Transform safety-critical Cyber Physical Systems into distributed solutions for end-users and partners

D9 (D3.2)

Selection of concepts for end-to-end security and privacy for distributed CPS solutions

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 101007260. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Netherlands, Finland, Germany, Poland, Austria, Spain, Belgium, Denmark, Norway.

Document Information

Project	TRANSACT
Grant Agreement No.	101007260
Work Package No.	W3
Task No.	T3.2
Deliverable No.	D9
Deliverable No. in WP	D3.2
Deliverable Title	Selection of concepts for end-to-end security and privacy for distributed CPS solutions
Nature	Report
Dissemination Level	Public
Document Version	v1.0
Date	30/05/2022
Contact	Paul Pop
Organization	DTU
Phone	+45 4525 3732
E-Mail	paupo@dtu.dk

Authors Table

Name	Company	E-Mail
Wolfram Ratzke	AVL	Wolfram.Ratzke@avl.com
Claus-Henning Friederichs	AVL	Claus-Henning.Friederichs@avl.com
Annalena Belnarsch	AVL	Annalena.Belnarsch@avl.com
Ralph Weissnegger	CISC	r.weissnegger@cisc.at
Mateusz Bonecki	DAC	mateusz.bonecki@bettersolutions.pl
Marek Tatara	DAC	marek.tatara@dac.digital
Marek Mioduszewski	DAC	Marek.mioduszewski@dac.digital
Patryk Monarcha	DAC	Patryk.monarcha@dac.digital
Paul Pop	DTU	paupo@dtu.dk
Nicola Dragoni	DTU	ndra@dtu.dk
Gaurav Choudhary	DTU	gauch@dtu.dk
Peter Mortier	FEops	peter.mortier@feops.com
Bjorn Kristinsson	FEops	bjorn.kristinsson@feops.com
Dries Desmet	FEops	Dries.desmet@feops.com
Reinjan Ergo	FEops	Reinjan.ergo@feops.com
Markus Kantonen	FLEET	markus.kantonen@fleetonomy.ai
Oscar Nissin	FLEET	oscar.nissin@fleetonomy.ai
Roope Ritvos	FLEET	roope.ritvos@fleetonomy.ai
Mika Jaakonaho	FLEET	mika.jaakonaho@fleetonomy.ai
Marko Komssi	FSC	Marko.komssi@f-secure.com
Pilvi Tunturi	FSC	Pilvi.tunturi@f-secure.com
Perttu Ranta-aho	FSC	perttu.ranta-aho@f-secure.com
Mateusz Groth	GUT	mateusz.groth@pg.edu.pl
Lukasz Szczygielski	GUT	lukasz.szczygielski@o365.pg.edu.pl
Jarno Kallio	NOD	jarno.kallio@nodeon.com
Lari Vaananen	NOD	lari.vaananen@nodeon.com
Timo Majala	NOD	timo.majala@nodeon.com
Bjørn Åge Hjøllo	NVT	bjorn.hjollo@navtor.com

Rafael Vidal	SNG	rafael.vidal@singlarinnovacion.com
Angel Guillemes	SNG	angel.guillemes@nunsys.com
Jordi Cabot	UOC	jordi.cabot@icrea.cat
Abel Gómez	UOC	agomezlla@uoc.edu
Iván David Alfonso Díaz	UOC	ialfonsod@uoc.edu
Juhani Latvakoski	VTT	juhani.latvakoski@vtt.fi
Pertti Peussa	VTT	pertti.peussa@vtt.fi
Vesa Kyllonen	VTT	vesa.kyllonen@vtt.fi
Jussi Ronkainen	VTT	jussi.ronkainen@vtt.fi

Reviewers Table

Version	Date	Reviewer
v0.9	15/04/2022	Wolfram Ratzke (AVL/DE)
v0.9	15/04/2022	Alexandr Vasenev (TNO)
v0.9	15/04/2022	Marko Komssi (F-SECURE)
v0.91	20/05/2022	Sasa Marinkovic (PMS)

Change History

Version	Date	Reason for Change	Affected pages
v0.9	04/03/2022	Final Draft for Review	All
v0.9	16/03/2022	Updates based on Paul Pop's Comments	All
v0.9	17/03/2022	Updates based on UCs Comments and FLEET Inputs	All
v0.91	19/05/2022	Updates based on Comments	All
v1.0	30/05/2022	Final version for submission	n/a

Table of Contents

List of Figures

List of Tables

1 Glossary

Term	Definition
Allocation	Task allocation refers to the runtime decision of task placement and scheduling associated with the resource management.
Application	The functionality that implements a particular solution to help the end-user to perform a specific task. An application can be composed of a monolithic service or a group of distributed services which are executed in different and distributed targets in the device, edge, cloud continuum.
Architecture	The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution.
Architecture framework	Conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders.
Component	One of the parts that make up a system.
Computing platform	A computing platform is the environment in which a piece of software is executed. It may be the hardware or the operating system (OS), even a web browser and associated application programming interfaces, or other underlying software, as long as the program code is executed with it. Computing platforms have different abstraction levels, including a computer architecture, an OS, or runtime libraries. A computing platform is the stage on which computer programs can run.
Concept	An abstraction; a general idea inferred or derived from specific instances.
Cross-cutting concepts	System-level methods and techniques for linking application and platform. They include concepts for designing and deploying the application on the platform, as well as analysing and run-time monitoring and managing the behaviour of the application running on a specific platform in the device, edge, cloud continuum.
Cyber-Physical System	Digital system that semi-automatically interacts with its physical environment as integral part of its functionality.
Device	Physical entity embedded inside, or attached to, another physical entity in its vicinity, with capabilities to convey digital information from or to that physical entity.
Method	A method consists of techniques for performing a task, in other words, it defines the “how” of each task.
Methodology	A collection of related processes, methods, and tools. A methodology is essentially a “recipe” and can be thought of as the application of related processes, methods, and tools to a class of problems that all have something in common.
Middleware	Middleware is computer software that provides services to software applications beyond those available from the operating system. It can be described as "software glue". Middleware makes it easier for software developers to implement communication and input/output, so they can focus on the specific purpose of their application.
Mission-critical system	A mission critical system is a system that is essential to the survival of a business or organization. When a mission critical system fails or is interrupted, business operations are significantly impacted.
Orchestration	Type of composition where one particular element is used by the composition to oversee and direct the other elements.

	Note: the element that directs an orchestration is not part of the orchestration.
Partitioning	Divides the application code into several parts that will be executed on different platforms, i.e., mobile devices, cloudlets, or the cloud.
Platform	The environment in which the application is executed. It comprises of the complete infrastructure in the device, edge, cloud continuum to execute the application, including hardware, hypervisors, operating system, containers, cloud computing services and run-time libraries.
Process	A process is a logical sequence of tasks performed to achieve a particular objective. A process defines “what” is to be done, without specifying “how” each task is performed.
Reference Architecture	A Reference Architecture (RA) is an architectural design pattern that indicates how an abstract set of mechanisms and relationships realizes a predetermined set of requirements. It captures the essence of the architecture of a collection of systems. The main purpose of a Reference Architecture is to provide guidance for the development of architectures.
Reference Model	A reference model is an abstract framework for understanding significant relationships among the entities of some environment. It enables the development of specific reference or concrete architectures using consistent standards or specifications supporting that environment. A reference model consists of a minimal set of unifying concepts, axioms and relationships within a particular problem domain, and is independent of specific standards, technologies, implementations, or other concrete details. A reference model may be used as a basis for education and explaining standards to non- specialists.
Root of Trust	A critical component of public key infrastructures (PKIs) to generate and protect root and certificate authority keys; code signing to ensure software remains secure, unaltered and authentic; and creating digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments.
Safety-critical system	A system whose failure or malfunction may result in one (or more) of the following outcomes: death or serious injury to people, loss or severe damage to equipment/property, environmental harm.
Service	Services are the mechanism by which needs, and capabilities are brought together.
Solution	A means of solving a problem or dealing with a difficult situation.
System	A combination of interacting elements organized to achieve one or more stated purposes.
System Component	A system architectural element.
Task	a usually assigned piece of work often to be finished within a certain time.
Technique	Technical and managerial procedure that aids in the evaluation and improvement of the [system] development process.

Table 1: Terms, Abbreviations and Definitions

2 Introduction

This report is a result of the TRANSACT project, in specific a result of TRANSACT Task 3.2 from WP3.

The overarching goal of TRANSACT is to develop a universally applicable distributed solution architecture concept, framework, and a transition methodology for the transformation of standalone safety-critical CPS into distributed safety-critical CPS solutions. WP3 has as main purpose to ensure that distributed safety-critical CPS solutions have the necessary means for their operation to be always safety, performance, security, and privacy preserving, yet also profiting from edge and cloud enabled services. To this end WP3 defines the requirements and develops the concepts and solutions that fit with the TRANSACT reference architecture, such as the components for 'Safety, Performance and Security Monitoring Services', 'Access, Privacy & Identify Services' and 'Operational Mode Coordinator' of the TRANSACT reference architecture.

This report includes the necessary concepts for preserving security and privacy in edge/cloud computing environments and when deploying and running distributed applications for safety-critical CPS. Consideration is given to adopting a secure-by-design principle that will also support the inherent dynamic and heterogeneous nature of safety-critical distributed CPS. This includes the considerations of inter-relation with safety and performance (T3.1), with the challenges of management and upgrading of devices connected to edge and cloud infrastructure, including Over-The-Air (OTA) updates. The report investigates both the human and machine sides of cyber security, aiming for an orchestrated concept that enforces security throughout the device-edge-cloud continuum.

Specific research items are:

- Security and privacy requirements for distributed application with identification of security and privacy risks and threats, as well as the regulatory aspects.
- End-to-end security and privacy concepts for distributed safety-critical edge/cloud applications considering, security and privacy protection, intrusion detection, and attestation.
- Applicability of state-of-the-art methods from related projects (e.g., Secredas, CyberSec4Europe) for e.g., securing communication in distributed architectures, security by contract for CPS.
- Specification of the trust assumptions that are inherent to environments comprising heterogeneous CPSs, running mixed-criticality applications, and are necessary towards defining and modelling the trusted activities between them and with the back-end infrastructure that have to be supported by the provided attestation enablers.
- The impact and relation of security concepts on safety and performance, including security attacks impacting safety (T3.1).

2.1 Role of the deliverable

This document has the following major purposes:

- Documentation of selected concepts for end-to-end security and privacy, applicable across the TRANSACT domains.
- Report on requirements and state-of-the-art concepts for end-to-end security and privacy for distributed safety-critical CPS.
- Selection of existing concepts and definition of novel concepts to security and privacy consistent with the TRANSACT reference architecture.

The results in this deliverable are closely aligned and harmonised with the 'sister' deliverable D3.1 targeting Requirements and concepts for end-to-end safety and performance assurance for distributed CPS solutions and ensured to be fitting with the TRANSACT reference architectures as described in Deliverable D2.1.

The results will be applied to and demonstrated in 5 Use Cases (**UC**) covering three of the ECSEL-MASP 2020 Key Application Areas, namely "Transport and Smart Mobility", "Health and Well-being" and "Digital Industry". Fleets of remote controlled, (semi-)autonomous vehicles in urban areas (**UC1**) could help to drastically reduce road fatalities and road accidents, as well as contribute to a more efficient urban mobility with less congestion. Combined with increased electrification of our European car park (**UC3**), it would be an important aspect in the fight against air pollution, which still kills 7 million people annually according to WHO. In the shipping industry, cloud-enabled shore-based bridges (**UC2**) will mean a breakthrough in reducing groundings and other incidents, as well as in increasing performance and reducing fuel cost and GHS-emissions. In the healthcare sector it will lead to better clinical outcomes at lower cost, increased medical staff's experience and new business models based on 3rd party tool integration (**UC4**). Ultimately, connected wastewater treatment plants (**UC5**) will be key to mitigate climate change induced water scarcity while preventing ecological disasters due to potential wastewater spills. Transforming the safety critical local CPS into distributed solutions based on the functionality (applications and services) deployed over the device-edge-cloud continuum is crucial to meet all those needs.

2.2 Relationship to other TRANSACT documents

This document relates to the following TRANSACT deliverables:

- D5 (D1.1) Use case descriptions, end user requirements, SotA and KPI's(M10)

  The selected concepts for end-to-end security and privacy for distributed safety-critical CPS are aligned with the needs of the use cases as documented in D1.1 and will be applied in the context of those use cases. This deliverable includes a brief overview of the TRANSACT use cases and security requirements.

- D6(D1.2) Technical requirements and TRANSACT transition methodology commonalities (M12)

  The selected concepts for end-to-end security and privacy for distributed safety-critical CPS are aligned with the technical requirements as documented in D1.2. This deliverable includes a short overview of needs and expectations per concept category to summarize D1.2.

- D7(D2.1) Reference architectures for SCDCPS v1 (M12)

  The selected concepts for end-to-end security and privacy for distributed safety-critical CPS are aligned, and ensured to be consistent, with the TRANSACT reference architecture as documented in D2.1. This deliverable includes a brief overview of this reference architecture for understanding.

- D3.1, Selection of concepts for end-to-end safety and performance for distributed CPS solutions.

  The selected concepts for end-to-end security and privacy for distributed safety-critical CPS are harmonised with the complementary concepts end-to-end safety and performance for distributed CPS solutions as documented in D3.1.

- D3.4, Solutions for end-to-end security and privacy

  The developed solutions to preserve end-to-end security and privacy in edge/cloud computing when deploying running distributed applications for safety-critical applications, consistent with the TRANSACT reference architecture and based on the concepts defined in this document.

2.3 Structure of this deliverable

The structure of this deliverable is as follows. Firstly, in the next section (Section 3), a brief overview of the TRANSACT project use cases is given, focusing on each use case's security and privacy challenges to provide context to the selected concept descriptions and associated examples for application in the context of these use cases. Also, in this section included is a brief capture of the TRANSACT harmonised technical and security requirements and a brief overview of the TRANSACT reference architecture. Section 4 then provides an 'abstract view' on the classification categories of the concepts, i.e. four categories and sixteen selected concept classes, divided up across these categories.

This overview sets the scene for the actual description of selected concepts. In Sections 5, relevant regulations and standards are discussed. Sections 6 and 7 focused on security & privacy concepts for Transact Core Services & value-added services, respectively. Section 8 covers the concepts for domain-specific functions, and Section 9 covers application-specific security and privacy concepts. Finally, a summary is presented in this investigation for a selection of concepts for security and privacy for systems in the device-edge-cloud continuum.

3 TRANSACT reference architecture, use cases, and technical security requirements

3.1 The TRANSACT reference architecture

The TRANSACT project has adopted a tree-tier, device-edge-cloud, architecture concept. Based on this concept, the project has proposed a first reference architecture in deliverable D2.1 (see Figure 1). In the deliverable D2.1 a full description is given of the TRANSACT reference architecture; here a summary is included for positioning the selected end-to-end security and privacy concepts in this reference architecture.

The domain specific functions or components are depicted in red, yellow, and green depending on their criticality. Domain specific functions may be offloaded from the device to other tiers. Core TRANSACT components, available to every use case, are depicted in grey. Finally, blue components refer to potential Value-Added functions that may be included depending on the use case.

The TRANSACT reference architecture defines the safety and mission critical functions, the core services and functions, and further value-added services and functions (see Figure 1).

The safety and mission critical functions are key in the safety-critical CPS. The distributed safety-critical CPS solutions will be deployed over 3-tier (device-edge-cloud) architecture continuum. Each tier in the architecture provides a specific quality of service level especially with respect to performance aspect such as response times and data transfer guarantees, ranging from best effort to reliable and time-deterministic data transfers. Safety critical functions often have hard real-time related constraints, whereas the mission critical functions may have soft real time constraints (which may degrade the system's quality of service when missed, but do not necessarily lead to failures). In the cloud also Big Data as a Service (BDaaS) services may be deployed.

TRANSACT aims at improving over monolithic CPS by offloading functions to the edge or cloud tier. A few use cases will offload safety-critical functions to the edge tier, more use cases will offload mission-critical functions to edge and cloud. Such offloading gives numerous advantages such as: improved reliability and performance of the device (as fewer services are running on the device), improved efficiency of the offloaded functions due to usage of better hardware in the edge or cloud, improved innovation speed of the distributed CPS as the new or upgraded functions can be deployed easier in the edge and cloud.

However, when considering offloading functions from the device it is critical to ensure CPS system end-to-end safety, performance, security, and privacy. Therefore, several dedicated core services are introduced to cooperatively realize that objective. The safety, performance and security monitoring services are responsible for monitoring, detecting, and preventing safety, security, and performance failures. In addition, they track the devices' KPIs (such as, latency, throughput, accuracy, availability) that are used by the operational mode manager (running on the device) and the operational mode coordinator (running at the edge/cloud tier) to decide at runtime whether a device's function can be executed remotely or not.

To achieve safe and predictable updates to the system the following core services have been identified: the remote update client (running on the device) and the update coordinator (running at the edge/cloud). Those services cooperate across tiers to perform remote automatic updates of the different device services in a secure and safe way. Each update activity is coordinated with the operational mode coordinator service to keep the system in the safe state at any time.

Further core services address additional security and privacy concerns. The identity & access services are responsible for granting/denying access to the system resources based on the policies defining who has what access (in which role) to which resources. Another core services contributing to the system security are the auditing services. These services collect information about accessing and using the system to help detecting

the security policy violations when system is accessed by unauthorized users or in an unauthorized way. The security aspects are also addressed by the (federated) data services and comms services helping in efficient and secured data handling, both, in transit and at rest

In this project, each use case will experiment with the TRANSACT reference architecture, its components, and the selected concepts presented in this deliverable with the aim to capture the overarching results across the various use cases. This allows TRANSACT to validate the approach and refine the proposed reference architecture over the course of the project. The domain specific functions or components are depicted in red, yellow and green depending on their criticality. Domain specific functions may be offloaded from the device to other tiers. Core TRANSACT components, available to every use case, are depicted in grey. Finally, blue components refer to potential Value-Added functions that may be included depending on the use case.

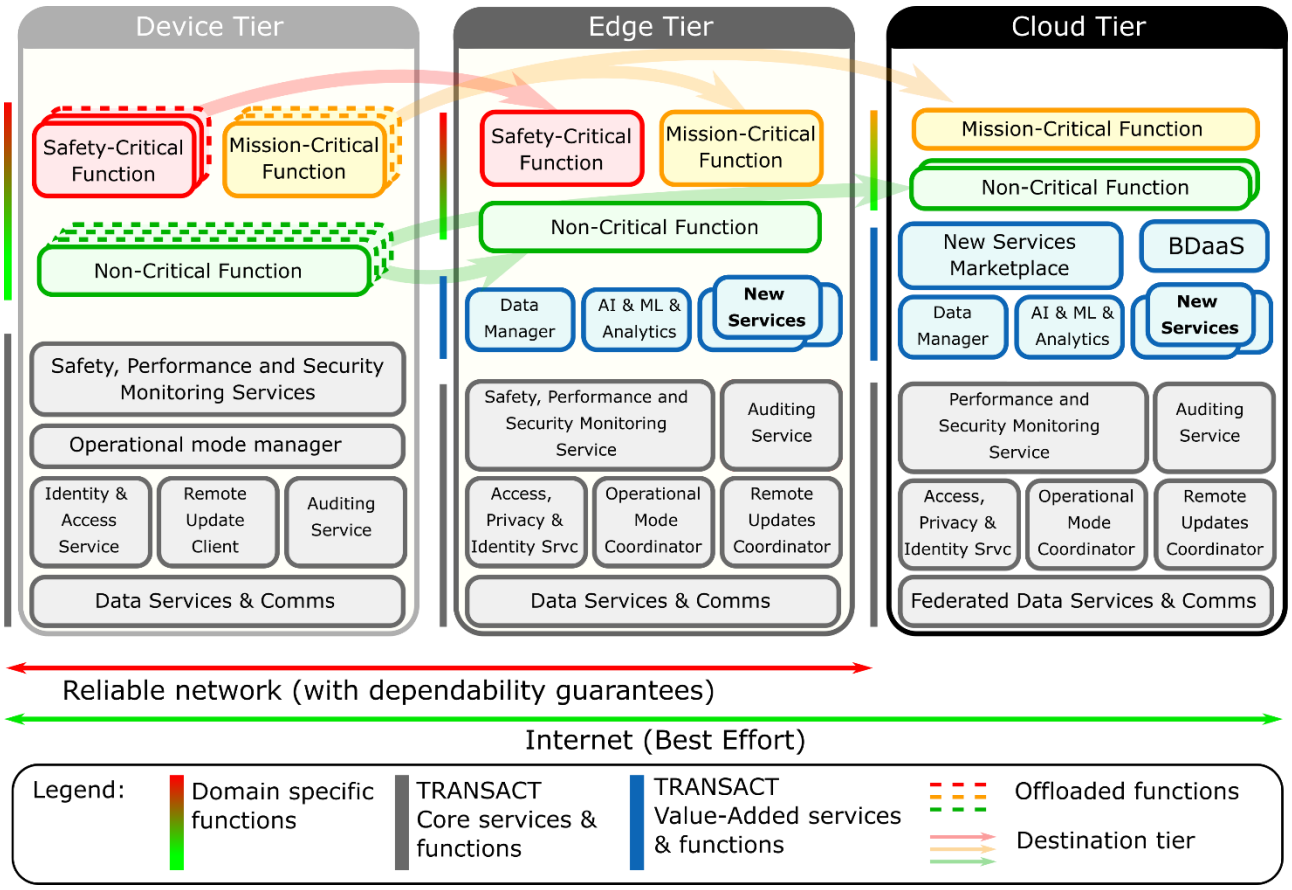

Figure 1: TRANSACT reference architecture.

