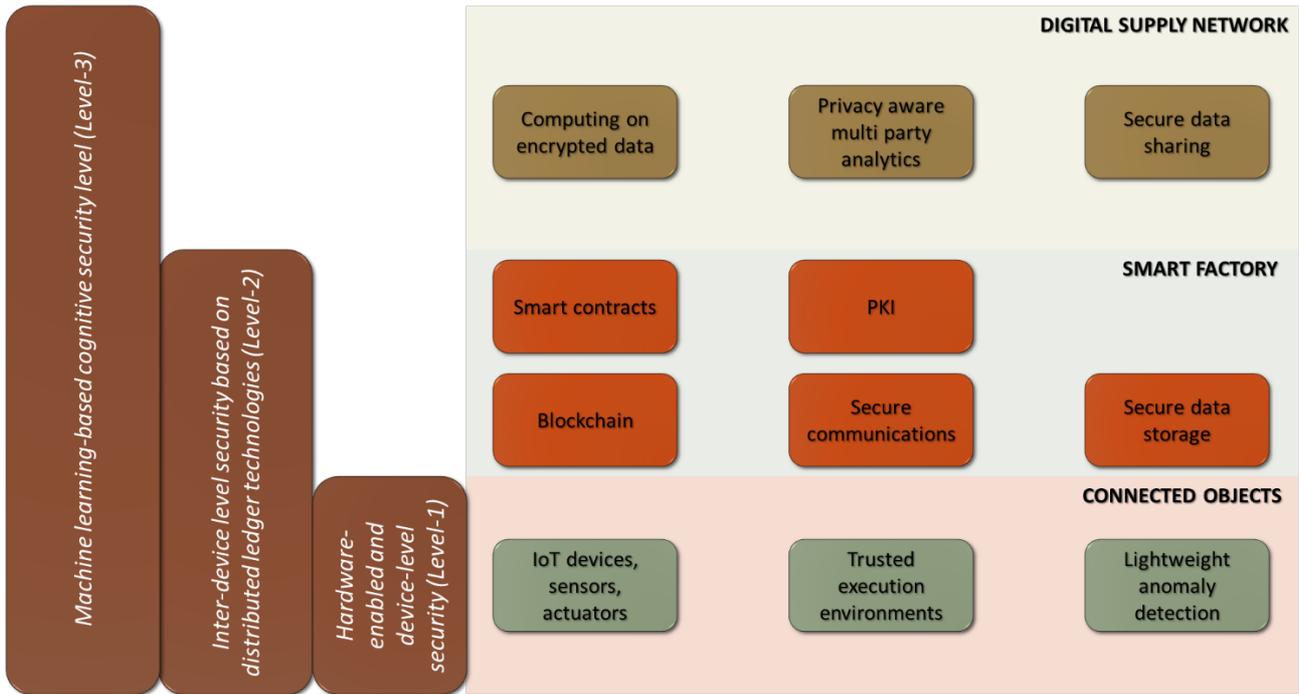


Figure 20. Cyber-Intelligence manufacturing framework for digital collaboration

5.1. Hardware-enabled and device-level security (Level-1)

Public Key Infrastructure (PKI), the topic of the T3.3, is a combination of hardware, software, and security policies and procedures that allow the safe execution of cryptographic operations, such as encryption, digital signature, and non-repudiation of electronic transactions. It is very important that PKI related operations are performed in a secure environment to ensure that the security objectives of this procedure are achieved. Likewise, it is essential that the hardware used for this type of communication has valuable data storage space that ensures that this data is not read or modified by third parties. To achieve this (secure storage and execution environment), the use of Hardware Security Modules (HSM) is very often used. These modules are non-programmable hardware focused on executing crypto operations in the safe and reliable way.

In the field of HSM Infineon has the Optiga family. In this family, the Optiga TPM (Trusted Platform Module) stands out, focused on its use in high computational capacity microprocessors, together with the Optiga trust M focused on its use in low computational capacity microprocessors. Thanks to these devices, secure and reliable communication can be achieved, both at a high level and at the edge device level. These tools are essential for the correct implementation of WP4 (T4.1 specified, providing a secure execution environment for the edge IoT devices).

These HSMs also allow an end-to-end encryption connection with blockchain network directly from edge IoT devices, being a very useful tool for providing data to the smart contracts, both public and private to the T3.2.

5.2. Inter-device level security based on distributed ledger technologies (Level-2)

This section describes how COLLABS ledger-based security modules can secure inter-device communications and enhance the trust level in inter-device collaboration, on several aspects detailed below, at several key moments of the Smart Factory lifecycle.