The TRANSACT reference architecture defines: the safety- and mission-critical functions, the core services and functions, and the value-added services and functions.

The safety- and mission-critical functions are key in the safety-critical CPS. TRANSACT aims at improving the CPS solution by: first, stripping the device of the functions that are not safety or mission-critical and can be executed remotely; and second, by offloading certain safety-critical functions to the edge tier. The functions to be offloaded are identified at the design time and deployed in the required tiers, as a result the device would only keep the basic and safety-critical functions while offloading the remaining functions to the other tiers. Such an approach gives numerous advantages such as: improved reliability and performance of the

device (as fewer services are running on the device), improved efficiency of the offloaded functions due to usage of better hardware at the edge or cloud, improved innovation speed of the distributed CPS as the new or upgraded functions can be deployed easier at the edge and cloud.

However, when considering the functions offloading from the device it is critical to ensure CPS system end-to-end safety and security, therefore, a number of dedicated core services are introduced to cooperatively realize that objective. The safety, performance and security monitoring services are responsible for monitoring, detecting and preventing safety, security and performance failures. In addition, they track the devices' KPIs (such as, latency, throughput, accuracy, availability) that are used by the operational mode manager (running on the device) and the operational mode coordinator (running at the edge/cloud tier) to decide at runtime if a device's function can be executed remotely. Thus, the offload of the function is associated with the operational thresholds or ranges of KPIs, which means that if a KPI is compromised or out of range, the operational mode manager takes control to switch back the function to a local on-device execution, ensuring system safety and performance.

Another area that the TRANSACT reference architecture addresses is updating the system. To achieve safe and predictable system updates the following core services have been identified: the remote update client (running on the device) and the update coordinator (running at the edge/cloud). Those services cooperate across tiers to perform remote automatic updates of the different device services in a secure and safe way. The updates ensure uniform software versions on the tiers and keeps the system services up-to-date with the latest functionality. In addition, the automatic updates allow rolling-out a new functionality or introduce new value-added services minimizing system downtime. Each update activity is coordinated with the operational mode coordinator service to keep the system in the safe state at any time.

The secure access to the system functionality is managed by the identity and access services. These services are responsible for granting/denying access to the system resources based on the policies defining who has what access (in which role) to which resources. Another core services contributing to the system security are the auditing services. These services collect information about accessing and using the system in order to help detecting the security policy violations when system is accessed by unauthorized users or in an unauthorized way. The security aspects are also addressed by the (federated) data services and comms services helping in efficient and secured data handling, both, in transit and at rest.

The TRANSACT reference architecture also defines the value-added services that enhance the system capabilities. Those functions can be introduced at the system design or after system release (as part of the system updates).The examples of added-value services could be data analytics services or dedicated AI&ML services giving insights in the collected data by extracting valuable information that helps improving the user activities (for example, in the healthcare domain those services can enhance the health specific algorithms assisting doctors in the diseases diagnostics and supporting them in making the clinical decisions; in automotive domain those services can enhance the routes predictability or leverage the risk analysis to assist in better automatic and human driver decisions). Next to the user tasks improvements, such services can help in optimizing the organizations operational performance and costs (for example by better equipment utilization in the healthcare or transportation domains). The new added-value services can be also available via the new applications and services marketplace service. Such a marketplace service opens possibilities to provide new solutions (applications, services, algorithms, AI models, etc.) not only by the system builder but also by the 3rd party vendors.

To realize all the above TRANSACT results, project developments will be driven by industrial use cases.

3.2 Overview of Use cases

3.2.1 Use Case 1–Remote Operations of Autonomous Vehicles for Navigating in Urban Context

In this use case, Fleetonomy and partners will develop a solution for remote control of (semi-) automated vehicles for navigating in urban environments (see Figure 2). The solution will allow vehicles to be moved from one location to another even without a driver, but with a remote operator. The operator will receive continuous feedback on vehicle state and environment, allowing him/her to assist the vehicle to navigate through urban traffic. The vehicle will have autonomy provided by current state-of-the-art automated driving solutions taking care of normal driving, and capable of detecting and reacting to arising hazardous situations.

During the TRANSACT project, the use case team will enhance the capability of the vehicle to understand its surroundings, react to pedestrian and other road user behaviours and make local decisions. The interaction and cooperation of vehicles and human operators in remote operating centre will be seamless and enhanced through visualisation and communication of the vehicle understanding and intent in augmented reality camera view and user interfaces with 3D data model of the driving environment. This allows the remote operator to understand the vehicle's independent capability to manage safe driving in a complex environment including people in different roles. The remote operator provides supervision and additional safety as well as the intelligence to resolve arising exceptional traffic situations. Hand-over of control between operator and vehicle is performed in smart way.

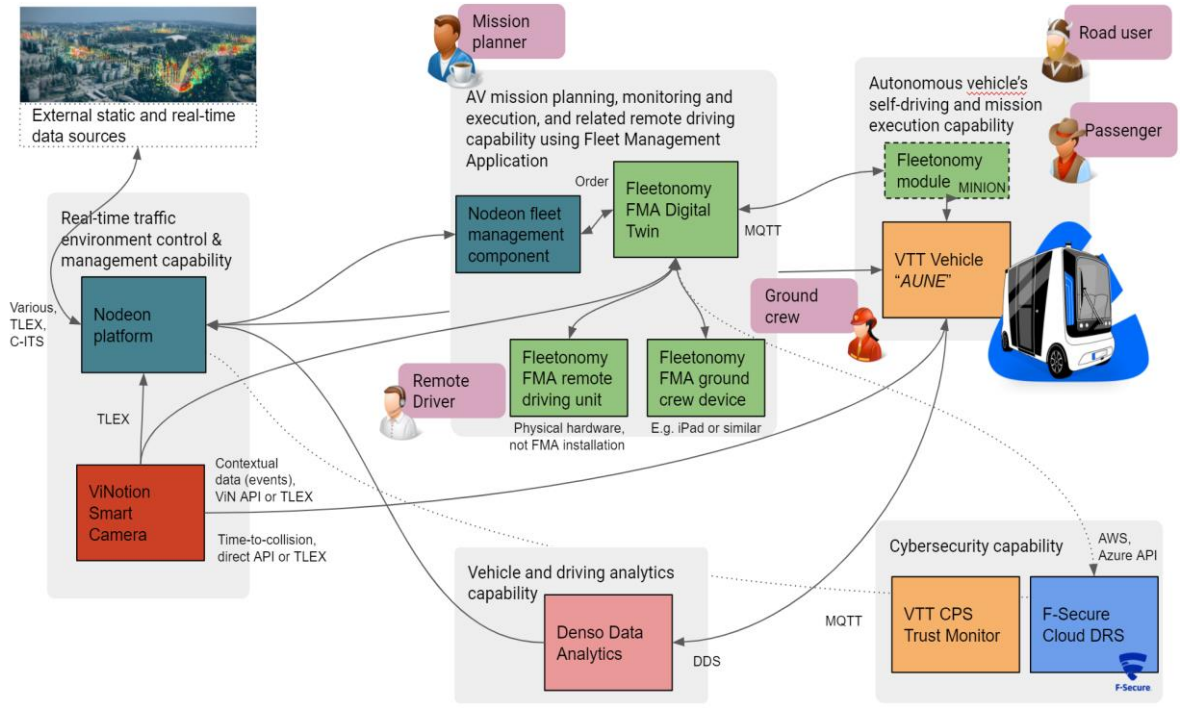

Figure 2: The remote operations use case cloud-edge-device continuum

TRANSACT security challenges: The architecture should be able to negotiate the Confidence Level with Vehicle automatically. Communication channel between data exchange hub and end user must be secure and safe, end-to end protected.

3.2.2 Use Case 2 - Critical Maritime Decision Support Enhanced by Distributed, AI Enhanced Edge and Cloud Solution

The maritime use case (UC2) will demonstrate advancements in safe and efficient maritime navigation made possible by enhancing the existing basic edge/cloud technologies in the NAVTOR e-Navigation Suite to the TRANSACT architecture. This will allow for integration of traditional advisory services, AI-based advisory services, and data-analytics services into the device-edge-cloud continuum to improve safety, efficiency, and security, as will be demonstrated for automated High Sea vessels and an autonomous harbour-based support vessel. In the Figure 3, NAVTOR's pre-TRANSACT e-Navigation suite is illustrated. In the following Figure 4 the planned device-edge-cloud services are detailed, building a holistic AI-based monitoring and decision support service for safe and efficient navigation.

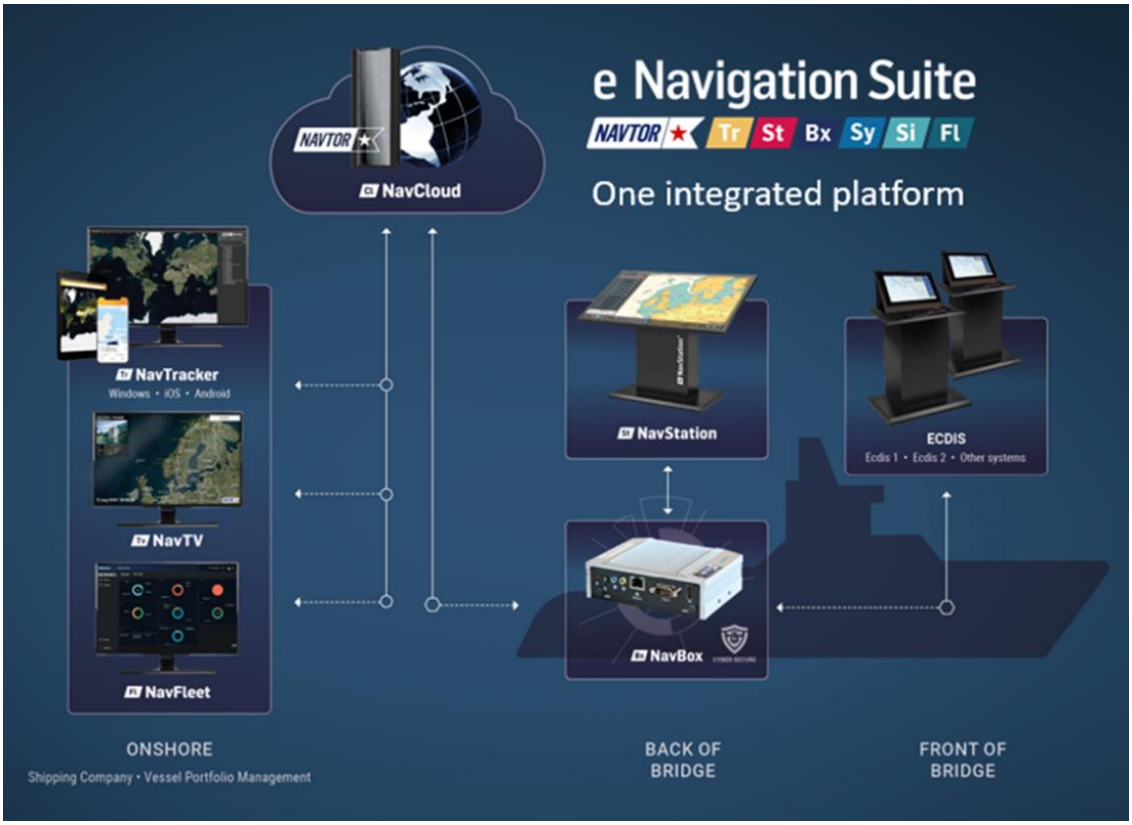

Figure 3: NAVTOR's pre-TRANSACT e-Navigation suite

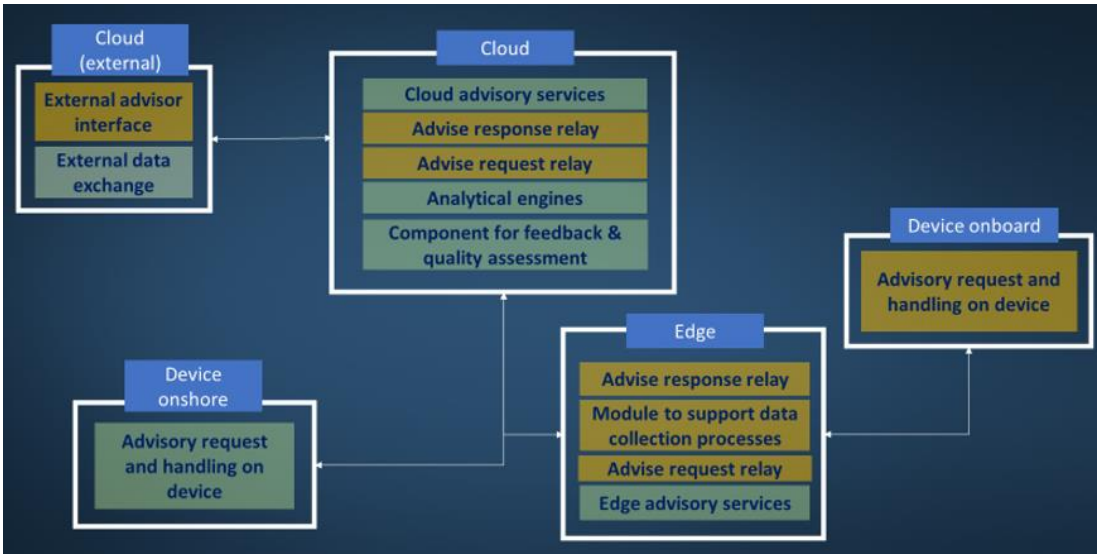

Figure 4: NAVTOR's e-Navigation suite build on TRANSACT architecture; yellow boxes are pre-TRANSACT, green boxes are by TRANSACT project, and will be demonstrated by UC-2.

TRANSACT Security challenges: The security challenges for the High Sea demonstrator are mainly related to the SatCom-connection between Vessel and Shore, in addition to the "connected Bridge" setting up a secure connection between Front of Bridge and Back of Bridge strictly when required. Normally the real time navigation system (ECDIS) is for security purposes a stand-alone system. In TRANSACT connection between vessel and shore is given, and security and performance issues must be handled by secure communication between cloud based advisory services and the vessel-based edge advisory services, utilizing decision data structure updated from the Cloud. The safety and security critical communication between the device (ECDIS Front of Bridge) and the edge (NavBox Back on Bridge), and new security structure including new APIs has to be developed to take advantage of the AI-based Cloud advisory services. Due to vessels' satcom related challenges, a distributed PKI system will be investigated.

In the demonstrator related to an unmanned surface vessel in port, near real time secure communication is a must, and security mitigation actions will be investigated to enhance the security level of the wireless communication.

List of main security related requirements includes: Distributed PKI (as vessel is off line at given times), remove data sharing by USB-sticks, encryption mechanisms on all messages, detection of false sensor or data injection, detection of spamming/jamming of signals.

3.2.3 Use case 3 - Cloud-featured battery management systems

Vehicle battery data is collected and transmitted using an advanced and secure data logger and transferred encrypted to a data broker cluster; the data is stored in an optimized database. All of this is happening while the Electric Vehicle Fleet (EVF) is driving. In the backend the data is analysed and used for the improvement of functionality (e.g. time left to charge), safety or autonomous driving (e.g. Fail-operation in Battery/BMS). Such improvements are sent back to the EVF, where the infrastructure is used in the opposite direction. The vehicles in the EVF are now consumers and consume the software update. All of this still happens in an encrypted way, ensuring the integrity of the software update. A further topic is the handling of the impact of low state-of-charge (Keyword "safe energy supply") on autonomous functionalities. Necessary updates or system decisions can be done over-the-air; safety-relevant warnings can be communicated to the driver. The generated data leads to a better estimation of battery remaining useful life (RUL), battery failure prediction and error management.

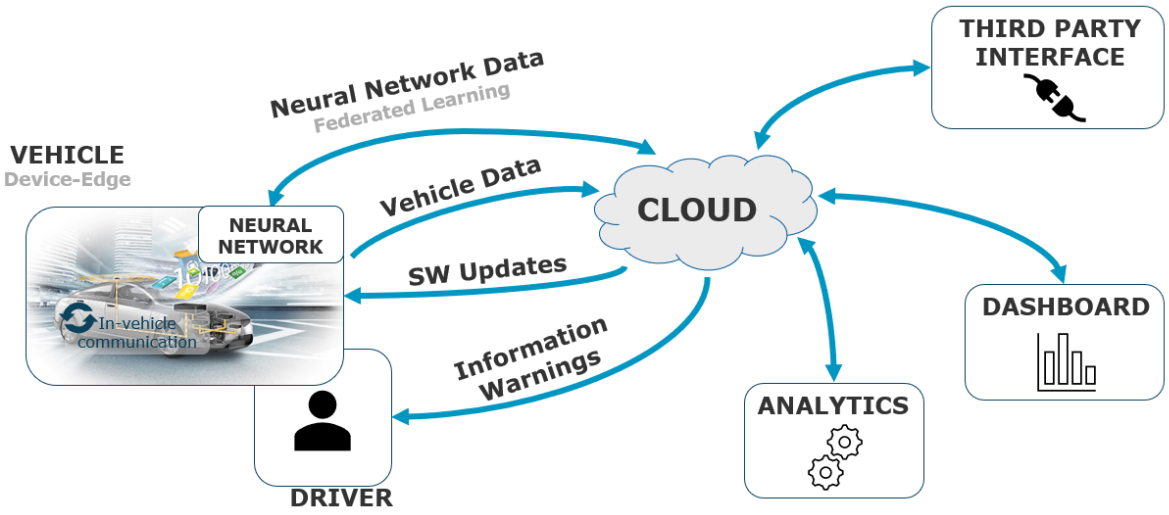

Figure 5: Involved components and communication paths of the cloud-featured battery managements use case.

TRANSACT security challenges: So far, the battery management system has been a closed system. The security is inherently guaranteed by the lack of possibilities to connect to the hardware. Dedicated hardware and special knowledge are required to access and change the software. Now, the system will be transformed into a distributed system which has a permanent accessible connection. With the increase of attack surface, the challenges arise.

Data are no longer processed locally but exchanged with the cloud backend. Beside of technical telemetric data, personal data are of interest as well. Beside of state-of-the-art encryption, further methods are investigated to establish a secure-by-design transmission channel. That means, data are pre-processed and abstracted before they are transmitted and stored.

Another challenge arises with the new possibility to perform software updates over the air. By design of the electrical-electronic architecture, the LTE gateway will have access to any control unit within the sub-system. It must be guaranteed, that only privileged person can access the gateway while, e.g. roles limit the control of the functions. Since changes to the software can be performed more easily, mechanisms must be established which confirm the integrity.

3.2.4 Use case 4 - Edge-cloud-based clinical applications platform for Image Guided Therapy and diagnostic imaging systems

Use Case 4 “Edge-cloud-based clinical applications platform for Image Guided Therapy and diagnostic imaging systems” is a healthcare use case, aiming to improve the workflow and interoperability in hospitals. In particular, the use case addresses image based minimally invasive clinical procedures which are typically performed in Cathlabs or Operating Rooms (see Figure 6).

In the currently deployed system, the security and privacy of data is guaranteed on a number of levels, i.e., by restricting access to the system in Cathlab (physical security), using the user access management to restrict system functionality and data access as needed per user roles, all sensitive data stored on the system is encrypted. Moreover, when healthcare data need to leave hospital environment it is anonymised to ensure data privacy.

Figure 6: Typical workflow setting during image guide therapy with physicians utilizing medical imaging equipment for the minimally invasive treatment of patients

TRANSACT security challenges: Changing the architecture of the healthcare diagnostic imaging systems from the centralized, on-device solution toward the distributed, cloud-based architecture significantly increases the attack surface of the new solution by making it more vulnerable for security threats. Also, the data privacy concerns are growing significantly in such architecture as the healthcare data is highly sensitive and require special care to not be exposed due to being transferred over a public network or due to security attacks and software vulnerabilities.

The new edge/cloud-based architecture of the healthcare diagnostic imaging systems should ensure that the risks of security breaches and privacy violations are minimized. Therefore, one of the biggest challenges in the healthcare systems is to ensure the end-to-end security and privacy, i.e., the system design and deployment need to apply the security mechanisms ensuring proper safeguards to comply with the regulatory requirements and preventing disclosure, compromise, or misuse the stored and processed healthcare data. The new edge-cloud-based components implementing security and privacy related functionality need to be designed with security and privacy in-depth approaches to ensure adequate quality and protection of the processed healthcare data.

Moreover, as the clinical procedures are typically very complex and involve a team of healthcare professionals (with a variety of expertise in multiple disciplines, who are located inside and outside the hospital) their effective collaboration is paramount to ensure the best treatment outcome for the patients. Therefore, ensuring the security and privacy of the shared healthcare data is critical to enable possibility for more efficient collaborations of healthcare specialists within and outside of the hospital's Cathlab.

3.2.5 Use Case 5 – Critical wastewater treatment decision support enhanced by distributed, AI enhanced edge and cloud solutions

Use case 5 "Critical wastewater treatment decision support enhanced by distributed, AI enhanced edge and cloud solutions" is an industrial use case, which attacks three problems: the detection upon industrial discharges, the need for better strategies for equipment maintenance and the need for a more efficient cross-WWTP operation.

Wastewater treatment plants (WWTP) aim cleaning sewage and water coming from citizen consumption, drainage and rainwater with propose of these wastewater streams can be returned safely to the environment. Sometimes, the environmental areas where the treated water is discharged are sensitive or protected areas and therefore, the correct water depuration has a strong impact in the environment, population welfare and agriculture in the surrounding zones. Therefore, disruptions and dysfunctions in the

management of the main processes related to the achievement of proper water quality may lead to high risks to the society, the environment and the local economies. The most extended kind of WWTPs involve physic-chemical treatment and biological treatment in different stages for removing solids and pollutants, breaking down organic matter and restoring the oxygen content of treated water (see Figure 7).