COLLABS protects the Smart Factory assets, in providing a comprehensive and decentralized access control (T3.1). Relying on a fine-grained authorization module (section 4.1.4), COLLABS ensures that all the data produced within the Smart Factory, collected from Connected Objects, and all the actions performed on Connected Objects, comply with the access rights granted by the effective security policy. Data sensitivity can either be manually identified by design, or automatically using machine learning algorithm through confidential data discovery (T3.4). Communication channels are secured in confidentiality, integrity, and authenticity thanks to a ledger-based PKI (T3.3), both for device-to-device as for user-to-device interactions. COLLABS users can be authenticated using innovative user identification technique through a specific infrastructure (section 4.1.11). Usage of a distributed secure storage relying on a blockchain (T3.2) enhances the availability of the security modules protecting the Smart Factory assets.

COLLABS also protects the Digital Supply Network by increasing the trust level in the Smart Factory. At design time, COLLABS provides formal validation tools for architectures cybersecurity evaluation (section 4.1.12). At run time, a decentralized architecture using smart contracts in the blockchain (T3.2) is also a trust enhancer, both for within the factory as between factories. Offering multiple protection layers, it enables the usage of a workflow-driven security framework (section 4.1.10), allowing collaboration and exchange between different stakeholders, while ensuring continuous data protection and security policy enforcement.

5.3. Machine learning-based cognitive security level (Level-3)

Machine learning based (ML) approaches are highly relevant for the COLLABS framework and will influence all layers of its architecture, coming from two different point of views.

On the one hand, ML-based approaches need to provide reliable security for being used in a distributed environment. COLLABS provides the ground for distributed workflows and processes. In that context, distributed ML-based computations are heavily used, and it needs to be ensured that those are executed reliably and secure, e.g., that the confidentiality of data processed is protected. In that sense, security is a key requirement for distributed ML-based computations as addressed in section 5.3.1.

On the other hand, ML-based approaches are also used to implement security measures: In COLLABS, machine learning algorithms are used to implement device fingerprinting and anomaly detection measures. From that point of view, machine learning is an enabler for core security mechanisms of COLLABS, see section 5.3.2.

5.3.1. Security of machine learning based models

COLLABS assumes a scenario where a required computation performed by a ML-based model is offered by a third-party provider. The key-question is how one can ensure that the inputs from each party are not exposed to other involved parties.

In particular, COLLABS is interested in two main variations of that scenario: a) the computation is conducted by a third-party provider and data has to be uploaded/made available to that provider. In such a case a consuming party wants to make use of the ML-based service and at the same time keep its data

confidential against the third-party provider. In a second scenario b), the ML-based computation demands for data input to be provided by multiple parties. Those parties are interested in the computation's results but, again, want to preserve confidentiality of their data against the other parties. In both cases, COLLABS needs to deal with the issue of the protection of sensitive data (business, private, etc.) from all involved parties, including the ML-model provider.

The high-level approach typically involves either breaking up the original problem to a smaller set of operations that can be executed in an isolated fashion e.g., via Secure Multi-Party Computation (SMC) [7]. Or, alternatively, it can be executed on an encrypted set of inputs and deliver approximations of the output, as if it were executed in the original model with plaintext input, e.g., Homomorphic Encryption (HE) [8]. The challenge is to use white-box approaches such as those proposed by the SMC and HE communities in order to implement black-box applications such as ML-based. In practice, COLLABS aims at achieving privacy-preserving interference on deep neural networks, but to get there, new models will have to be trained.

For that purpose, we will investigate the full range of SMC and HE algorithms that can be used. The SMC solutions range from the Yao Garbled Circuits and the Oblivious Transfer protocols to the Goldreich-Micali-Wigderson (GMW) protocol and secret sharing schemes. On the other, though the HE schemes are rather new, they support a variety of options (BFV, BGV, TFEW, fully/partially HE etc.). Each one of these algorithms offers a different level of security and its performance strongly depends on the characteristics of the function that protects.

Both techniques, HE and SMC, have limitations that need to be taken into account: The bottleneck of HE techniques usually is their computational complexity, while SMC typically bears high communication complexity. COLLABS aims to design a framework that combines both techniques for the secure evaluation of ML models. In order to address performance requirements, trusted execution environments (TEE) capabilities will be employed: Building on hardware security, we aim to reduce the overheads introduced by SMC and HE techniques, by performing (limited) computations efficiently and securely through the use of dedicated crypto chips.

Based on the above-mentioned arguments and explanation, in terms of implementation, a universal solution for all possible use cases can hardly be realized. Instead, COLLABS will provide building blocks that can be integrated and easily tailored to the needs of each use case. That way, combinations of the developed SMC and HE algorithms can easily be reused. Depending on the industrial use cases of COLLABS, security, communication, and computational requirements, as well as the type of the ML model, the design of a secure algorithm for training and using the ML model will be influenced. COLLABS will implement some of these designs, using publicly available SMC and HE libraries. Of course, these implementations will also depend on technologies that the COLLABS consortium decides to use.

Data confidentiality protection in the context of distributed and ML-based processes is highly relevant for the digital supply network layer of the COLLABS architecture. As highlighted in Figure 6, the described aspects secure data sharing and computing on encrypted data will be handled and integrated there.

5.3.2. Machine learning-based device fingerprinting and anomaly detection

Data coming from each field device will be continuously reviewed and pre-processed for device identification and verification, anomaly detection, etc. For that purpose, COLLABS plans to develop dynamic behavior models using real-time data collected from IoT devices, including channel status data, radio reception quality, device activity patterns, etc.

An enclosed public space (a building on the UNSPMF campus) will be used to setup and test fingerprinting by pre-collecting a set of device signals. Deep learning models will be applied to improve the effective

identification of fingerprint-based devices. A set of new methods will be developed for the rapid and efficient training of deep learning models using established indoor channel models, ray-tracing tools, and 3D object modeling. Such training methods will provide an important layer to the security and ambient intelligence and its deployment in real world Wi-Fi IoT systems. For training and inference, we plan to use structured convex and non-convex methods and neural network-based methods. Since IoT devices have low processing power and storage capabilities, we plan to use lightweight complexity machine learning methods such as auto-encoders with a small number of hidden layers or first-order stochastic methods.

Another option worth considering in this scenario is the use of federated learning schemes [9]. In such an approach, we would have auto-encoders running on IoT edge devices, doing anomaly detection analysis, and exchanging neural network weight updates through a central server. Edge devices would connect to the central server using NB-IoT.

Identifying anomalies of local field devices and of interconnected objects are key concerns of the layers connected objects and smart factory. As illustrated in Figure 6 those aspects will be addressed in these two layers of the COLLABS architecture.

5.4. End-to-end security aspects

In addition to the technologies belonging to the 3 dimensions covered by COLLABS, as described in the previous subsections, several end-to-end security aspects will be integrated into the developed solution.

More specifically, and in the context of the WP5 efforts, the project will also design, develop, and integrate building blocks towards an end-to-end integrated cybersecurity framework for collaborative manufacturing environments. Said framework will provide an assurance and accountability-based solution to address the IIoT challenges, featuring a transparent, dynamic, security assessment and certification tool that will be used for monitoring, testing, and assessing the COLLABS framework.

The latter tool will be based on the Assurance Platform of Sphynx, as detailed in 4.1.13, which will be extended in the context of T5.1 to meet the security requirements of the COLLABS solution, integrating a number of event captors and deployed security mechanisms. The aim is to allow the real-time security assessment of the security posture of COLLABS. Components to be integrated within the Assurance Platform will include data protection, threat protection, monitoring and prevention, as well as real-time response mechanisms of COLLABS. As mentioned, the exact interactions and the associated workflows involving the Assurance Platform will be specified once the detailed static and dynamic architecture of the COLLABS framework are defined.

Moreover, the end-to-end security solutions integrated into COLLABS will include distributed ledger technologies (Blockchain) to enhance the IIoT environment in terms of auditability, reliability and accountability, thus supporting data federation partners that may want to protect their data and analytics results from competitors, or to monetize their data selectively. These will, again be carried out in the context of WP5 (T5.1, in specific), building on work delivered in T2.6 and T3.2.

The above will be augmented by advanced informative forensics mechanisms and interactive visualizations developed in the context of T5.2, that will be exploited in order to ensure real-time event management related to potential cyber threats. Aiming towards the envisioned end-to end integrated security solution of COLLABS, informative mechanisms for predicted security threats, current incidents, and the system actions to mitigate them will be deployed, also including the delivery of forensic information to analyse and understand the cause of a problem so as to take preventive measures for the future.

Integrating the above into a homogeneous solution will be achieved through continuous integration efforts which, in the context of T5.3, will ensure that all developments towards the envisioned integrated COLLABS

IIoT framework will be realized under trusted execution environments following at every step the Quality Assurance and Control procedures (ISO 9004:2018) of the project.