Unfortunately, those disruptions on the depuration processes usually happen, especially in industrial areas, where the WWTP are severely affected when the toxic spills reach the facilities, leading to an interruption in the operation of the critical biological reactors, avoiding an appropriate water depuration. Therefore, these toxic discharges have impact on environment and could seriously affect the protected natural area (fish kills). The re-establishment of each biological reactor may involve around 20k-25k euros, aside from the heavy penalties for the plant managers.

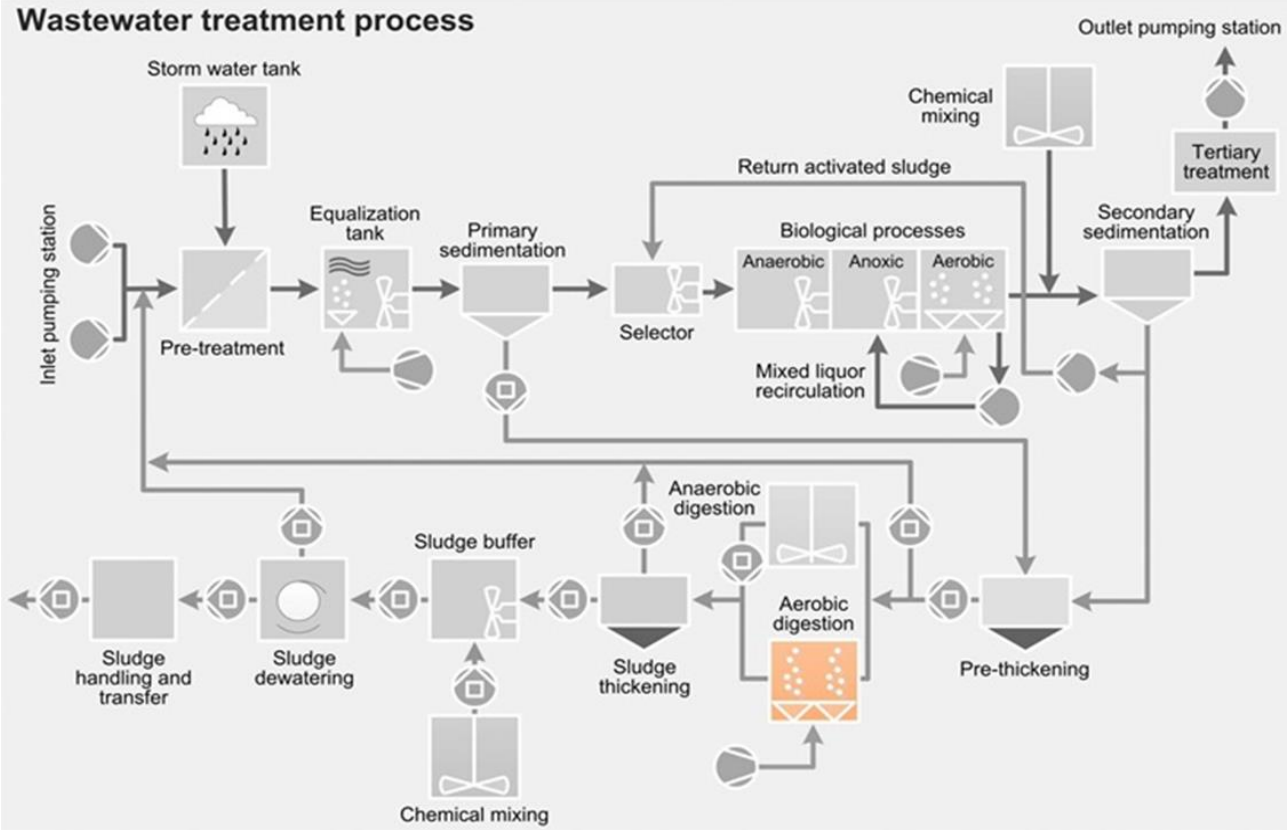

Figure 7: General scheme of a typical wastewater treatment plan process

TRANSACT security challenges: The security challenges in this use case are mainly related to the Authentication and Authorization Attacks. The system must implement an artificial intelligence algorithm capable of detecting anomalies in the usual behaviour of each machine. The system must identify rare elements, events, or observations of the parameters of the machine that arouse suspicion by significantly differing from the usual or daily behaviour. The system should be protected against most attacks on edge computing infrastructures and cloud services.

4 Overview of selected concepts classification for security and privacy

In the course of the investigation in task 3.2, an overall structure was created to organise the selected concepts and maintain an overview. This section presents a brief overview of this structure with four major classification categories.

- Security & Privacy Concepts for Transact Core Services & Functions
- Security & Privacy Concepts for Transact Value-added Services & Functions
- Security & Privacy Concepts for Domain-Specific Functions
- Application-Specific Security and Privacy Concepts

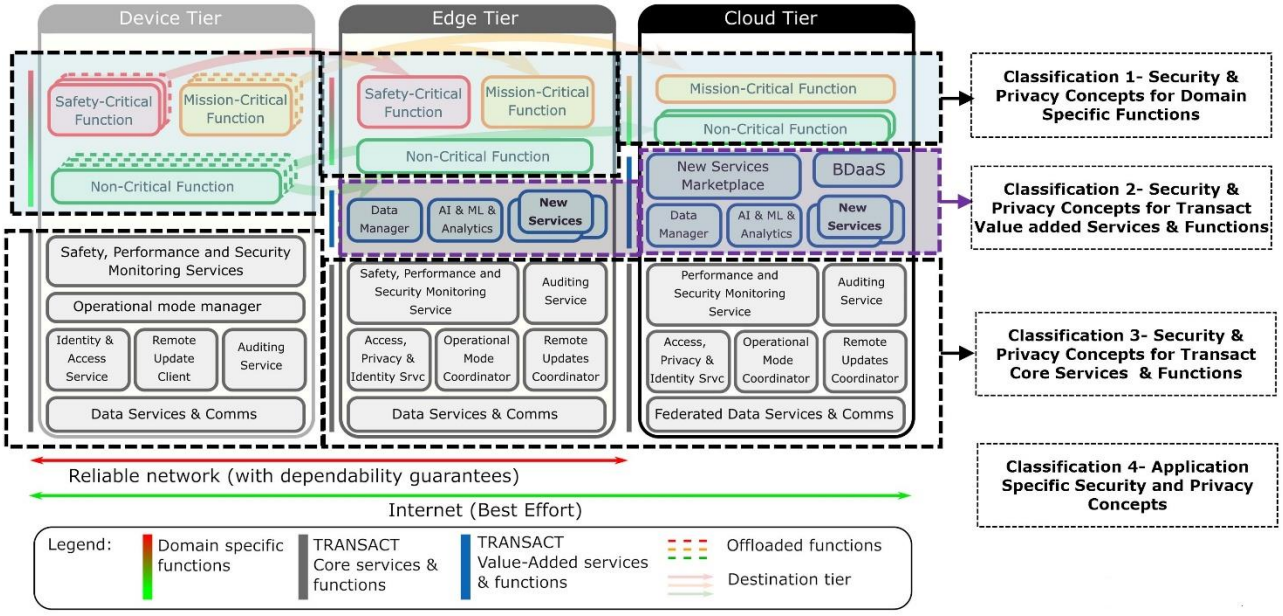

Figure 8: Selected classification categories for security and privacy concepts.

Several concept classes have been identified for each of these four categories. Within each concept class, then the selected concepts and methods are described. A concept class then may contain a small number of related concepts as needed to cater to the needs of the use various use cases and their domain characteristics.

5 Relevant regulations and standards

This section provides an overview of some relevant security and privacy related standards and regulations, with the aim of providing some background when defining concepts for end-to-end security and privacy for distributed cyber-physical systems.

The focus will be on the ISO/IEC 27000 family of standards and on the GPDR regulation. Both of them are related to data confidentiality, integrity and availability, but there are important differences. The GDPR (EU, 2016) focuses on data privacy and the protection of personal information, but it lacks details on how to maintain an appropriate level of data security. Such details are provided by the ISO 27000 standards, in which a framework and best practice recommendations regarding information security management are described.

The standards and regulations that are relevant might of course depend on the specific use case. For example, protection of personal information and data privacy are crucial in the medical use case and there are additional region-specific regulations that need to be considered (e.g. HIPAA (HIPPA) for the US), while these aspects are likely of lower important in other use cases such as the maritime use case.

5.1 ISO/IEC 27000 family

The ISO/IEC 27000 series is a well-known family of standards published by the International Organization for Standardization and the International Electrotechnical Commission. A central concept is the use of an Information Security Management System (ISMS), which is introduced in ISO/IEC 27000 and further specified in ISO 27001. This ISMS shows many similarities to other systems, such as the Quality Management System (QMS) described in the ISO 9000 series. The ISMS is a centrally managed framework consisting of policies and procedures to manage information systematically in a secure way using a risk-based approach. It covers processes, people, and IT systems.

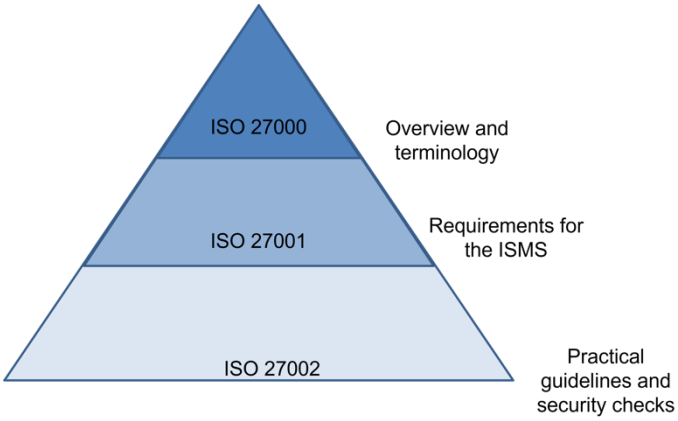

Figure 9: Schematic overview of three important standards within the ISO/IEC 27000 family.

A core principle of the ISMS is the Plan-Do-Check-Act (PDCA) cycle or model, and this is also applied in other ISO standards such as the 9000 series (see Figure 10)

1 **Plan** means to establish ISMS policies, objectives, processes, and procedures relevant to managing risk and improving information security.
2 **Do** refers to Implementing and operate the security policies and procedures.
3 **Check** is about monitoring (and measuring where possible) the effectiveness of ISMS policies and controls. This can for example be done through certain KPIs or by auditing certain processes.

4 **Act** means to take (corrective and preventive) actions, based on the results of the internal ISMS audit and management review or other relevant information, with the aim of achieving continuous improvement of the ISMS.

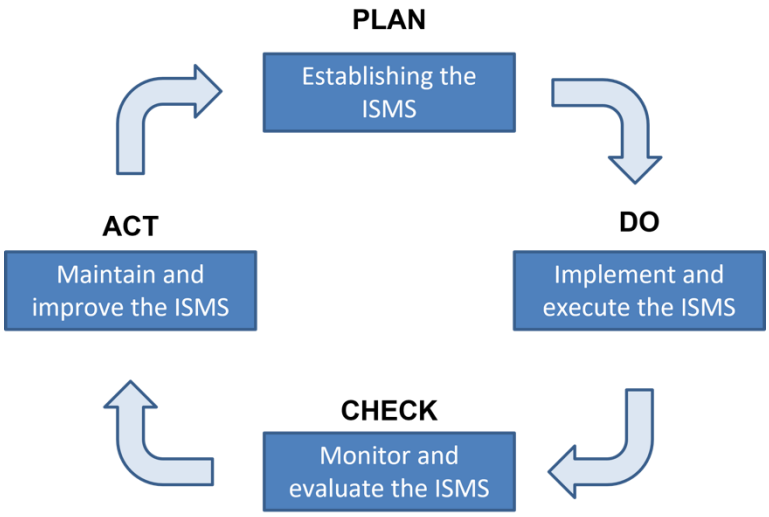

Figure 10: Overview of the typical plan-do-check-act cycle that is part of an Information Security Management System (ISO 27001).

The ISO 27002 framework provides best-practice guidance on applying the controls listed in Annex A of ISO 27001. When determining which security controls should be selected and implemented, a risk-based approach should be followed. The ISO 27002 groups the possible controls into 14 control sets (e.g. access management, cryptography, incident managements, business continuity).

5.2 GPDR

The General Data Protection Regulation (GDPR) is a European Union (EU) law that came into effect on 25th May 2018. GDPR governs the way in which we can use, process, and store personal data (I.e. information about an identifiable person), and gives individuals more control over their personal information. It applies to all organisations within the EU, as well as those supplying goods or services to the EU or monitoring EU citizens.

The GDPR specifies 7 core principles that should be taken into account when dealing with personal data:

- **Lawfulness, fairness and transparency:** Organizations should have a valid legal basis for processing personal data. Examples for such legal bases are when individuals have given consent, or when the activity is required for fulfilling a legal obligation (e.g. employment). Fairness relates to the fact of not mis-using the data you collect, while transparency refers to being clear with data subjects about who you are, and why and how their personal data is being processed.
- **Purpose limitation:** This means data is “collected for specified, explicit, and legitimate purposes”. The purpose must be clearly communicated, and the processing of the data should be limited to this purpose.
- **Data minimisation:** This refers to the fact that only the smallest amount of data should be collected that is really needed.

- **Accuracy:** The stored data should be accurate, and inaccurate data should be corrected or erased without delay.
- **Storage limitation:** Data should only be kept for the period that is really needed.
- **Integrity and confidentiality (security):** Technical and organizational measures should be taken to protect unauthorized or unlawful processing and against accidental loss.
- **Accountability:** Organization must keep records in place as proof of their compliance with the data processing principles. This audit trail is required to prove compliance when needed.

Finally, there are a few other GPDR related terms that are relevant to mention:

- **DPO (Data Protection Officer):** DPOs are independent data protection experts who are responsible for monitoring an organisation's compliance and advising on its data protection obligations. The DPO also acts as a contact point for data subjects and the relevant supervisory authority.
- **DPIA (Data Protection Impact Assessment):** Under the GDPR, DPIAs are mandatory for any new high risk processing activities. They can be used to identify and mitigate against any data protection related risks

6 Security & privacy concepts for Transact core services & functions

6.1 Concept for Risk Analysis and Management

6.1.1 Overview

To carry out a complete risk analysis it is necessary to evaluate potential threats and how they would affect the following five dimensions, as those are considered the features or attributes that make an asset valuable, nonetheless, risks may be analysed by focusing on a single facet, regardless of what happens with other aspects:

Availability: Have access to assets when they may be needed [UNE 71504:2008].

Integrity: Assets must have not been modified [ISO/IEC 13335-1:2004].

Confidentiality/ Non-disclosure: Asset's information should not be available to unauthorisedly parties [UNE-ISO/IEC 27001:2007].

Authenticity: An entity or asset is what they claim to be [UNE 71504:2008].

Accountability: The activity of the entity or asset can be monitored [UNE 71504:2008].

To develop a High-Profile analysis, MAGERIT methodology can be used, which is a standard that establishes principles for the effective, efficient, and acceptable use of IT. It has been prepared by the CSAE (Spanish Higher Council of E-Government) and published by the Ministry of Finance and Public Administrations (HIGHER COUNCIL FOR ELECTRONIC GOVERNMENT). This methodology is well known and recommended in Europe by ENISA (the European Union Agency for Cybersecurity). Thus far, ENISA also accept other Risk Management developed by Members states of the European Union, as in Spain. Over the years, MAGERIT has been developed and improved. It was firstly elaborated in 1997 and CSAE has been working on its development and updating continuously, taking into account, not only a practical experience, but also ISO standards. (MAGERIT, 2005)[1]

The MAGERIT methodology (Methodology of Analysis and Management of Risks of Information Systems) has as objective to help organisations balance risks and encouraging opportunities arising from the use of IT. Risk analysis allows to know the information systems: their assets, their value, and the threats to which they are exposed, moreover, it provides a balanced framework for Governance, Risk Management and Compliance, to prevent conflicts and threats.

The Figure 11 shows graphically the steps in the MAGERIT methodology. The system to be assessed is modelled by identifying the assets that form part of the system. Assets are exposed to several threats and vulnerabilities. When an incident occurs, it may depreciate the asset(s) affected by it, causing a certain impact. Despite the unfortunate event, if we figure out the probability of materialising the threat, we could conclude the risk in the system or the loss to which it is exposed. On the other hand, depreciation and probability qualify the vulnerability of the system to a threat.

Once the most critical risks are known, the entity can deploy safeguards or controls to deal with threats. Safeguards mitigate the impact and risk values to residual values. Residual values mean the risk and impact

[1] Magerit — ENISA (europa.eu)

that remains after putting effort to identify and eliminate or mitigate some or all types of risks previously identified.

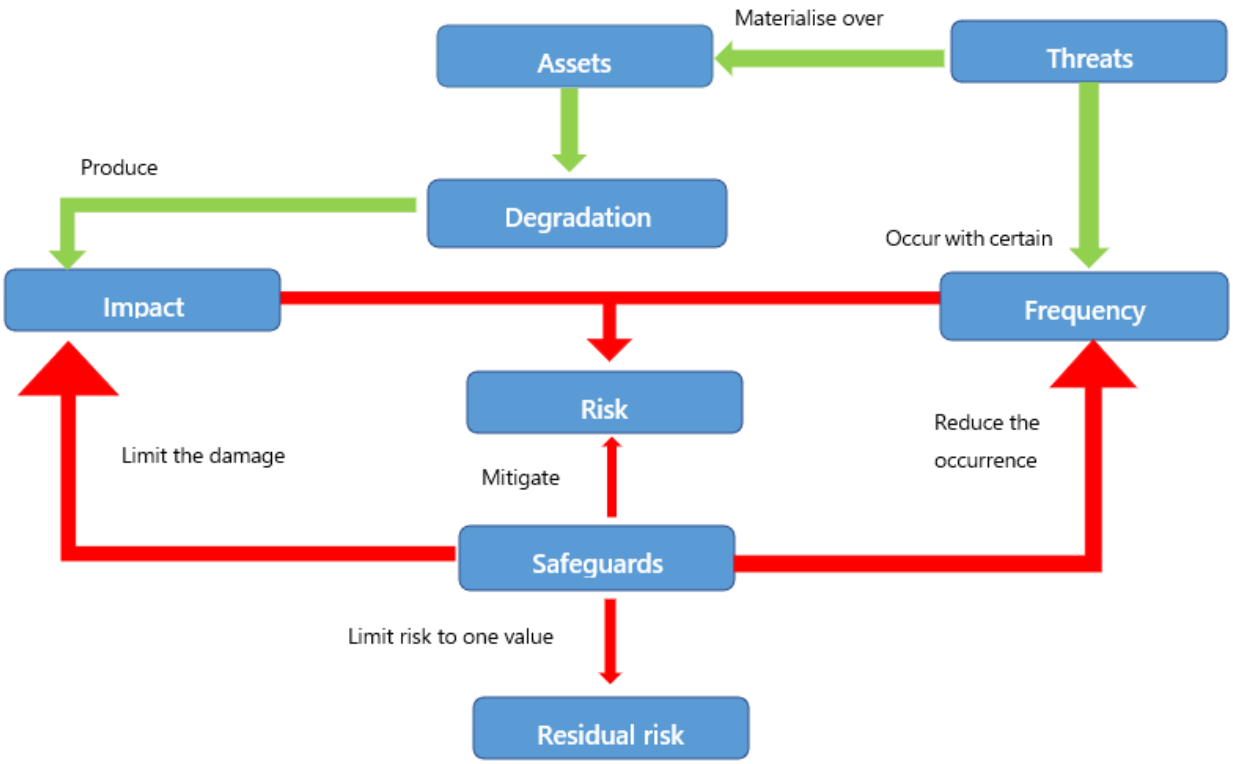

Figure 11: The MAGERIT methodology.

The following Figure 12 summarises the process of risk analysis following the MAGERIT methodology.

Figure 12: Process of risk analysis.

6.1.2 Fit with concept TRANSACT reference architecture/components

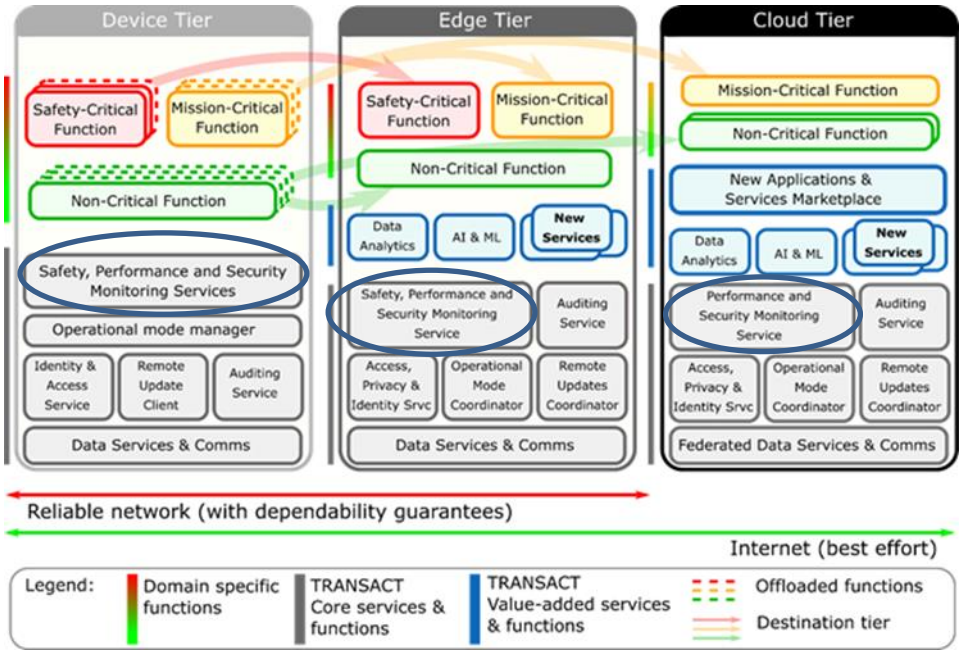

Figure 13: Scope of Risk Analysis in the TRANSACT reference architecture.

In Figure 13, arrows highlight the line of reasoning about safety is recursive across all the tiers involved in the provided solution. So, in here it is shown how Privacy and Security is a core service in Transact architecture. The blue ellipses show the components on three tiers of the Transact reference architecture that are responsible for performance management.

For carrying out the risk analysis itself, besides MAGERIT standard, the platform GConsulting can be used. This tool is based on the international standard on how to manage information security ISO/IEC 27001. In addition, to a wider perspective, this is not the only reference that will be use. In fact, to succeed in a complete risk analysis, both, MAGERIT and GConsulting integrate the Spanish Royal Decree 3/2010, 8th January, of regulation of the National Security Framework, which performs on establishing the policy of security in the use of electronic means, setting the principles and requirements that adequately ensured information security treatment.

Although MAGERIT is specialised in Information and Communication Technologies, it also covers Safety, Performance, Security, and Privacy.

6.1.3 Example in context of a Use case

The need to implement a risk analysis can be illustrated by the use case scenario *"*Transformation of the monolithic critical system in wastewater treatment plants to the distributed system supported in the cloud: management of the biological reactor*"* of UC5. This scenario is concerned with controlling the process and improving water quality. As risk analysis allows to know which work elements are subject, a wastewater treatment plants analysis will enhance the analysis and obtention of insights by the operator and lead to newer more advanced applications (predictive maintenance) that will result in a reduction of downtime, costs, and better service; due a risk management process facilitate governing bodies to make decisions considering the risks derived from the use of IT and AI.

Risk analysis has an important role in this use case. The Safety, Performance, and Security Monitoring Services can identify the potential threats involved (*e.g.,* a spill or a natural disaster) so an unfortunate event can be avoided, or, at least, the potential damages may be diminished.

6.1.4 Challenge for application within TRANSACT context

Risk management in TRANSACT requires a thorough study and adaptation for five different applications of a distributed CPS. Furthermore, due to the specialities of a distributed CPS, it is crucial to have a profound knowledge of the combination of physic and computer elements, so for that purpose it is necessary a collaboration with the partners.

6.2 Role-based access control rules at the business/design level

6.2.1 Overview

To maintain confidentiality, integrity, and availability of any information system, it is necessary to implement security rules or policies that restrict the behaviour of all system users. Access control policies can be implemented as an effective cybersecurity strategy to prevent situations that put data and system performance at risk. An access control policy (see Figure 14) involves three main concepts (Salvador Martínez, 2018) (Antonia M. Reina Quintero, 2022): the Object represents the resource that we want to protect; the Subject represents the actors for which access to the Object is controlled; and Action represents the operation that the Subject could perform on the Object in the system. The relationship between Action(s) and Object(s) represent a Permission, which can be assigned to a Subject.

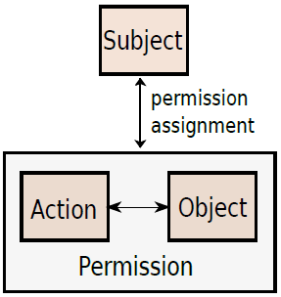

Figure 14: Access control (Salvador Martínez, 2018).

Role-based access control (RBAC) is an access control strategy that restricts users based on roles and privileges. RBAC enables the assignment of permissions by grouping users into a set of roles that are ordered by hierarchy. In the TRANSACT architecture, our plan is to address RBAC at the business/design level to restrict access and manipulation of system components and resources. However, the specification of RBAC policies can become a complex task involving hundreds of ***Subjects*** (and roles), ***Actions***, ***Objects***, and ***Permissions*** for distributed safety-critical CPS solutions. A strategy to address the specification or modelling of RBAC policies for distributed CPS systems is to design a domain-specific language (DSL). DSL offers a set of abstractions and vocabulary closer to the one already employed by domain experts facilitating the modelling of new systems (Czarnecki, 2004). Each language requires an abstraction and representation of the essential concepts of the domain known as metamodel. Martinez et al. (Salvador Martínez, 2018) propose a metamodel for modelling access control policies (see Figure 15). Concepts such as rules, policies, roles, and actions are adopted. This metamodel can be leveraged to represent RBAC policies for distributed CPS systems in the context of TRANSACT. However, an extension of the abstract syntax is required to represent the architectural model concepts and their entities as orchestration services.

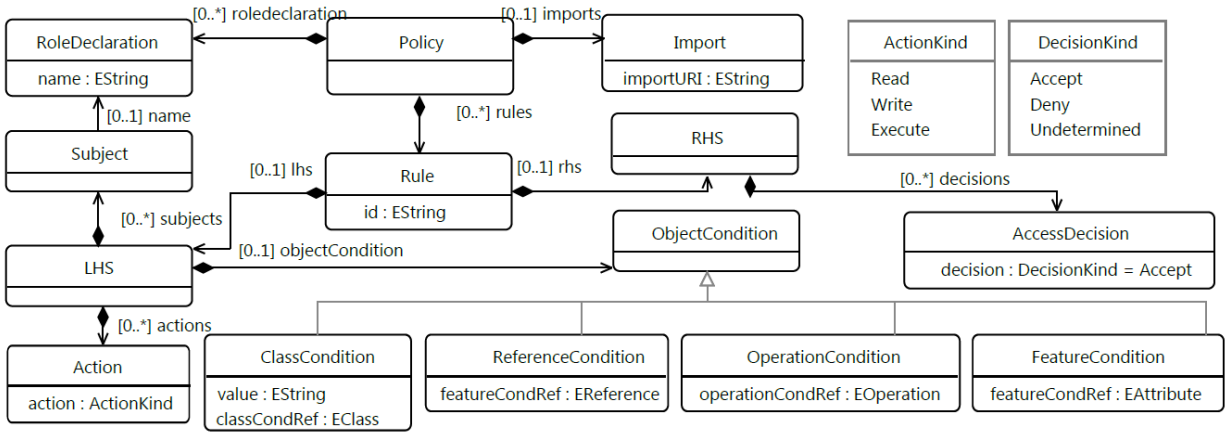

Figure 15: Access-control Policy Metamodel (Salvador Martínez, 2018).

6.2.2 Fit with concept TRANSACT reference architecture/components

The abstract syntax for RBAC policies is orthogonal, it allows to describe the access control to resources for all TRANSACT tiers (device, edge, and cloud). The ***Identity & Access*** services deployed in the tiers of the architecture (green boxes are responsible for granting/denying access to the system resources based on the RBAC policies defined.

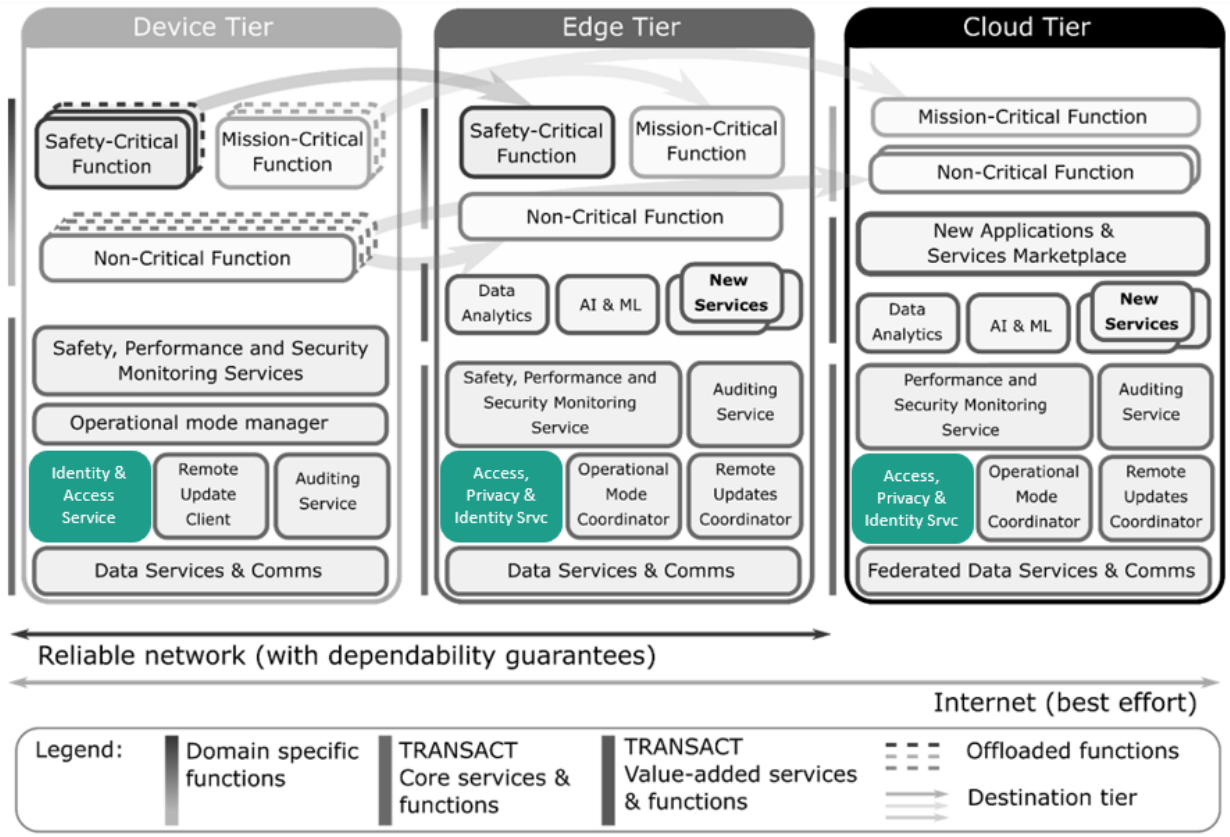

Figure 16: TRANSACT Architecture (RBAC).

6.2.3 Generic security requirements

RBAC policies: This requirement refers to the ability to specify RBAC policies over system resources in any of the three tiers (device, edge, and cloud). The modelling of policies should involve the definition of roles and permissions (resource-related operations) to control access/denial of system resources and platform servers.

6.2.4 Phase considerations

The metamodeling development process occurs at the design phase. This process is typically divided into three stages (Marco Brambilla, 2017).

The first stage is the *Modelling domain analysis* (i.e., requirements elicitation) whose objective is to identify the purpose, realization, and content of the language. In this stage, the concepts and properties that describe the domain such as roles, permissions, system resources, and other concepts that involve the implementation of RBAC policies are identified.

The second stage is the *Modelling language design* (i.e., design), whose objective is to represent the concepts of the domain by the metamodel design, i. e., to model the abstract syntax of the language and to model the constraints or well formedness rules to restrict the models.

The last stage, Modelling language validation (i.e., validation of the design), involves the instantiation of the metamodel using examples to validate the correctness. In this step, desired modifications to the metamodel are identified.

6.2.5 Participate components/entity

As mentioned earlier, the abstract syntax that enables the modelling of RBAC policies is orthogonal to the TRANSACT architecture. The role-based permissions modelled in a rule could be applied to any resource, service, server, and other TRANSACT components. However, the definition and modelling of these components depends on the architectural model of the distributed CPS.

6.2.6 Example in context of a Use case

Use Case: Monitoring and alarm triggering for Wastewater Treatment Plants (WWTP)

Applicability: WWTPs aim to clean sewage and water coming from citizen consumption, drainage and rainwater. Various physical, chemical, and biological treatments are performed in different stages to remove solids and pollutants. During these treatments, a set of physical variables (such as acidity, turbidity, temperature, and oxygen) are monitored in real time and a set of equipment or actuators (such as centrifuges, motor generators, and aeration rotors) are controlled according to the process. Several of these treatments are critical and require constant monitoring to alert of any anomalous process. However, this information collected in real time should be accessible only by workers with the appropriate role. The specification of such access control rules could be achieved by modelling the RBAC policies for the entire WWTP system. The subjects involved are grouped into roles by hierarchy to which a set of permissions are assigned that allow access to certain system services, resources, and servers. For example, query the real-time sensed data of the disinfection treatment.

6.2.7 Challenge for application within TRANSACT context

The main challenge is related to the definition of the abstract syntax of the domain. The design of the metamodel and abstraction of the main concepts for the specification of the business level policies/design of the distributed CPS system can be a complex task. The TRANSACT architecture involves the provisioning of servers and deployment of several types of resources in any of the three tiers (device, edge, and cloud) of the distributed system. Therefore, the abstract syntax for designing the metamodel should address the concepts of access control and TRANSACT architecture to enable modelling RBAC policies for operations on distributed architecture resources and servers.

6.3 Runtime verification

6.3.1 Overview

Cyber-physical systems are coengineered interacting networks of physical and computational components. CPS end devices face several security vulnerabilities and security risks. Intelligence is one of the main trends in the current evolution of the CPS system. These smart IoT devices are closer to our lives and thus store sensitive information, which is an interesting asset attractive for attackers. Most CPS enabled IoT devices provide remote control interfaces to facilitate unattended settings. However, these interfaces are also usually accessible by attackers, rendering these devices extremely vulnerable. Runtime verification is a computing analysis paradigm based on observing executions of a system to check its expected behaviour. The typical aspects of a runtime verification application are the generation of a monitor from a specification and then using the monitor to analyse the system's dynamics under study. Providing a security mechanism for these IoT devices becomes an enormous challenge. In this context, remote attestation is one of the most valuable basic security services, which establishes a static or dynamic trust root in the device. It allows a decision-making party (verifier) to assess the other party's state (prover). The verifier is usually a trusted party, e.g., cloud server, fog node, or base station, with rich computational and storage capabilities (Boyu Kuang, 2022) (George Coker, 2011). RA mechanism reduces the computing and energy consumption on the prover side. It requires no significant device modification, which is suitable for protocol extensions. Moreover, it can serve as the foundation for other security services such as firmware updates and patches.

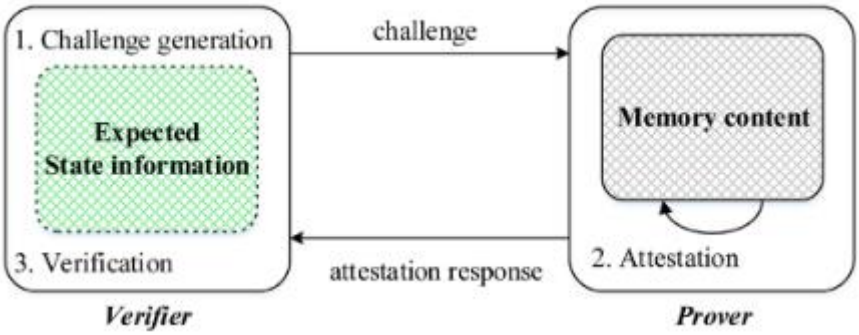

Figure 17: System overview of remote attestation (Boyu Kuang, 2022).

6.3.2 Fit with concept TRANSACT reference architecture/components

TRANSACT relies on a dependable edge computing platform to host mixed-criticality applications with stringent safety, security, and performance requirements. The cyber-physical systems combine IT systems with physical world entities, which enlarges the traditional cyber security addressing towards operational security of physical assets, to protect them from possible attacks that could cause damage to the physical assets, their environment, and even to surrounding people (Boyu Kuang, 2022). To verify the trust and protect key the privacy of nodes, we need to consider a new concept requirement as a remote attestation mechanism that can apply to sensing layer nodes. Remote attestation is a method to report the configuration information to a remote platform and verify the essential information and the authenticity. The remote attestation concept can be applied on distributed devices, cloud, and edge level in Transact reference architecture at the safety performance and security monitoring segment.

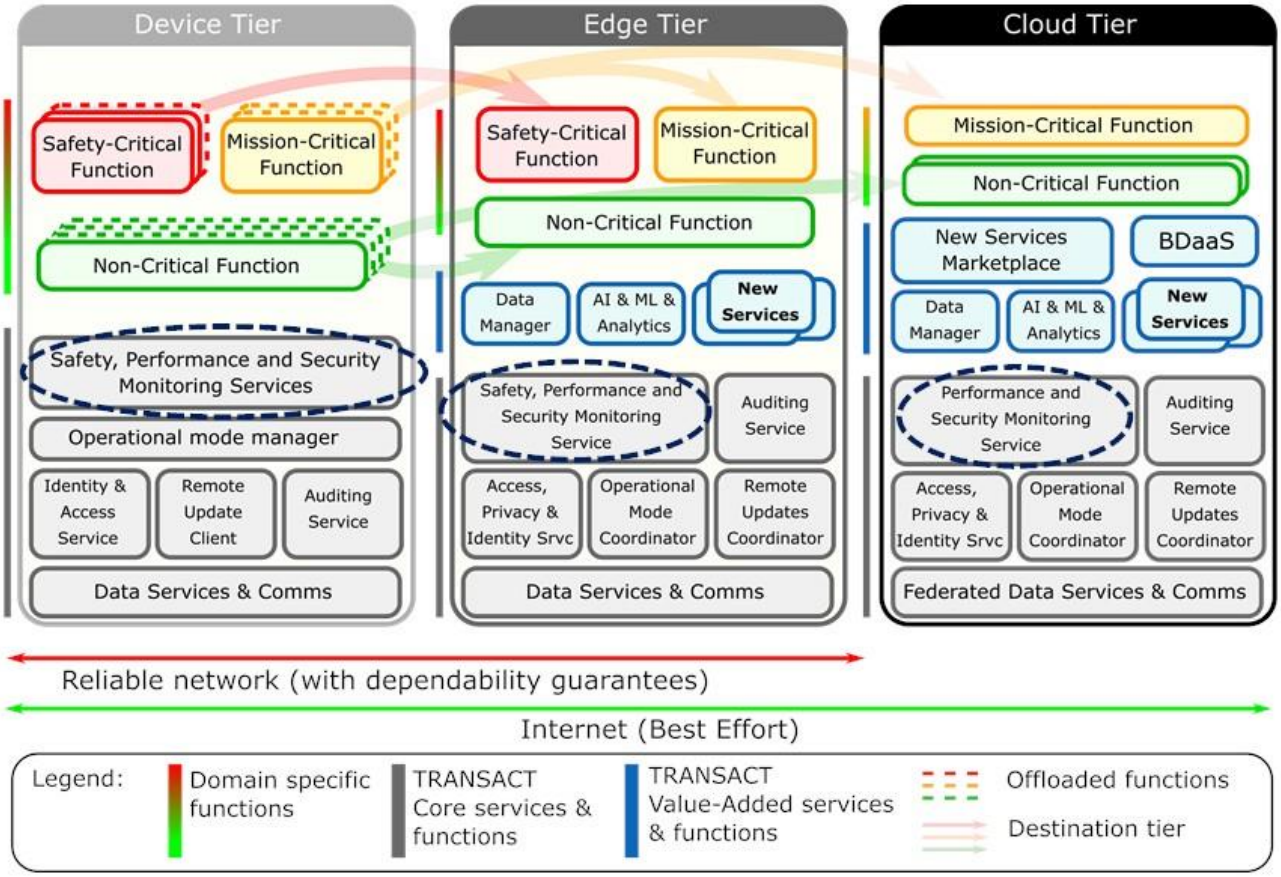

Figure 18: Applicability of remote attestation in TRANSACT reference architecture.

6.3.3 Security risks/ threats

The Distributed CPS systems have been combined with critical infrastructures such as healthcare, smarty industry, supply chain, etc., opening new doors for security attacks. Thus, new emerging threats and vulnerabilities are dangerous for distributed CPS and its integrated devices. To enable the broad adoption and deployment of CPS systems and to leverage their benefits, it is essential to check these systems from any possible attack, internal or/and external, passive, or active with a remote attestation service. Single frame security for CPS is challenging due to the heterogeneous nature of CPS devices since they operate in different IoT domains and communicate using various technologies and protocols.

1. Software adversary: adversary can compromise the program binary of an CPS service either remotely by introducing malware (i.e., remote adversary), or by being present physically near (i.e., local adversary). In both the scenarios the adversary can also eavesdrop or control the communications among services.
2. Mobile adversary: adversary is intelligent and able to move between different devices within the CPS system to avoid being detected.

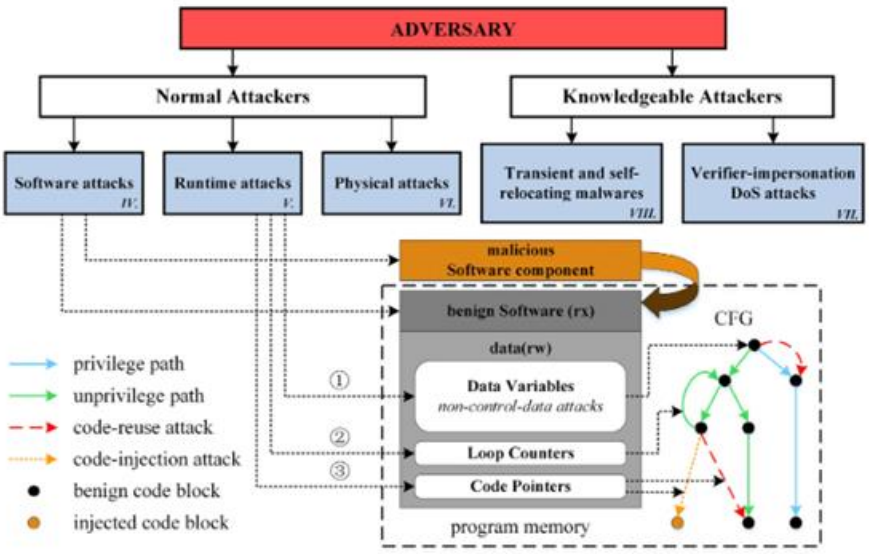

Figure 19: Security risks and threats (Boyu Kuang, 2022).