Finally, following the integration of the end-to-end security aspects, significant effort will be dedicated (see T5.4) to support the commercialization activities of COLLABS, by releasing a stable and reliable solution for any end-to-end Industrial IoT environment. These efforts will include the definition of best practices for maintaining and operating the framework in the long-term, and verifying the usefulness of the proposed solutions and its efficient use in a large-scale utilization. Moreover, these efforts will also address the legal, ethical, privacy, operational and accessibility concerns related to the utilization of the solution in real world scenarios, while coordinating the production of an end-user guide for installing, deploying, and using the COLLABS framework and its components.

6. Real-life industrial demonstration - pilots

This section defines a preliminary plan for demonstration. First, it describes the rationale of the experimentation protocol. Then, it determines the outlines and preparation for COLLABS demonstration and pilot's execution. Finally, it defines the evaluation guidelines and objectives for results analysis.

The experimentation protocol

The scope of the experimentation campaign is to demonstrate the COLLABS solution in real-world setting. In particular, an evaluation of the COLLABS KPIs (identified in Section 1.1.2 of the proposal) is going to be performed on demonstrators representing the use cases proposed by the industrial partners of COLLABS. A detailed description of those use cases can be found in a dedicated section of the deliverable D1.2.

The experimentation protocol will organize the lifecycle of verification and validation methodology including arrangements for how they will be run and what processes need to be put in place to check that the output is both correct (verified, does what it is intended to do) and valid (relevant, meets the needs of users). In particular the evaluation will be performed not only considering COLLABS objectives but also taking into account the industrial requirements and common threats identified in deliverable D1.2 throughout the analysis of all the use cases presented.

The experimentation protocol will characterize the demonstrators by defining all the organizational aspects required such as: dates and place, prerequisites, panel of users, speakers, stages of development, planning, material means, various elements to be supplied by all partners, deployment and integration strategies and testing methodology. The experimentation protocol will also outline the setting limitations to provide a fair evaluation of the results.

The result evaluation will be defined in the experimentation protocol. All the policies and rules for the collection, process, storage, and publication of the result data will be properly defined taking into account both the proper regulations such as GDPR and the consortium members confidentiality requirements. The result data will be used to evaluate the success of COLLABS according to the KPIs listed in proposal section 1.1.2 "Detailed Objectives". A plan for giving feedbacks to use case and technology provider will also be defined.

More details on this topic can be found in D1.2 and or they will be formalized in WP6 deliverables.

Collaborative manufacturing demonstration outlines

Following the use cases described in Deliverable 1.2, we plan to address a set of schemas that will reproduce the principal digital integration needs arising in collaborative manufacturing:

1. **Multi-tier:** interaction of manufactures at different layers of the supply chain (e.g. materials, parts, systems), with accompanying quality and certification data;
2. **Multi-factory:** geographic distribution of manufacturing sites of the same company, collection of real-time data and maintenance at global scale;
3. **Multi-role:** customer/supplier interaction, interaction with service provider, authority requiring access to data for compliance audits, cybersecurity operations (monitoring, detection, response, forensics), non-malicious threat actors (human error in normal operations), malicious internal or external threat actor (profile: position and attack surface, motivations, capabilities and tools);
4. **Multi-tenant:** integration of external services in the manufacturing process, such as in service-oriented infrastructures (offload of computations, such as on sensitive production, or cloud-based IT infrastructures) or in third-party subcontracting for manufacturing process activities (e.g. parts quality inspection, test, validation);

Preparation for the experimentation protocol

Pilots will start from existing smart manufacturing infrastructures to improve their security through COLLABS technologies. We define a template to collect needs, requirements, and constraints for deployment of COLLABS technologies from both the infrastructure owners and the technology providers. This will enable a feasibility assessment for deployment and operation and start planning the preparatory work for demonstration:

1. **Security measures deployment:** can be a new physical device added to the existing infrastructure, a new software on existing device, an additional hardware device attached to an embedded platform or policies & rules (e.g. physical access policies management). These features should be characterized with their target domain, integration requirements and constraints, interaction with the existing systems and if applicable their data model (what info they access and how this is treated).
2. **Operational requirements:** describe configuration plan, connectivity needs, and pilot owner's involvement. Document the interaction with existing infrastructure in operation and define process for capturing and documenting bugs or malfunctions. A rollback plan for restoring operations should also be devised.
3. **Legacy (integration and retrofitting):** consider legacy technologies and define lightweight deployment plans. If deployment is unfeasible, define strategies for integration and protection, to allow partial benefit of COLLABS innovation and broader exploitation.
4. **Safety and integrity constraints:** defines rules and policies for accessibility to real world infrastructure. Factory/enterprise infrastructure in operation may not be accessible to avoid any impact due to COLLABS experimentation, and expensive equipment may not be available for direct hands-on experimentation, but may be accessible through other controller devices. Due to IP protection requirements real network traffic data might not be available.