6.3.4 Generic security requirements

Trusted Updating: This concerns the ability to configure, reconfigure, and update (parts of) a system. In CPS integrated devices, these concepts become crucial as the software and configuration of IIoT systems must have the ability to be changed to provide protection against previously unknown security threats (Edlira Dushku, 2020). Updateability can be considered a countermeasure against security attacks since it allows for continuous changes to firewall configurations as threats are identified and software patches for newly discovered software vulnerabilities. The challenges relating to maintenance are again associated with resource constraints and the dynamism of CPS and IoT environments, making traditional maintenance solutions insufficient to address the needs in this security domain adequately (Koen Tange, 2020).

6.3.5 Phase considerations

Phase: Operation, and Maintenance

6.3.6 Participate components/ entity

End Devices, Edge servers, Cloud Facilities

6.3.7 Example in context of a Use case

Use Case: Remote operation of autonomous vehicles for navigating in urban environments

Applicability: the data in the autonomous vehicles needs real-time transmission and processing, so the trust of the sensing node needs real-time confirmation; secondly, when data is transmitted in the network or server, it needs not only to confirm the trust of the data source but also needs to eliminate the untrusted nodes. Furthermore, the autonomous vehicle contains a variety of components, the remote attestation mechanisms for the end device/components should have good environmental adaptability.

6.3.8 Challenge for application within TRANSACT context

The use of attestation should be validated to secure fog and edge computing architectures. Moreover, collective remote attestation protocols should be tailored around fog or edge in TRANSACT architecture by first locally aggregating attestation reports, still leveraging on the clustered nature of the architectures, and later broadcasting aggregated results to the cloud for attestation result fusion.

6.4 TPM2.0-based edge and device security

6.4.1 Overview

The main goal is to develop a secure Root of Trust chain allowing for safe communication from devices, through the edge to the cloud. Security aspects of all three tiers (device, edge, and cloud,) will be taken into consideration. The developed architecture may be used for uploading new versions of firmware and configuration securely. The practical implications of this work can be reflected in features like firmware commissioning or secure booting.

6.4.2 Fit with concept TRANSACT reference architecture/components

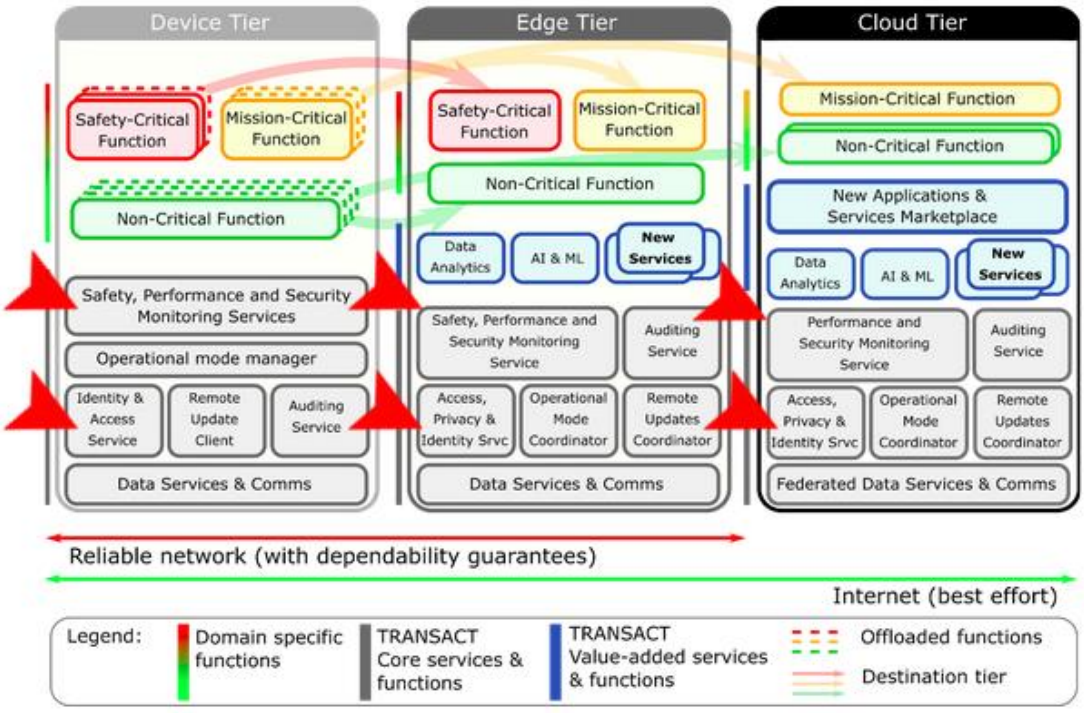

Figure 20 TRANSACT Reference Architecture.

The work will be focus on the “Safety, Performance and Security Monitoring Services” and “Access, Privacy & Identity” aspects of TRANSACT Core services and functions.

6.4.3 Security risk/ threats

The possible security risks and threats accompanying embedded systems are, for instance, side-channel attacks. These kinds of attacks may break cryptosystems and as a result, for example, retrieve secret keys. The most common attacks are based on:

- fault injections
- power glitching
- power analysis

Such threats may breach the system’s privacy and confidentiality resulting in architecture’s integrity and trust issues. There are also other kinds of attacks targeting embedded systems. General forms of attacks are concentrated on breaching the security of such systems to gain upper administrative privileges. This can be done by exploiting the systems using known bugs. The fact that simple software/firmware signing might not

be enough should also be considered. Rollback attacks, the firmware-level kind of attacks trick the system into downgrading it to some lower, yet completely legit OEM version, containing bugs and allowing for breaking the security. Therefore, a secure upgradeability model should be considered, including the ability to install only the latest version of firmware.

6.4.4 Generic security requirements

In order to counter and prevent possible risks and threats, embedded system should be equipped with a piece of hardware designed for performing the cryptographic operations. For TRANSACT, such a piece of equipment was chosen to be the TPM module. It allows for encryption, signing, attestation, secure boot functionality etc. The developed architecture must provide secure ways of verifying the integrity and validity of a system. The TPM must provide industrial JEDEC JESD47 standards, be TPM2.0-compliant, have CC EAL4+ Certification, be proof against physical and logical attacks and be tamper-resistant.

6.4.5 Phase considerations

- Collecting detailed requirements
- Designing security-related system architecture
- Developing mechanisms allowing for signing and verification of a ready-to-be-downloaded firmware
- Testing the developed solution
- Deploying the solution
- Maintenance

6.4.6 Participate components/ entity

Infineon Iridium SLM 9670 TPM2.0 was chosen as the component providing the functionalities. It has different cryptographic algorithms such as RSA (1024, 2048), SHA (1, 256), ECC NIST P256, ECC BN256 built-in, bus encryption and NIST SP800-90A random number generator. It can operate in a wide range of temperatures (-40°C to 105°C) and store up to 10 keys. This solution can be applied to end devices.

6.4.7 Example in context of a use case

Secure Over-The-Air updates of new versions of firmware for the automotive sector.

OTA process requires the interaction between all the system segments. A piece of software running on a cloud allows for the management of new firmware versions. A specially crafted mechanism signs the packages attesting that they are legit. All end devices are listening for updates. If an update is ready, they begin to download it. The downloaded firmware is checked for possible corruption and then the end device verifies its legitimacy, and after that the update procedure commences. Customization of a rollout strategy is also possible. Then the update will not be sent to every device at once, but partially, according to the established plan. Such an approach prevents possible bugs from spreading to all devices.

6.4.8 Challenges for application within TRANSACT context

General description of tasks that need to be done:

- Describing detailed, exact requirements
- Developing the architecture
- Designing workflow for OTA updates
- Developing signing and verification mechanisms
- Testing the solution

6.5 Anonymization: prevent personal data leak

6.5.1 Overview

Artificial intelligence, Internet of Things (IoT) and smart sensors are great new technologies. For society, this is also accompanied by a loss of privacy. Data from public spaces, may contain personal data that can jeopardize the privacy of people whereas in for many use cases, the personal data is not relevant. Take surveillance cameras as an example. Nowadays, these types of sensors are used in combination with video analytics to gather data about traffic and crowds while the identity of the vehicles and people is not relevant for traffic control and crowd control. To allow such systems to be used, GDPR compliance is required. This implies that not personal data may be accessible and the risk for a data leak should be minimal. Hence, the data that contains personal data such as video footage in public spaces should be anonymized. For a CFS this could be performed on the device, on the edge or in the cloud. However, to minimize the risk, the anonymization should be applied as soon as possible in the processing chain. This implies anonymization on the edge or even on the device.

6.5.2 Fit with concept TRANSACT reference architecture/components

Considering the reference architecture of TRANSACT, the privacy is protected by a component “Access, Privacy & Identity Service”. This one way of offering a solution. The GDPR is only a concern when personal data is involved. The GDPR only allows the processing of personal data when the goal for doing this is unavoidable, proportional to the goal and if the objective is legitimate. There are many more strategies that can be applied to ensure the privacy of individuals.

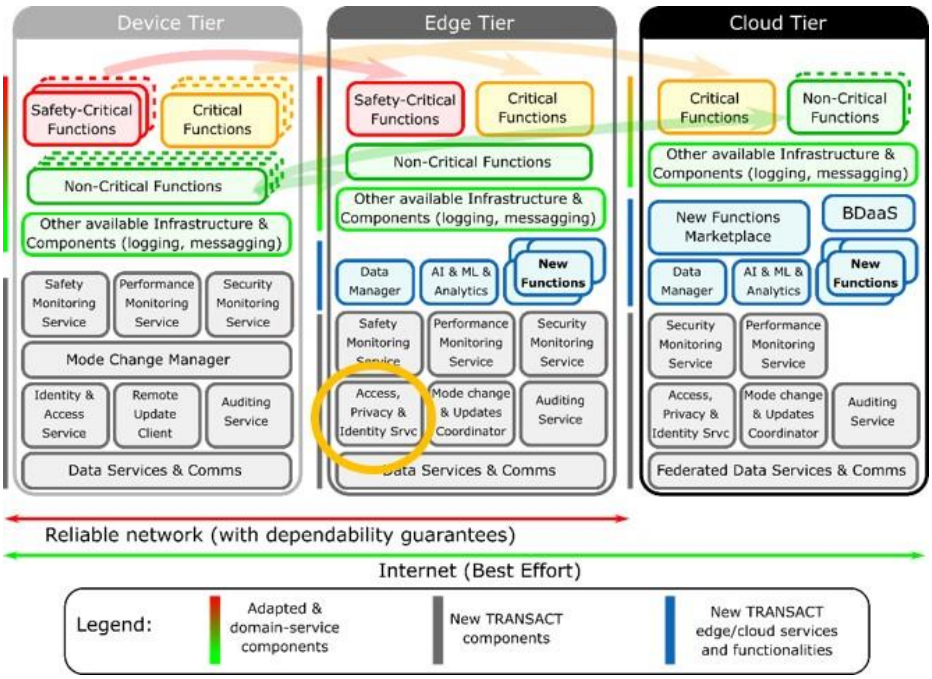

Figure 21: Applicability of anonymization in the edge tier.

6.5.3 Mitigation of privacy threats/risks

We also acknowledge that using data processing requires us to adhere to privacy regulations. We care about the privacy of all people involved in the data processing. Therefore, a TRANSACT system must adheres to the Privacy by Design paradigm of prof. Jaap-Henk Hoepman of the Radboud University Nijmegen (Hoepman,

2014). The Figure 22 below shows the 8 strategies required to process data correctly while ensuring privacy of individuals whose identity is present in the data.

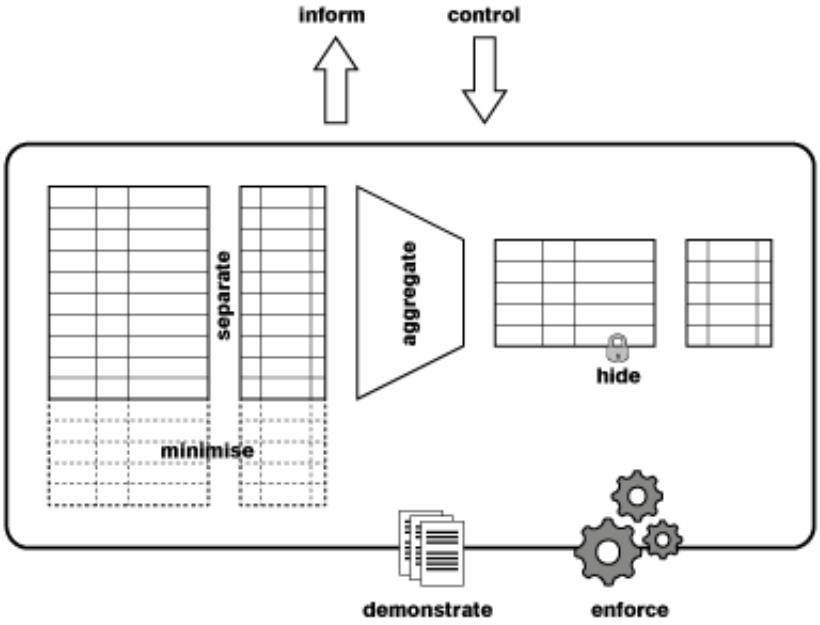

Figure 22: Privacy design strategies.

The eight strategies are the following:

Minimize: The amount of personal information that is processed should be minimal. Personal information is also described as personal identifiable information (PII), which can be collected, stored, and disseminated.

Hide: Any personal information that is processed should be hidden from plain view, for example by using encryption, mix networks, or unlinking techniques. Data is being hidden as long as possible until an authorized person requests access. The data is only accessible in predefined circumstances (e.g., an offense) and by authorized persons.

Separate: The processing of personal information should be done in a distributed fashion whenever possible. This way, access can be granted to certain data parts without being able to compose complete profiles of one person.

Aggregate: Processed information should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.

Inform: Data subjects should be adequately informed whenever personal information is processed.

Control: Data subjects should have agency over the processing of their personal information. Data subjects should have the right to view, update and ask for deletion of personal data collected.

Enforce: A privacy policy compatible with legal requirements should be in place and should be enforced.

Demonstrate: Be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

6.5.4 Phase considerations

The anonymization function is part of the Privacy-by-Design and must be considered during the design time (by definition) but also during, deployment, operation, and maintenance phase.

6.5.5 Participate components/entity

Preferably in the Device or Edge tier but this depends on the application. If personal data is required at the cloud level, the information security is more complex and the risks for a data leak increases.

6.5.6 Example in context of a Use case

Below we give an example that applies for UC1 where video sensors are used in the public space. People in the video footage may be recognizable and license plates of vehicles may be readable. For this example, each of the eight components explained at the previous section can be applied as follows:

Minimize. We only store metadata that is used for analytics. Video data that is received from the camera (tier) by the edge device is analysed and not stored. With respect to detected objects, only the following data is stored: counting results per 30 seconds per object class (for example: car, pedestrian, bicycle); trajectory/path per object; classification per object (into car, pedestrian, bicycle etc.); speed per object; density of the counting area per 30 seconds.

Hide. Analysis data is stored on a local hard disk. When connected to the edge Tier, the user has to provide authentication (username, password) to obtain rights to retrieve the stored data or to access the web UI. Data is sent to clients using HTTP or web socket connections. This data does not involve personal data.

Separate. The data mentioned in point 1 is stored in separate storages on the same hard disk. For example, object trajectories are stored separately from their classifications, counting results are stored separately from the camera configuration. Databases containing object information are only linked together using unique identifiers (UUIDs) but require access to the different containers. These UUIDs are not traceable to individual persons.

Aggregate. Personal information in the form of video images containing natural persons is discarded directly after usage and any visual data about detected objects is discarded after analysis. The only information available is classification into a type (for example: person, car), location (with respect to camera, and GPS) and speed. However, this information cannot be traced to individuals. This information is required for correct analytics for mobility research and crowd management.

Inform: According to the GDPR, data subjects, in this case the observed people, need to be informed when video surveillance is present, and/or when personal information is processed (such as unique MAC addressed from Bluetooth/Wi-Fi sniffers). However, since the video feed of the camera is not stored or used for surveillance, and no personal information is detected or stored, informing the public is not strictly required. However, we do strongly recommend that system integrators and customers are correctly informed about the people that they are being monitored and ensure them that their privacy is respected.

Control: Since no personal data is stored nor exposed outside the edge device, the right of access, rectification, erasure, and restriction does not apply. Nevertheless, everyone is allowed to contact the Data Protection Officer of the contractor that is responsible for the processing.

Enforce: A privacy document describes the technical safeguards that the TRANSACT product uses to protect the privacy of the data subjects. This is enforced by the appointed Data Protection Officer of the supplier and reviewed at every TRANSACT release. In case of systems that process personal data, a Data Protection Impact Assessment (DPIA), should be performed. This enables both customers and data subjects to read about our privacy policy and data processing methods.

6.5.7 Challenge for application within TRANSACT context

A DPIA should be performed per use case and the above privacy-by-design strategies should be implemented to mitigate the risks to a minimal.

6.6 Security and privacy concepts for wireless communications

6.6.1 Overview

One of the most vulnerable elements of the Cyber Physical Systems is the wireless communication. Due to the open character of the wireless communication channel, the signal can be easily eavesdropped or jammed putting on risk the security of the data transmitted or the proper operation of the system. Even though private and important data is encrypted before being transmitted, the ability to record the signal gives the potential attacker chances to identify such crucial information as the type of encryption or modulation.

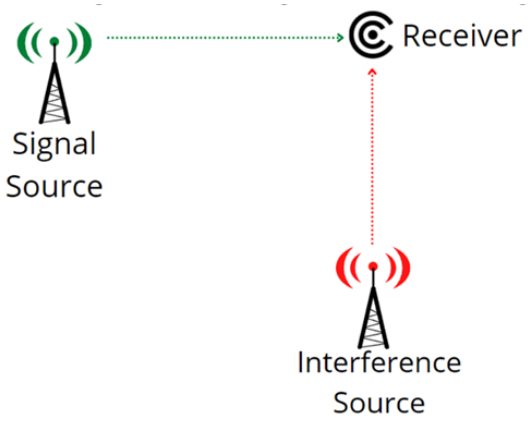

Figure 23: Illustration of the wireless communication in real environment.

To improve the quality of the communication, it is expected to have the received power of the desired signal as high as possible, while the interference as low as possible. If this cannot be done by controlling the power of these transmitters, a directional antenna can be used and configured towards the receiver, to achieve the highest gain towards the signal and to minimize it towards the interference source (Michal Tarkowski, 2017).

The main drawback of the approach is that it may be inefficient when there are many attackers or signal sources. Additionally, due to the fixed antenna radiation pattern, in that case it has to be assumed that the attacker and the receiver are in fixed locations and not moving. Furthermore, in the scenario where many receivers are considered, it might be difficult to transmit the signal towards them being able to omit the unexpected actor.

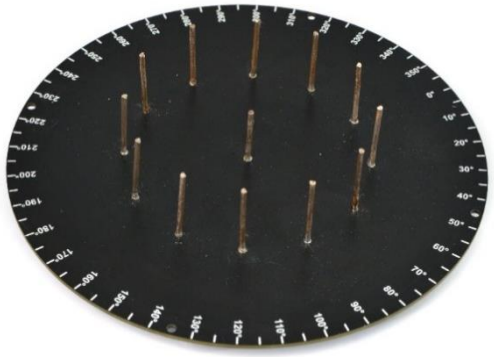

Figure 24: Electronically Steerable Parasitic Array Radiator (ESPAR) antenna.

To solve the abovementioned problems, it is possible to detect the unwanted signal (in case of jamming – intentional or unintentional) and to utilize dedicated switched beam smart antenna which is possible to switch between a number of radiations patterns and use adaptive beamforming algorithms to adaptively adjust the antenna radiation pattern to optimize the communication parameters for current environmental conditions. Example of such antenna Is Electronically Steerable Parasitic Array Radiator (ESPAR) antenna where the main beam can be switched around 360 degrees. This can be done by shorting or opening the passive elements located around the active element in the middle That way, it is possible to maximize the signal-to-noise ratio achieving high efficiency of the communication regardless the occurred interferences (Chen Sun, 2004). Additionally, by utilizing switched beam antenna and dedicated direction-of-arrival algorithms, it is possible to estimate the direction from which the jamming signal is transmitted.

6.6.2 Fit with concept TRANSACT reference architecture/components

The component will fit the Safety, Performance and Security Monitoring Services aspects, mostly focusing on Device and Edge Tier.

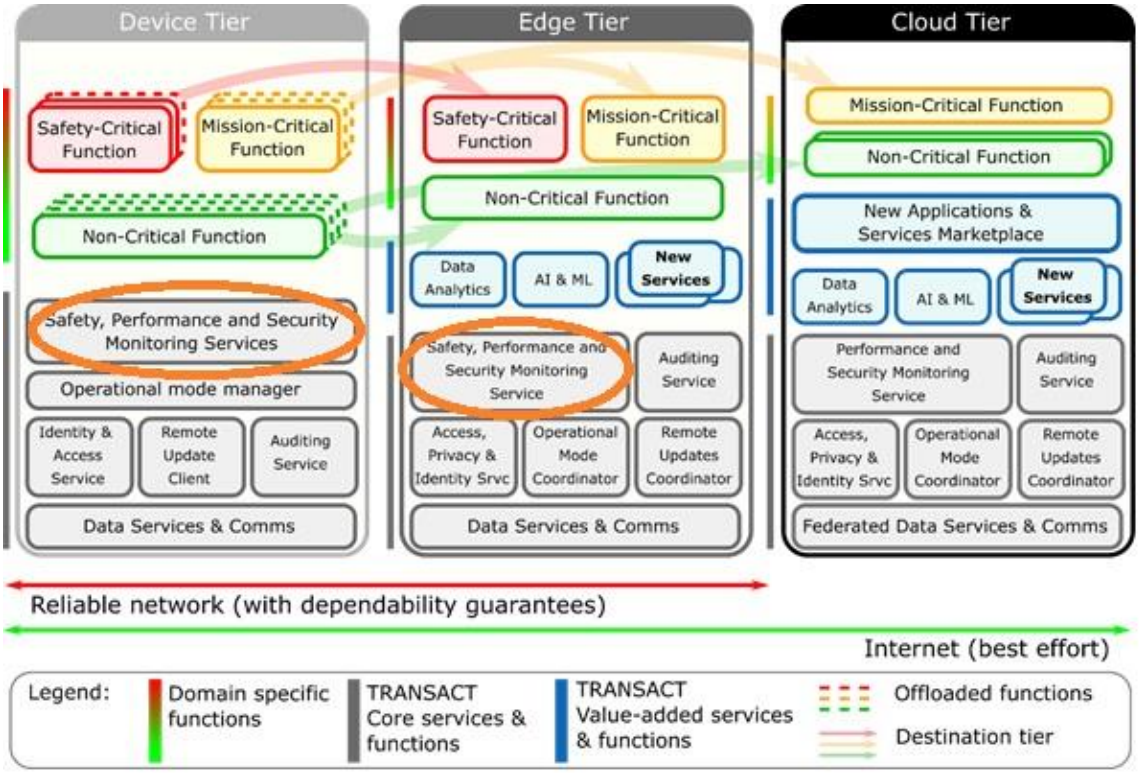

Figure 25: Concept fit in the TRANSACT reference architecture.

6.6.3 Security risk/ threats

Threats in the physical layer of wireless communication:

- Access based attacks
- Channel Disruption

6.6.4 Generic security requirements

In general, all the data transferred through the wireless communication channel needs to be protected. Especially critical and private data needs to be protected. Especially, security measures for critical and private

data should be undertaken. Additionally, it is important to not to impact on the consistency of the data and keep the data rate as high as possible so that other systems can work without interruption even in environment where high interference occur.

6.6.5 Phase considerations

Phases: Development, deployment, operation, maintenance

6.6.6 Participate components/ entity

End Devices and Edge servers.

6.6.7 Example in context of a use case

Use Case: UC2: Maritime decision support enhanced by distributed, AI enhanced cloud solutions.

Within the use case, unmanned surface vessel equipped with several dedicated sensors will be employed to perform unmanned inspections of the surrounding. Data from the sensors will be collected by the edge and transferred to the cloud. To increase reliability of the communication, presented component would be implemented to increase the resistance to any external intentional and unintentional interferences.

6.6.8 Challenge for application within TRANSACT context

The main challenge is to develop and implement a suitable algorithm that will analyse and adapt the current parameters of the communication to continuously assure security of the communication in the changing environment and considering its specifics. Additionally, the efficiency and computation power consumption need to be optimized. Developed solution needs to be tested in different conditions, verified, and validated.

6.7 PKI Infrastructure

In this task, CISC is working on the Public Key Infrastructure, which acts as the glue between the different components:

- Server
- Client
- Kiosk

The server acts as certification authority and token management system. It issues the certificates and tokens. The server certificate is signed by the external root CA and is known by all entities (stored in the trust CA store). Revocation is possible through CRL (certificate revocation list).

The business logic communications with the server through TLS connection with server authentication based on an API key.

The Kiosk is a mobile or stationary device for receiving and validating tokens. It communicates with the server through TLS connection with mutual authentication based on a client certificate. The communication with the Client is either possible through non-encrypted NFC, BLE or QR based channels with challenge-response authentication.

The Client is a mobile personal device owning digital tokens. The registration is based on a server authentication (using a ticket) through TLS connection. Further communication with the server is done through TLS connections with mutual authentication using the client certificate.

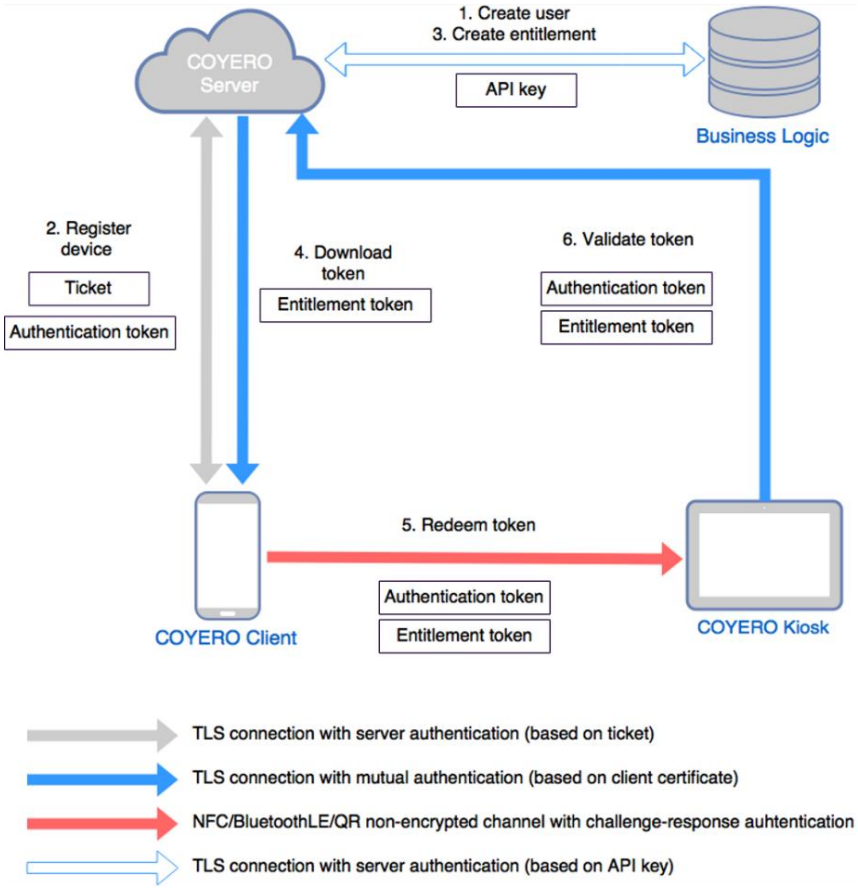

Figure 26: PKI Infrastructure.

Token management

Authentication token: an extended certificate tied to specific client or kiosk device. It represents the identity of a user through a public key. It is used for the secure communication with the server.

Entitlement token: is tied to an authentication token and represents the digital ownership of an item/service. Attributes are used for additional properties like validity.

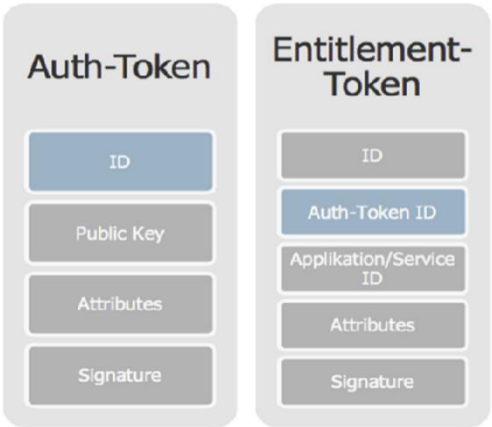

Figure 27: Entitlement token.

7 Security & privacy concepts for Transact value added services & functions

7.1 Centralized machine learning with decentralized data

7.1.1 Overview

One of the major bottlenecks when it comes to training of neural networks is the lack of data. Assuming, that a single client does not generate sufficiently enough data on its own for accurate training results, it is a straightforward idea to collect data from several clients by forwarding and aggregating them on a central server where the neural network is trained (see Figure 28).

The central server also orchestrates the clients and manages the data transfer and update mechanisms. Such a setup is called centralized machine learning (Peter Kairouz, 2021).

When the training is finished, the inference can either be performed on the server as well *or* the neural network is sent back to the clients and inference is performed on edge devices (see Figure 28 where a) Several clients send data to the central server which performs the training of the neural network. b) The clients send data of interest to the central server where the inference is performed. c) The trained neural network is sent back to the clients which infer the local dataset).

In any case, the transmission of raw and private data must comply with the general data protection regulations, which is not feasible in most of the cases. Especially in the case of data-silos, e.g., data originate from different companies, an exchange of data is not an option. On one hand, all partners would benefit from each other. But on the other hand, they cannot exchange sensitive data. Leveraging the complete data while complying with privacy is a major challenge for centralized training.

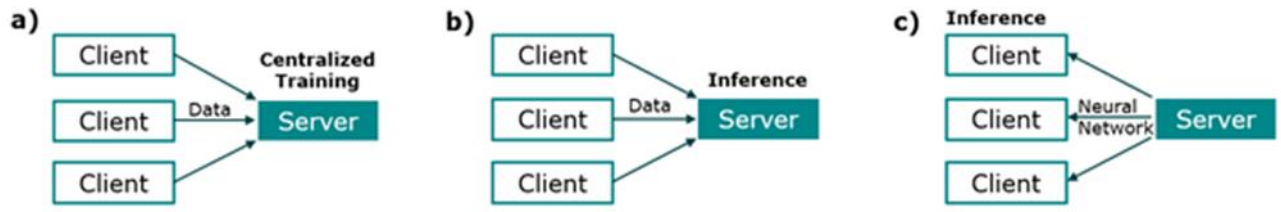

Figure 28: Client-server architecture for centralized machine learning.

In contrast, decentralized training is based on a peer-to-peer architecture and does not have a central server and hence no central orchestration which makes such a concept not feasible for the TRANSACT architecture (Paul Vanhaesebrouck, 2017).

7.1.2 Fit with concept TRANSACT reference architecture/components

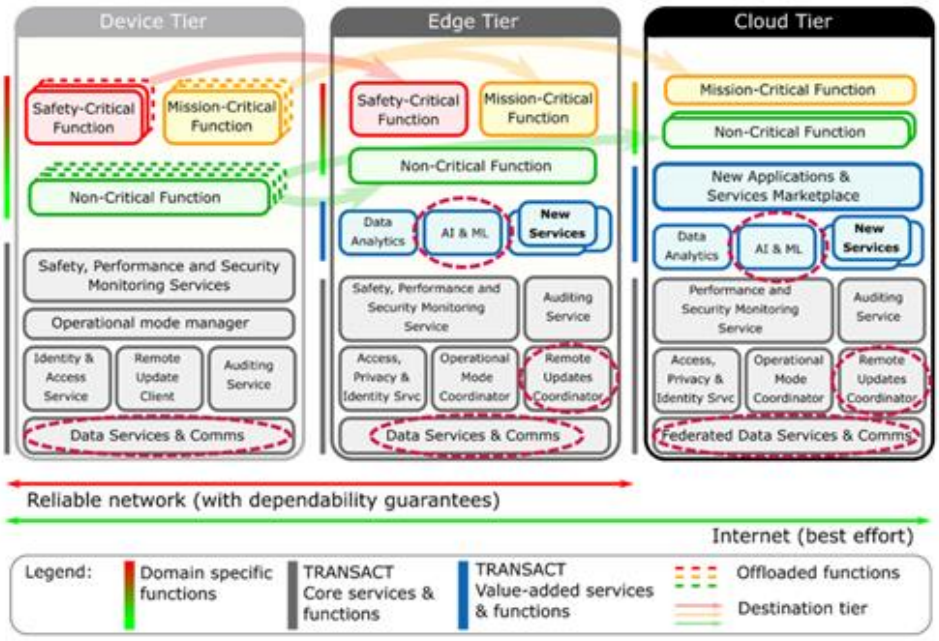

Figure 29: TRANSACT architecture.

Centralized Training affects several points within the TRANSACT architecture:

- **Data Services & Communications:** For centralized learning, data need to be passed through from the device to the cloud backend. When dealing with sensitive data, the communication must be secured, and data need to be end-to-end encrypted.
- **AI & ML:** Depending on where the training and inference is performed, either the Edge or Cloud AI & ML component is affected.
- **Remote Update Coordinator:** In the case that the inference is performed on the Edge Tier, the neural network must be updated. A server in the Cloud Tier is responsible of the orchestration of the connected clients and managing the different versions of the neural networks.

7.1.3 Generic security requirements

In general, there are two assets which need to be protected: data and the trained neural network. Since both are transferred across the three tiers, end-to-end encryption is a minimum requirement.

Depending on the domain, further standards must be considered. E.g., for the automotive Use Case 3 “Cloud-Featured Battery Management”, following standards may be relevant:

ISO/SAE 21434: “Road vehicles – Cybersecurity engineering”

UNECE R 155: “Cyber security and cyber security management system (UN Regulation No. 155, 2021)”

UNECE R 156: “Software update and software update management system (UN Regulation No. 156, 2021)“

7.1.4 Phase considerations

Design, development/deployment, and operation.

7.1.5 Participate components/entity

- **Device**: Generator of data.

- **Edge**: Hosts the AI client for inference and transmits the data to the cloud.
- **Cloud**: Orchestration of clients and training of neural network.

7.1.6 Example in context of a Use case

The following example relates on the automotive Use Case 3 “A Cloud Featured Battery Management System”:

Data are generated by the battery management system, power train, control units and sensors. In order to identify abnormal degradation of the battery which can originate from a defect, the historic data can be used as input for a neural network to predict the remaining useful lifetime. However, this requires that a neural network has already been trained. Since battery pack testing in the lab is very expensive, not every condition and combination can be simulated. To sidestep this limitation, vehicles could learn from each other by exchanging data. To do so, data from vehicles of a fleet are forwarded to a central server and used for training and inference. The driver receives the result of the prediction. The application of centralized learning requires a cross-silo approach which comes along with all security and privacy needs as discussed in previous chapters.

7.1.7 Challenge for application within TRANSACT context

In order to apply centralized training with decentralized data, a corresponding framework comprising of server and client applications must be developed. Security aspects as discussed must be guaranteed.

7.2 Security and privacy concepts for cloud-based applications

7.2.1 Overview

Cloud applications are frequently targeted by criminals as these attacks can be easily automated. However, security of cloud-based applications is more than protection against attackers, and covers potential accidental loss of data, unintentional misuse, etc. It always comes down to protection of information of all kinds, such as personal information, IP, or financial information.

The way products are designed is central to the security of those systems. In other words, security needs to be built-in from the ground up. Concepts as “security by design” and “security by default” are commonly used in this respect. Security by design means organizations acknowledge the importance of security from the start, rather than being an afterthought. Security by default means that the default configuration settings are the most secure settings possible. It remains of course important to deliver user-friendly products, and balancing risks and usability is therefore crucial.

Security is not only important during the design phase, but during the total product lifecycle, including development/implementation, testing, operational use and even when dealing with end-of-life products. There are so many aspects related to security of cloud-based applications, and it is impossible to cover everything. In the next sections, we will list the most common risks/vulnerabilities of cloud-based applications and use this as a starting point to highlight some important security requirements.

7.2.2 Fit with concept TRANSACT reference architecture/components

In the Figure 30 below, the orange ellipses show the components in the TRANSACT reference architecture that are relevant for this section.

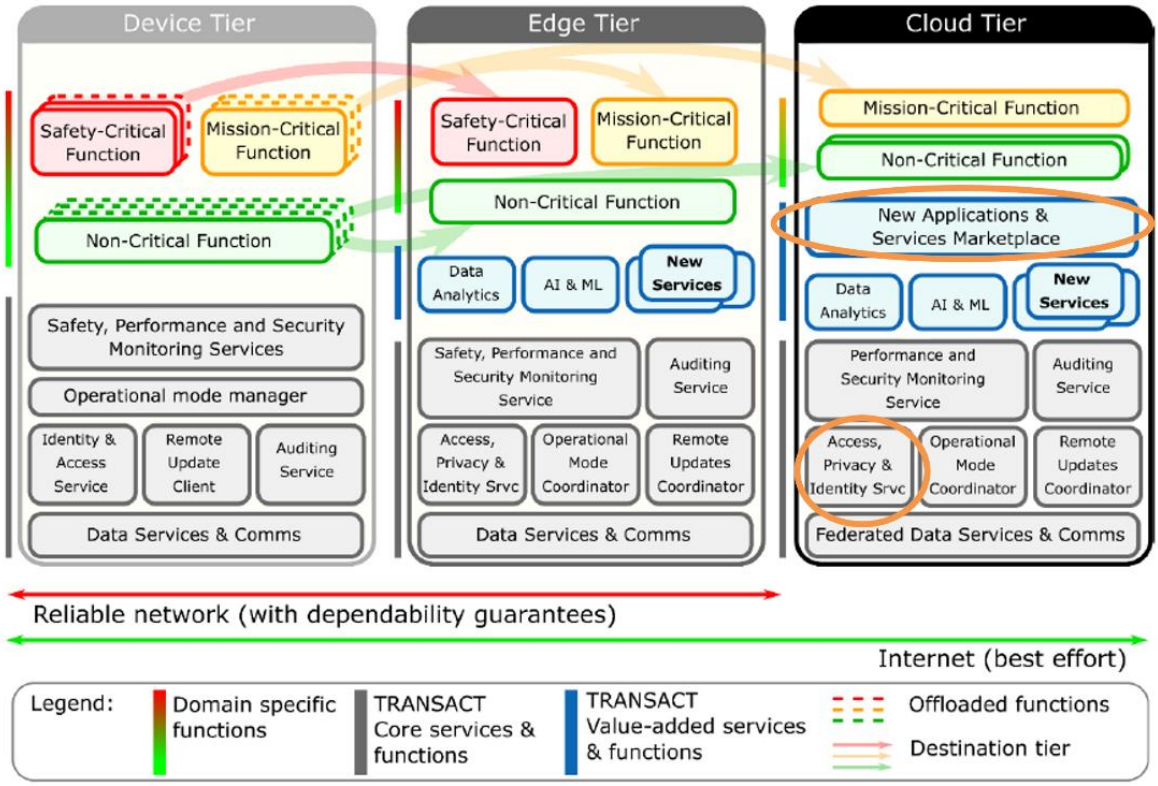

Figure 30:TRANSACT reference architecture.

7.2.3 Security risk/ threats

There are numerous risks for cloud-based applications, related to technical vulnerabilities. The Open Web Application Security Project (OWASP) is a worldwide not-for-profit organization that periodically publishes a list of the top ten most critical web application security risks. This is important and helps people to focus their attention and efforts.

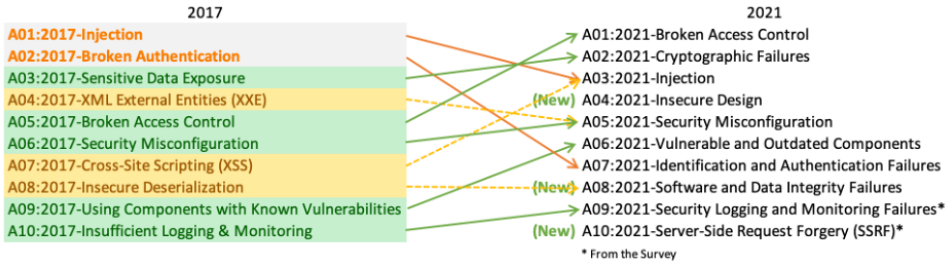

Figure 31: Top ten security risks for web applications in 2017 and 2021 according to the OWASP (https://owasp.org/www-project-top-ten/).

Here is a brief overview of the top ten security risks:

Broken access control: Access control are important to prevent that user can act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data.

Cryptographic failures: Often, there is a lack of data encryption for sensitive or personal information. Alternatively, the cryptographic algorithms or protocols that are used might be old or weak.

Injection: Injection flaws allow an attacker to "inject" data into a system, which can then enable the attacker to execute commands or access data without proper authorization. SQL is commonly targeted by such injections.

Insecure design: It is important to differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.

Security misconfigurations: Many server-side issues are due to misconfigurations. These can vary from default accounts being left unchanged through to unprotected files and directories.

Vulnerable and outdated components: Using components that are outdated, unsupported or vulnerable is an important risk. Attackers may detect unpatched components, and target these.

Identification and authentication failures: These failures refer to web applications that use default, weak or well-known accounts/passwords, or that do not prevent attackers from performing brute-force attacks (e.g., dictionary attacks).

Software and data integrity failures: Software and data integrity failures relate to web applications that do not protect against integrity violations. An example of this is where an application relies upon plugins or modules from untrusted sources. An insecure pipeline can introduce the potential for unauthorized access, malicious code, or system compromise.

Security logging and monitoring failures: Sufficient monitoring and logging is fundamental to detect security breaches, and to react to these in an adequate manner.

Server-side request forgery (SSRF): SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination.

7.2.4 Generic security requirements

There are many ways to prevent and mitigate the above-mentioned security risks. In this section, some important requirements for secure cloud-based applications are highlighted.

Security-by-design: As already mentioned, security should already be taken into account during the design phase. For example, account lockout after a number of failed login attempts could be implemented to increase an application's resilience against attacks.

Security-by-default: The default configuration settings in a product should be the most secure.