The evaluation and objectives

The evaluation and objectives will put in situation the COLLABS framework with real-world use cases from manufacturing domain. The evaluation will involve representative operating requirements and constraints provided by end users. This evaluation will allow:

- To validate the adequacy between the technologies provided in the COLLABS framework and the cybersecurity challenges.
- To identify the successes and the limitations of the COLLABS framework to address users use-cases.
- To identify the efforts to industrialize the COLLABS framework.

The main objectives associated to the evaluation of the COLLABS framework are listed below:

- **Objective 1:** guarantee the continuity of the production process as a main objective.
- **Objective 2:** cover cybersecurity threats identified in each scenario of the demonstrators.
- **Objective 3:** COLLABS framework should be easy to integrate and deploy.
- **Objective 4:** facilitate a secure exploration of IIoT's full potential in collaborative manufacturing environments and realize societal and industrial opportunities.
- **Objective 5:** provide scientific and technological advances in IIoT-based digital collaboration and security in the context of Industry 4.0
- **Objective 6:** provide effective means for digital collaboration and data exchange in a secure fashion

D1.2 - System Architecture Definition

These high-level objectives are detailed with KPIs that can be found in section 1.1.2 of the proposal and will be formalized for real success measurement in WP6.



7. Summary and Conclusion

This deliverable provides the specifications of the COLLABS platform architecture, based on a thorough overview of state-of-the-art methods, functional and non-functional requirements, reference infrastructures and use cases. It draws on research and conclusions from Deliverable 1.1 - COLLABS Innovations for Industrial IoT Systems and Deliverable 1.2 - Positioning of COLLABS.

Components of the COLLABS architecture have been described in detail, including runtime components and secure development and configuration components, as well as their integration and interaction, with an indication of the efforts that must be made to implement, integrate, and demonstrate such an architecture. Special attention was paid to functional elements of the framework and their interaction with security levels by using them as dimensions onto which runtime components were positioned, i.e., classified. In the first iterations of development of the framework, we expect to achieve an even higher level of understanding of requirements and functional elements together with their interactions. In accordance to this, we plan to further refine the connection between requirements and proposed architecture of the system in further deliverables within the COLLABS project.

Deliverable defines a mapping between the components offered by technology providers and common security requirements (CSRs) defined. On the other hand, the components have been mapped to the key performance indicators to which they potentially relate. By combining these two mappings, we in fact defined the mapping between CSRs and KPIs.

Integration of security aspects was also discussed in detail. Finally, the groundwork was laid for real-life industrial demonstration and evaluation.

The specifications given in this deliverable will serve as input for further work towards the implementation of the COLLABS framework components and their integration. The first part of the project will focus on the development and internal testing of system components, while the second part will focus on integration activities, testing and demonstration of the platform as a whole.

The COLLABS architecture will be continuously updated following the technical and business achievements of the project and growth of consortium's knowledge of the system components and their interactions through the process of implementation and integration.



References

- [1] P. Bernus and L. Nemes, "A framework to define a generic enterprise reference architecture and methodology," *Computer Integrated Manufacturing Systems*, vol. 9, no. 6, pp. 179-191, 1996.
- [2] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle and G. Guissanie, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST 800-171 Rev 2," NIST, 2020.
- [3] T. J. Williams, "The Purdue enterprise reference architecture," *Computers in Industry*, pp. 141 - 158, 1994.
- [4] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, San Jose, CA, 2014.
- [5] W. S. Alaloul, M. S. Liew, N. A. W. A. Zawawi and B. S. Mohammed, "Industry Revolution IR 4.0: Future Opportunities and Challenges in Construction Industry," *MATEC Web of Conferences*, vol. 203, pp. 1-7, 2018.
- [6] P. Kasinathan and C. Jorge, "Securing emergent IoT applications," in *International Summer School on Engineering Trustworthy Software Systems*, 2018.
- [7] R. Cramer and I. Damgard, "Multiparty Computation, an Introduction," in *Contemporary Cryptology*, 2005, pp. 41-87.
- [8] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41. annual ACM symposium on Theory of computing*, Bethesda, MD, USA, 2009.
- [9] J. Konecny, B. McMahan and D. Ramage, "Federated Optimization: Distributed Optimization Beyond the Datacenter," *CoRR*, 2015.
- [10] S. Lin, B. Murphy, E. Clauer, U. Loewen, R. Neubert, G. Bachmann, M. Pai and M. Hankel, "Architecture Alignment and Interoperability—An Industrial Internet Consortium and Plattform Industrie 4.0 Joint Whitepaper," 2017.