Security testing: It is important to test cloud-based applications from security point-of-view, in addition to functional tests. This could be static or dynamic code analysis. Static code review refers to analysing the source code for vulnerabilities without running the code, while dynamic analyses are performed while executing the code. Related to this, external penetration testing could be considered to detect vulnerabilities.

Encryption: Data encryption with strong and up-to-date algorithms should be used to protect important data, both "in transit" and "at rest".

Access control + role management: Effective account management principles such as strong password requirements and 2FA are very important. In addition, every user should be given as little privileges as possible for them to get what they need from the system (I.e., minimal privileges principle).

Logging / monitoring: Logging is important, not only for recording that suspicious activity is taking place, but also to analyse possible incidents or data breaches.

7.2.5 Phase considerations:

Security and privacy of cloud-based applications must be considered during the design, deployment, operation, and maintenance phase.

7.2.6 Participating components/ entity

This concept is about cloud-based applications, so this sections obviously relates to the cloud tier.

7.2.7 Challenge for application within TRANSACT context

In TRANSACT, we are dealing with safety-critical CPS, and security vulnerabilities may thus have an impact on safety. Hence, it is important to use all best practices related to the security of cloud-based applications. In addition, it is important to acknowledge that there will always be remaining risks, and additional controls on device and edge tiers are required.

7.3 Multi-cloud concept for cloud security posture management (CSPM)

Figure 32 introduces multi-cloud concept for cloud security posture management (CSPM). It visualises the use of AI and ML as well as the heuristic rules to identify weaknesses, such as configuration mistakes and anti-patterns of security best practices, in the cloud that organizations are using.

CSPM is a fundamental area of cloud security. Cloud services are constantly evolving that also creates new security challenges. Therefore, there are many unknown security threats and future is unknown. While CSPM will utilize AI/ML, it cannot fully rely on it. Threat researchers and security experts dedicated to cloud security research are paramount.

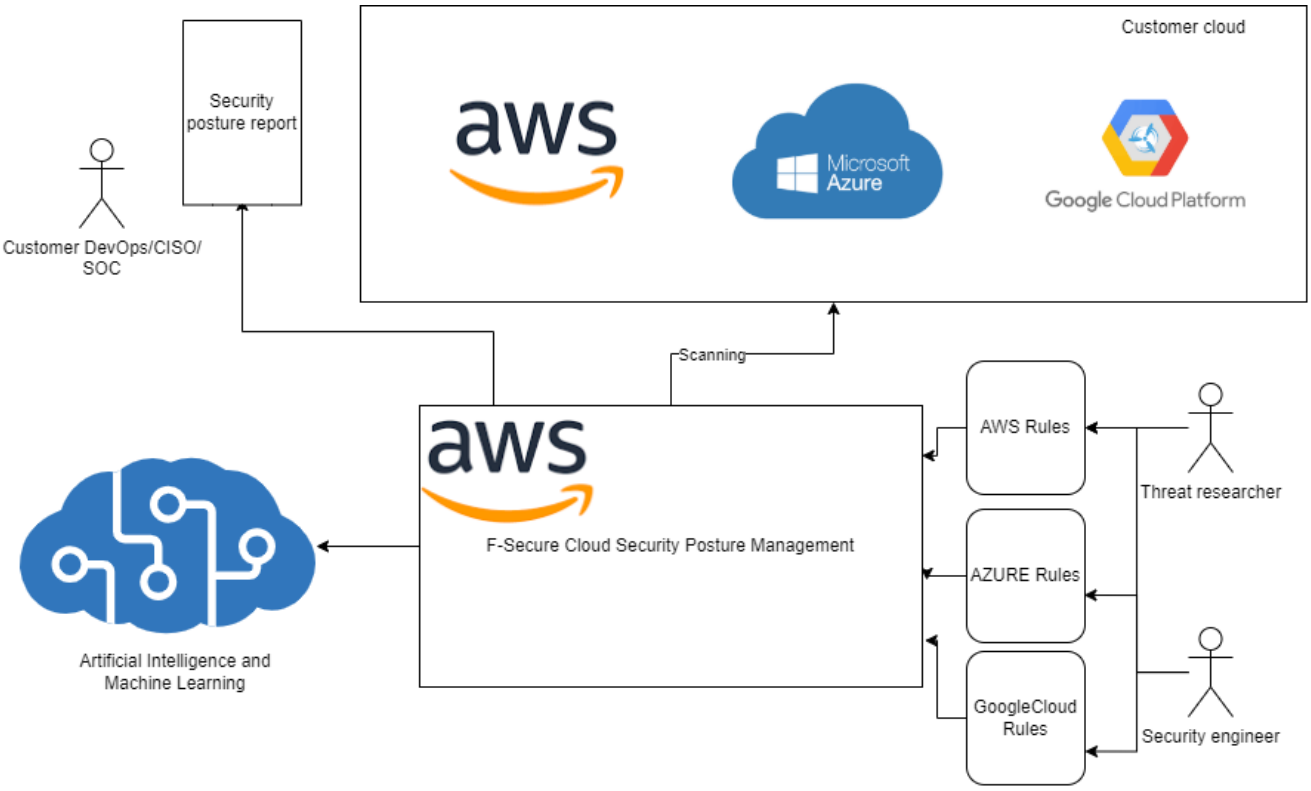

Figure 32: Illustration of the CSPM concept for cloud security.

7.3.1 Fit with concept TRANSACT reference architecture/components

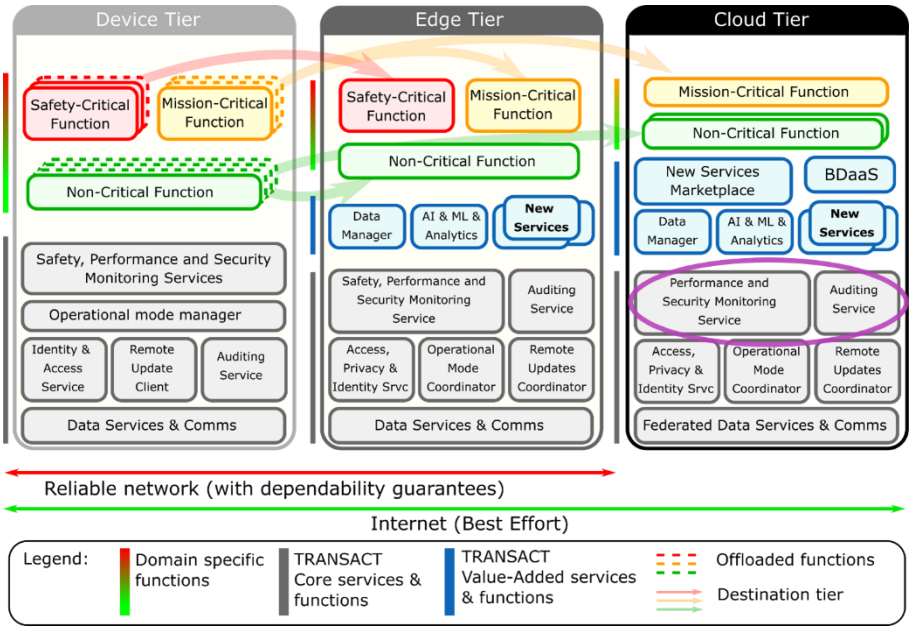

Figure 33: CSPM applicability with TRANSACT reference architecture

7.3.2 Security Risk/ Threats

Without CSPM, the users of cloud services include major risks in cloud misconfigurations and compliance. There are also risks associated to CSPM. It has access to cloud infrastructure and could potentially leak sensitive data.

7.3.3 Generic Security Requirements

CSPM is a fundamental area of cloud security. Cloud services are constantly evolving that also creates new security challenges. Therefore, there are many unknown security threats and future is unknown. While CSPM will utilize AI/ML, it cannot fully rely on it. Threat researchers and security experts dedicated to cloud security research are paramount.

7.3.4 Phase Considerations:

CSPM is applicable in deployment, operation, and maintenance phases.

7.3.5 Participating Components/ Entity

CSPM is for securing cloud infrastructure and relates to the cloud tier.

7.3.6 Example in context of a Use case

For instance, Use Case 1 is using AWS cloud infrastructure and CSPM could detect an unencrypted S3 bucket.

7.4 User and entity behavioural analytics (UEBA) concept for cloud security

As security threats to clouds are currently unknown, we should think how the things will change from the attackers' point of view. For example, uncertainty of malicious intent is growing. Maliciousness of an event can no longer be determined. Instead, we must look at the context and typical usage.

Figure 34 exemplifies user and entity behavioural analytics (UEBA) concept for cloud security that addresses the context of the events. In the example, AWS is the cloud service, and the data source is CloudTrail, which is the de-facto solution for tracking user activity and API usage. There is a fundamental challenge in interpreting the AWS CloudTrail logs. By design, user identity is not visible in the audit-trail. In the first UEBA prototype, the authors have resolved the challenge by tracking the actual user entity and enriching the logs based on it. The enriched logs are being sent to a backend for further analysis.

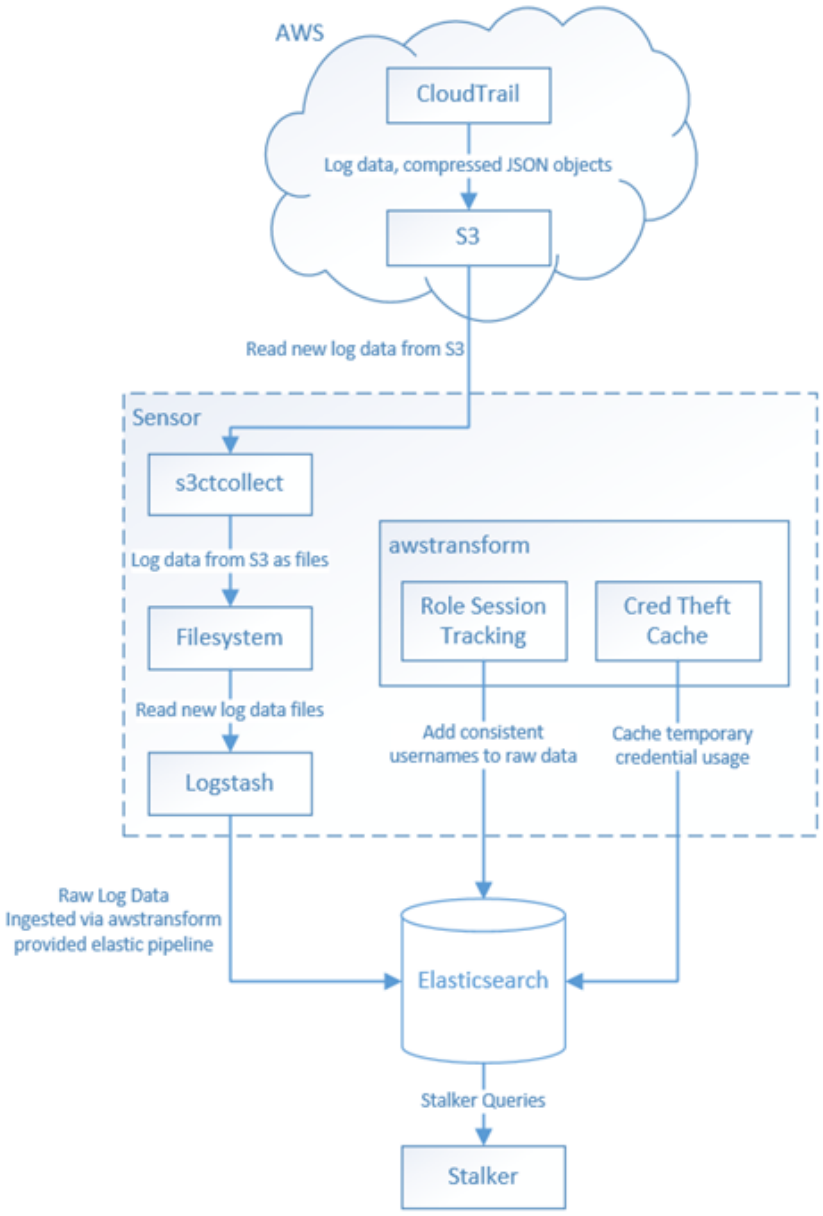

Figure 34: An example of the UEBA concept in interpreting AWS CloudTrail.

7.4.1 Fit with concept TRANSACT reference architecture/components

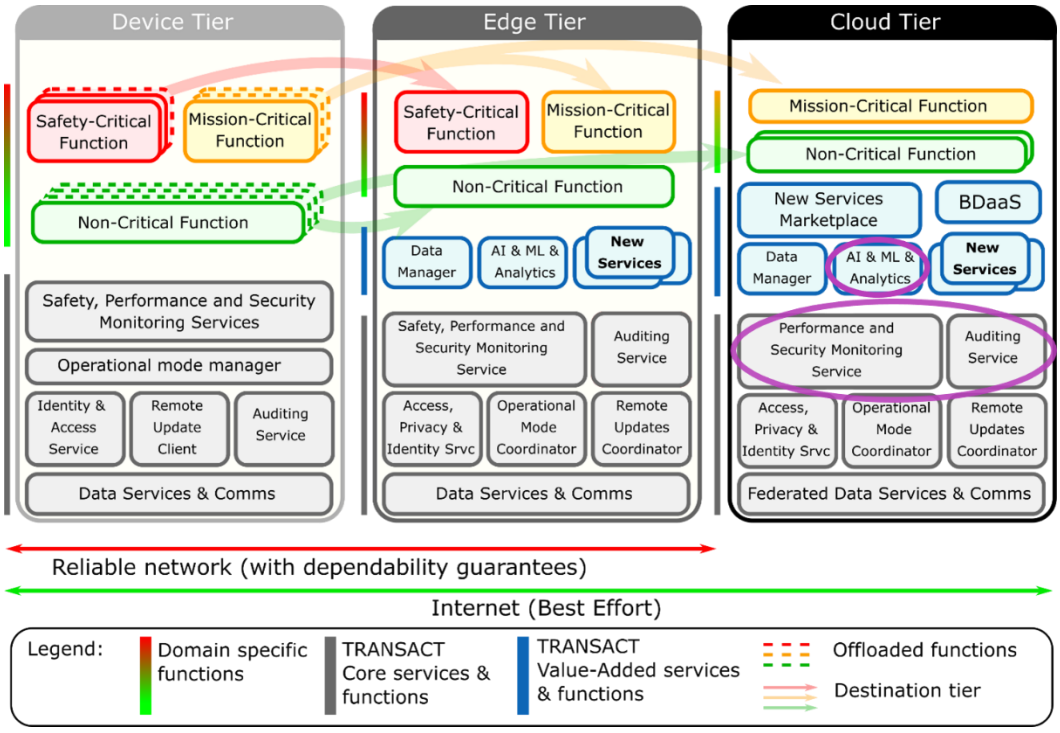

Figure 35: UEBA applicability with TRANSACT reference architecture

7.4.2 Security Risk/ Threats

Without security solution adapting UEBA, this traditional security solution can cause a lot of false-positive security alarms that, in turn, will hide the real security incidents.

7.4.3 Generic Security Requirements

UEBA is central part of the Cloud DR and the generic security requirements are part of the generic security requirements of Cloud DR.

7.4.4 Phase Considerations:

UEBA is applicable in development, deployment, operation, and maintenance phases. The UEBA maintenance include retraining of AI models when needed.

7.4.5 Participating Components/ Entity

UEBA is a part of Cloud DR and securing customers' cloud infrastructure and is thus relevant in the Cloud Tier.

7.5 Cloud detection & response (Cloud DR) orchestration for multiple clouds

Attackers are starting to leverage automation, for example, with stolen credentials in criminal purposes such as crypto-currency mining and stealing sensitive information. In future, it is not enough to separately manage each platform and data source. Contextuality and data fusion will be crucial to recognize the criminal activities in future.

Following attackers with Cloud Detection & Response (Cloud DR) orchestration for multiple clouds is a next-generation and high-level concept for detecting security exceptions in cloud environments and digital platforms. Cloud DR extends UEBA to cover different cloud systems and extends the detection & response paradigm.

Figure 36 introduces an inspirational architecture for installing a cloud sensor in customer AWS infrastructure. We have started to generate the architecture in a single cloud service. The next step is to extend this architecture to cover multiple clouds.

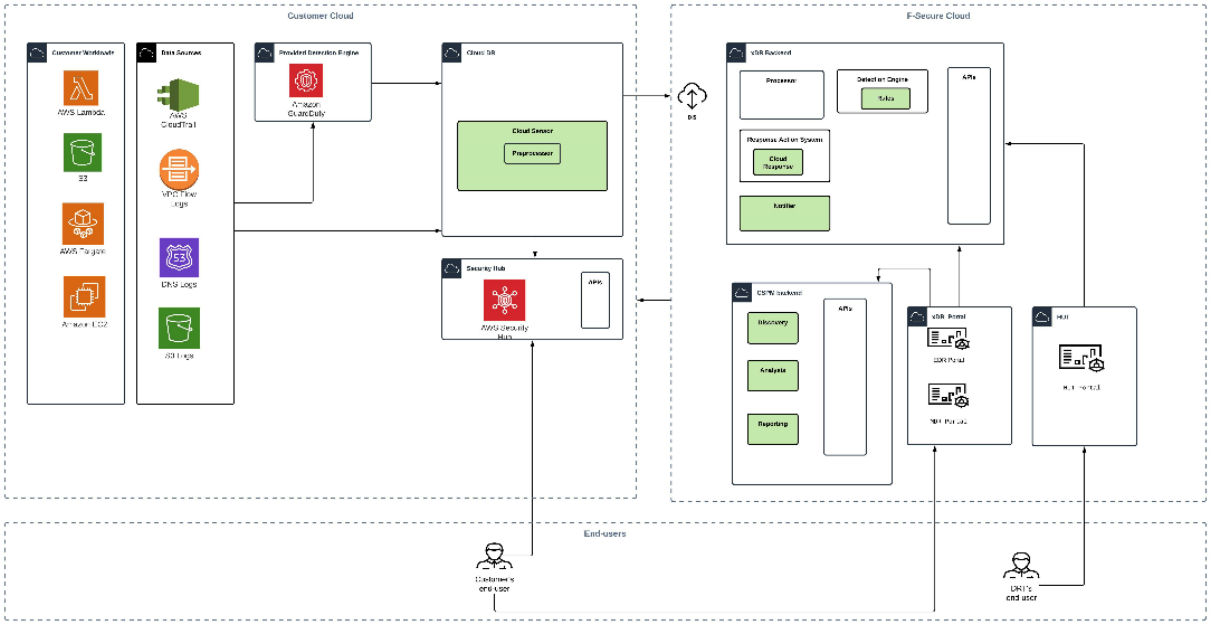

Figure 36: An illustration of Cloud DR in AWS infrastructure.

7.5.1 Fit with concept TRANSACT reference architecture/components

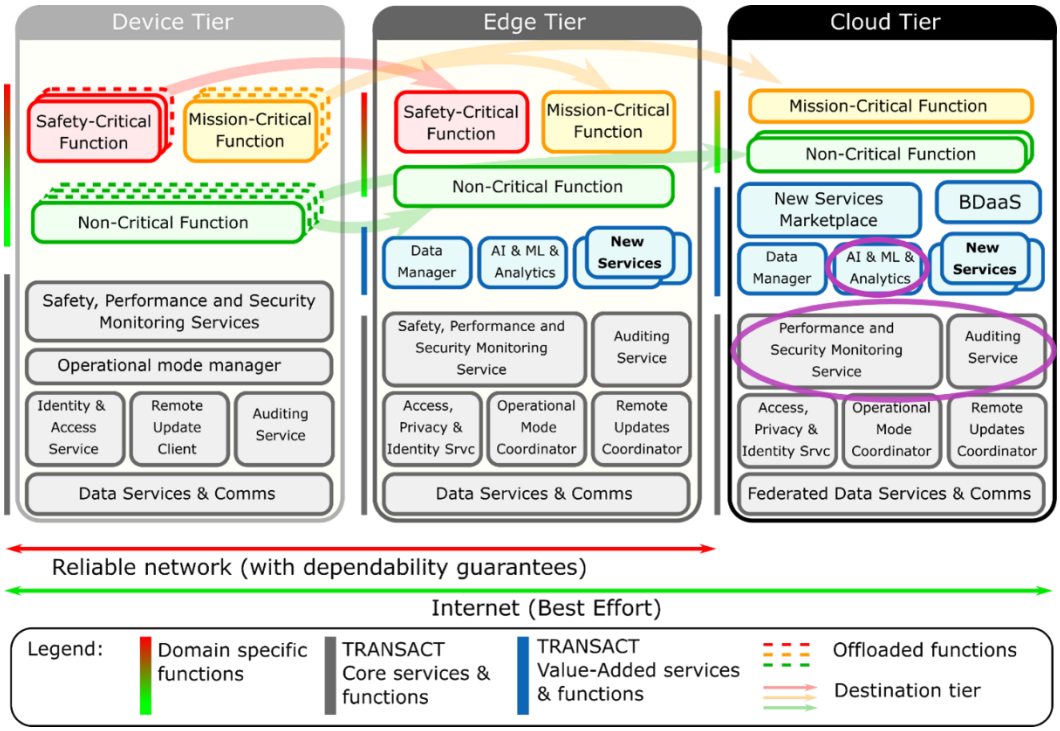

Figure 37: Cloud DR applicability with TRANSACT reference architecture

7.5.2 Security Risk/ Threats

As already explained in the overview section, the stolen credentials provide a major risk for the users of cloud infrastructure. A role of Cloud DR is to detect such incidents.

7.5.3 Generic Security Requirements

While Cloud DR is a powerful technology to detect malicious incidents in cloud infrastructure, it involves insider threats. In other words, security response actions can be also to criminal activities. This is a generic security requirement for any security technology that has the permissions to operate inside the customers' cloud infrastructure.

7.5.4 Phase Considerations:

Cloud Detection & Response is applicable in development, deployment, operation, and maintenance phases.

7.5.5 Participating Components/ Entity

Cloud Detection & Response monitors events happening in customers' cloud infrastructure and is thus relevant in the Cloud Tier.

8 Security and privacy concepts for domain specific functions

8.1 Safety and privacy of off-the-shelf components, including MQTT, non-doubled 4G networks, open IP networks, Unity3D

8.1.1 Overview

Off-the-shelf components, or commercially available off-the-shelf (COTS) products are ready-made hardware or software, which are then adapted to the needs of the purchasing organization. Such products may offer significant savings in procurement, development, and maintenance when compared to a custom-made solution developed in-house specifically for intended purpose.

COTS can provide increased reliability and quality over custom-built software as these are developed by specialists within the industry and are validated by various independent organizations, often over an extended period of time. Although COTS products can often be used out of the box, in practice the COTS product must be configured to achieve the needs of the business and integrated to existing organizational systems.

Extending the functionality of COTS products via custom development is also an option, however this decision should be carefully considered due to the long-term support and maintenance implications. Such customized functionality is not supported by the COTS vendor, so brings its own sets of issues when upgrading the COTS product. COTS trade-offs include an increase in software component-integration work, dependency on the vendor, security issues and incompatibilities from future changes (McKinney, August, 2001).

Out of all possible COTS products, we are focusing on selected items for closer inspection for their relevance:

MQTT: MQTT (Message Queue Telemetry Transport), is a simple protocol designed for devices with low processing power.

Non-doubled 4G network: LTE internet from commercial service providers without secondary connection for situations where 4G reception is low or temporarily unavailable.

Open IP network: Connection happens from endpoint-to-endpoint over public internet IP address pool instead of completely isolated network setup.

Unity3D: Unity is a cross-platform game engine developed by Unity Technologies. The engine is able to create three-dimensional, two-dimensional, virtual reality, and augmented reality games, as well as simulations and other experiences. In UC1, Unity is used as software to run Fleet Management Application (FMA). FMA has digital twin of the operating environment and vehicles. It allows remote operating controls and mission execution for vehicles. If attacker gains access to FMA, it poses serious security risk for safety.

8.1.2 Fit with concept TRANSACT reference architecture/components

In TRANSACT reference architecture, safety and privacy of selected off-the-shelf components apply to Mission-Critical Function and Non-Critical Function segments in Cloud Tier. Off-the-shelf components can be used in Device and Edge tiers, but safety and privacy become major concern when open IP networks cloud access to components is possible.

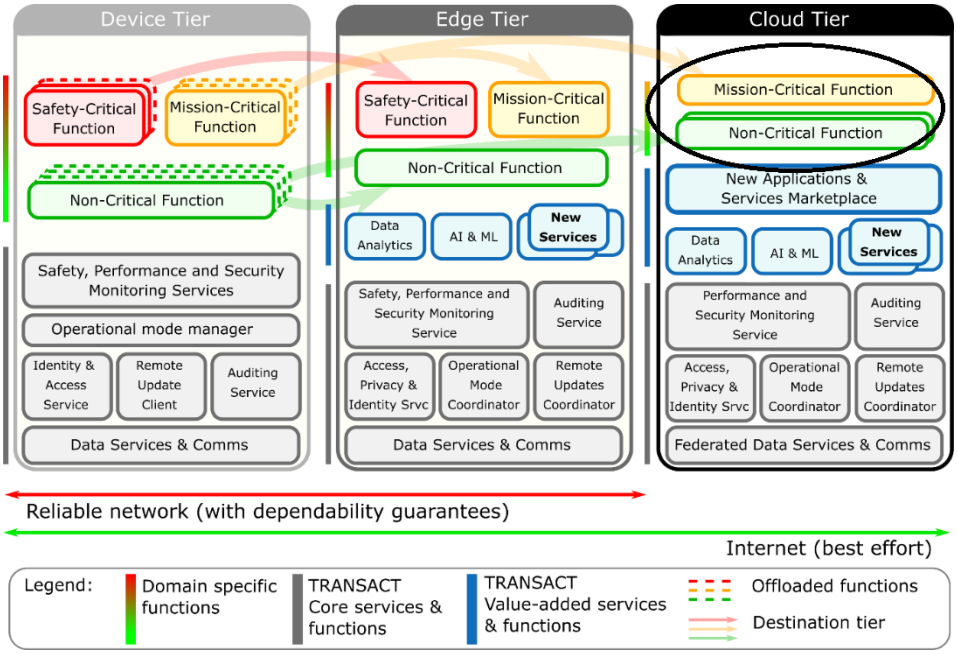

Figure 38: Applicability of off-the-shelf components in the cloud tier

8.1.3 Security risk/ threats

MQTT: By default, MQTT protocol tries to minimize the processing needed to exchange messages, which means that serious security problems arise. Most of these shortcomings can be solved with an adequate protocol configuration (Santiago Hernández Ramos, 2018).

MQTT messaging out-of-the-box is not secured in any way. Any connected MQTT client can listen to all data traffic that goes through MQTT server, and clients can freely send messages to each other. Clients can connect without authentication. Extra attention needs to be directed towards validity of client credentials when establishing MQTT connection. It is necessary to apply proper security settings before MQTT meets criteria for safety and privacy.

Open IP networks: Open IP network endpoint is vulnerable to attacks on a network router level. Firewall settings are necessary

Non-doubled 4G network: non-doubled 4G connection has the same limitations for safety and privacy as public networking has. If operations are done in area with high use of 4G network (for example large gathering of people), it can limit or prevent reception of wireless 4G connection and add major latency to data traffic.

Unity3D: Unity itself does not provide security or authentication tools out-of-the-box. Games industry has traditionally relied on custom-built security and authentication solutions or delegated authentication from other products. Security measurements are added as needed on a project-per-project basis.

Unity supports Transport Layer Security (TLS) version 1.2, but not the currently recommended TLS 1.3. This sets a limitation for all MQTT clients to use TLS 1.2 when FMA is one of the connected clients. TLS1.3 is a security update response to various vulnerabilities (Y. Sheffer, 2015) found in TLS1.2.

8.1.4 Generic security requirements

Using off-the-shelf components in TRANSACT context requires adding security layers and user authentication to. Off-the-shelf components might have customer-grade security and privacy measures applied to them, but in many cases that might not be the case.

MQTT: Well-secured MQTT network has MQTT server configuration that requires clients to provide username, password, and valid certificate for connection. Data transfer happens over encrypted protocol layer (TLS1.2 for example).

For safety MQTT messages have Quality of Service (QOS) feature, which should be used to ensure delivery of mission critical messages in situations where network connectivity is unreliable. Such messages include infrequently sent control commands i.e., new mission route, start/stop engine, request transfer of control. QOS works as an additional layer to ensured message delivery (TCP protocol being primary method).

- QOS level 0 (at most once), a message is sent without checking if anyone received it. Rapid pace, quickly outdated telemetry and remote-control commands are sent with this QOS.
- QOS level 1 (at least once) means each recipient has to acknowledge receiving the message by sending back acknowledgement message. If no acknowledge message is received, message is sent again to the recipient.
- QOS level 2 (exactly once), MQTT protocol uses back-and-forth message acknowledgements to make sure message is received and both MQTT server and client have confirmed to each other their knowledge of successful message delivery.

Unity: FMA with digital twin is expected to be running on a computer with access only to those who have authenticated to the computer with sufficient user account credentials. Same applies to remote operators as the level of control over FMA is the same for them.

Non-doubled 4G networks: When using off-the-shelf non-doubled 4G networks, it is important that any data transmitted over the network is encrypted. Virtual Private Networking (VPN) provide that encryption in addition of creating a device-to-device private network. Firewalls at each endpoint only need to allow one VPN port to be accessible from outside, rather than multiple ports to handle software connections.

Open IP endpoint: Proper security settings for router & firewall should be applied. Security updates should be applied.

8.1.5 Phase considerations

Applies to phases: design, development, deployment, operation, maintenance

8.1.6 Participate components/ entity

Off-the-shelf components are used in Mission-Critical and Non-critical Functions.

8.1.7 Example in context of a Use case

Use Case: Remote operation of autonomous vehicles navigating in urban environments

Applicability: In UC1, vehicle uses off-the-shelf components (NetGear, Mobile Router, Internet Provider) to connect to the public IP address of Fleetonomy Office router. Router firewall allows vehicle to establish a Virtual Private Network connection with Fleetonomy server using authentication credentials.

After secure VPN connection is established, MQTT messaging connection is initiated using additional security of username/password, certificate file and encrypted data connection. Any control commands sent to vehicle with MQTT messages is therefore double secured. Additional measures for safety include MQTT QOS settings to ensure important messages are delivered with multiple attempts if network connection for initial delivery attempt has not succeeded.

8.1.8 Challenge for application within TRANSACT context

For remote operation in Distributed CPS, the main challenge is to define which off-the-shelf components are safe to use. Adding security layers to them is the main tool for increasing overall safety. Knowing what kind of security configuration is the least vulnerable to attacks requires up-to-date knowledge of security systems and the extent they apply to the choice of off-the-self components.

9 Application specific security and privacy concepts

9.1 Security and privacy concepts for secure remote driving operation

The operational context of the targeted use case is visualized in the Figure 39. The aim of the case is to drive Aune, autonomous electric shuttle bus in urban area, under control of a remote driver. The case has already been described in D1.1, and related requirements has been described in the D1.2. This contribution has taken these descriptions and requirements as the input, and focused especially on analysis security, privacy and trust requirements related to remote driving operation.

Figure 39: VTT's autonomous shuttle bus AUNE operating in manual mode in Hervanta, Tampere in early 2021.

Thus, the purpose of this section is first to analyse the critical elements related security, privacy, and trust of the targeted cyber-physical system, then analyse the potential threats and the security, privacy and trust requirements of the remote driving operation. And finally, to discuss on proceeding towards security, privacy and trust traceability and control concepts.

The analysis of critical elements includes identification of the *main actors*, physical systems related *assets* such as critical physical entity, information, or functional operation. The critical *interactions* including data exchanges are analysed to detect potential *risks, problems and challenges* for security, privacy and trust. These aspects are then used for detecting *potential threats* that may occur in remote driving operation. All these aspects are summarized in the form of *security, privacy and trust requirements* that are relevant for realizing the remote driving operation. After that, finally the security practises of ETSI and NIST relations to remote driving system operations are analysed.

9.1.1 Analysis of critical elements

The remote driving system has 13 different kinds of actors (mission planner, ground crew member, road user, remote driver, backup remote driver, in-vehicle safety supervisor, IT/Traffic security manager, passenger, autonomous vehicle, traffic assets (-signs, -lights, cameras) provider/services provider, city traffic service provider, authorities). In addition, there are at least 14 critical physical assets related to information, operation and devices that may/or may not be critical for the operation when system elements are interacting with each other.

9.1.2 Analysis of security risks and threats

9.1.2.1 Risks, problems, and challenges

The remote driving case includes serious risks for safety. For example, there is a risk that some external stakeholder (e.g. cyber attacker) is able to attack against the targeted system, such as e.g. make remote driving control action(s) which may trigger or lead to accident/terroristic attack with loss of human life and damages in traffic/infrastructure of urban areas; steal the vehicle and use it for the external stakeholder own actions which are against the interests of the owner of the vehicle and related service provider(s); mislead the remote driver or the positioning / route following / situational awareness subsystems of the autonomous vehicle to make wrong decisions by providing wrong/misleading information, which results an accident with potentially loss of human life's and damages in traffic/infrastructure of urban areas; expose privacy sensitive information from the system and misuse it for some purposes without the permission from the owner against GDPR regulations.

These are only examples of the risks that can be serious for the safety of the remote driving. There are several other risk areas such as e.g., possibility for erroneous operation within the autonomous vehicle. For example, there can be error in positioning of the autonomous vehicle, error in steer control actuator system, or error in break control system. In addition, there are risks arising from the stakeholders' mistakes, there may be errors in the communication channels, unexpected situations in the surrounding of a vehicle may lead to erroneous actions, and attacker may trigger some surrounding entity to work in malicious manner.

9.1.2.2 Threats in remote driving operation

The detailed threat analysis revealed 30 potential threats related to the identified actors, physical systems related assets or operation, which consequences were estimated to compromise security, privacy and or trust related issues leading to potential safety problems in the remote driving case.

9.1.3 Security and privacy requirements

In this part, application-specific security and privacy concepts are highlighted. The security requirements are similar to the D1.2; however, they are presented in a more detailed description corresponding to the security and privacy concepts and mapped with standard security practices.

Table 2. An analysis of requirements for security, privacy, and trust in the remote driving operation.

ReqID	UC1-sec-1.1
Short name	Trusted mission plan.
Category	Trust
Link to UC1 requirements	EUR-ID-1 Mission planning of the vehicles
Requirement	Source/sender of the mission plan must be trusted. It must be verified that plan is sent by real mission planner and that the plan is not modified.
Justification	Autonomous vehicle is not misused.
Threats	T1.1

ReqID	UC1-sec-1.2
Short name	Safe mission plan.
Category	Privacy
Link to UC1 requirements	EUR-ID-1 Mission planning of the vehicles
Requirement	Mission plan must be stored encrypted and can be updated only by trusted source.
Justification	Autonomous vehicle is not used for illegal purposes.
Threats	T1.2

ReqID	UC1-sec-4.1
Short name	Safe autonomous driving.
Category	Safety
Link to UC1 requirements	EUR ID 4: Autonomous driving of the fleet
Requirement	Autonomous vehicle must be able to drive safely. Note, there are some restrictions: Some physical attacks are excluded from this service e.g. “running fast in front of the vehicle”
Justification	Safe autonomous driving.
Threats	T4.3

ReqID	UC1-sec-4.2
Short name	Trusted input information for autonomous driving.
Category	Trust
Link to UC1 requirements	EUR ID 4: Autonomous driving of the fleet
Requirement	Information on presence, location and mobility of humans/animals/artificial entities on the road must be trusted. It must be verified that input information is sent by real entities and the information is not modified.
Justification	Fraud information is not sent to the system.
Threats	T4.2

ReqID	UC1-sec-4.3

Short name	Input information location for autonomous driving.
Category	Safety
Link to UC1 requirements	EUR ID 4: Autonomous driving of the fleet
Requirement	Location of input information must match location of the vehicle.
Justification	Safe autonomous driving.
Threats	T4.2

ReqID	UC1-sec-5.1
Short name	Safe emergency reasoning results for autonomous driving.
Category	Safety
Link to UC1 requirements	EUR ID 4: Autonomous driving of the fleet
Requirement	The results of the emergency reasoning based on vehicle situation information must be kept safe. Manipulating the results may cause wrong emergency operations.
Justification	Emergency stops and vehicle pullovers are performed as they should.
Threats	T5.2

ReqID	UC1-sec-6.1
Short name	Trusted vehicle information for remote driver
Category	Trust
Link to UC1 requirements	EUR ID 5: Remote driving of a vehicle
Requirement	Vehicle information for remove driver must be trusted. It must be verified that vehicle information is sent by real vehicle and that the information is not modified.
Justification	Remote driver gets correct information from the vehicle.
Threats	T6.2

ReqID	UC1-sec-6.2
Short name	Real-time vehicle information for remote driver

Category	Safety
Link to UC1 requirements	EUR ID 5: Remote driving of a vehicle
Requirement	Vehicle information for remove driver must be real-time i.e., delay must be below defined threshold (ms/sec). Otherwise, remote driver can do fatal remote driving operations. This can be checked for example by timestamps.
Justification	Remote driver gets correct information from the vehicle.
Threats	T6.2

ReqID	UC1-sec-6.3
Short name	Trusted remote driver commands to vehicle.
Category	Trust
Link to UC1 requirements	EUR ID 5: Remote driving of a vehicle
Requirement	Information from remote driver to vehicle must be trusted. It must be verified that information is sent by real remote driver and that the information is not modified.
Justification	Vehicle gets correct information from remote driver.
Threats	T6.4

ReqID	UC1-sec-6.4
Short name	Real-time remote driver commands to vehicle.
Category	Safety
Link to UC1 requirements	EUR ID 5: Remote driving of a vehicle
Requirement	Information from remote driver to vehicle must be real-time. This can be checked for example by timestamps.
Justification	Vehicle gets correct information from remote driver.
Threats	T6.4

ReqID	UC1-sec-7.1

Short name	Secure operating systems.
Category	Security
Link to UC1 requirements	EUR ID 4: Autonomous driving of the fleet EUR ID 5: Remote driving of a vehicle
Requirement	Operating systems of all system components must be kept up to date. Use firewalls and antivirus software. Use complex passcodes and passwords. Use secure networks. Check router security, which can be low by default. See also table in Chapter 6.8.1
Justification	Emphasize system confidentiality.
Threats	

ReqID	UC1-sec-7.2
Short name	Secure communications.
Category	Security
Link to UC1 requirements	EUR ID 4: Autonomous driving of the fleet EUR ID 5: Remote driving of a vehicle
Requirement	Communication between all the components of the system should be secure. Use secure communication protocols (HTTPS, SSH, SFTP, FTPS), encryption. Protect cryptographic keys for example using subsystem isolation.
Justification	Emphasize system confidentiality.
Threats	

ReqID	UC1-sec-7.3
Short name	Traceability.
Category	Safety
Link to UC1 requirements	EUR ID 4: Autonomous driving of the fleet EUR ID 5: Remote driving of a vehicle
Requirement	System must be traceable. It makes it possible to analyse reasons for problems which is increasing the system safety in the future.
Justification	To be able analyse what happened in dangerous situation or accident. Developing system safety.
Threats	

9.1.3.1 Mapping security practices in ETSI EN 303 645 to Remote driving use case

The following table maps the security practices in ETSI EN 303 645 and describes how they are applied and planned to be applied in remote driving use case:

Requirements	Applicability in UC1 remote driving	Notes/constraints from UC1 remote driving
No universal default passwords	Yes	This is applicable, because the scenario involves systems that may need authentication either by systems or users. The use of the system can be done remotely, so this relates to communications security. The requirement is addressed by not using system default passwords and the access control system need to generate unique access tokens for each use.
Monitor for vulnerabilities in used technologies and solutions	Yes	The system parts need to make perception, comprehension, and projection for the situation awareness. Such perception refers to monitoring, and vulnerabilities need to be included on comprehension and projection too.
Keep software updated	Yes	The system components are designed to be updateable quickly from the development perspective and easily from the deployment perspective. From the communications security perspective, the system will have support for remote updates to be able to address communication security vulnerabilities and allow e.g. crypto agility in the system.
Securely store credentials and security-sensitive data	Yes	The requirement for trustworthiness is that generated access tokens are encrypted in mobile endpoints with the secure storage backed keys. On the server side components, the security of the credentials is to be implemented with at least one of the following mechanisms: SELinux backed isolation or with transparent data-at-rest protection.
Communicate securely	Yes	TLS v1.3 and/or IPsec (with IKEv2) are used for data-in-transit encryption. The sessions are mutually authenticated (with X509v3 certificates or raw public keys).
Minimize exposed attack surfaces	Yes	The proxy server exposes only the network ports that are mandatory for operations.

		From the mobile entities perspective, the "Securely store credentials and security-sensitive data" requirement mandates that sensitive data is stored in an encrypted format and thereby protected against device loss or theft.
Ensure software integrity	Yes	It is important to take care of the integrity of the software packages.
Ensure that personal data is protected	Yes	All the data that may be connected with persons on streets or autonomous vehicles need to be protected.
Make systems resilient to outages	Yes	Outages, disruptions, malfunction must not expose the communications interfaces in insecure manner and the security controls must be such that they cannot be bypassed even during outages.
Examine system telemetry data	Yes	May be relevant as a mechanism for detecting cyber-attacks.
Make it easy for users to delete personal data	Yes/No	If the persons related data is stored, then the users shall be able to control it.
Make installation and maintenance of devices easy	Yes/No	The installation must be carried out in secure manner. Furthermore, the installation must not be more complicated with recommended security settings.
Validate input data	Yes	Input data validation must be applied to prevent malformed or malicious data being inserted to the system through the communication channels. Exposed network interfaces must employ validation (in addition to encryption and authentication of the communications channel)

Table 3: Security practices in ETSI EN 303 645 and describes how they are applied and planned to be applied in remote driving use case

9.1.3.2 Mapping security practises in NIST SP800-53 to Remote driving use case

The following table maps the security practices in NIST SP800-53 and describes how they are applied and planned to be applied in remote driving use case:

Security Control	Control enhancement	Applicability in remote driving use case	Notes/constraints from remote driving use case
SC-5-1	DENIAL-OF-SERVICE PROTECTION | RESTRICT ABILITY TO ATTACK OTHER SYSTEMS	Yes	Different servers/services within the scenario only expose the interfaces relevant for the scenario's operations.

			All inter-server communication is authenticated.
SC-5-2	DENIAL-OF-SERVICE PROTECTION | CAPACITY, BANDWIDTH, AND REDUNDANCY	Yes	This is a general IT system design requirement.
SC-5-3	DENIAL-OF-SERVICE PROTECTION | DETECTION AND MONITORING	Yes	The servers must have capabilities to detect potentially hostile behaviour and be able to distinguish such behaviour of normal operations. The capability to intrinsically implement detection features decreases reliance on external monitoring systems and thereby contributes to the trustworthiness of the remote driving scenario.
SC-7-3	BOUNDARY PROTECTION | ACCESS POINTS	Yes	See “Minimize exposed attack surfaces”
SC-7-4	BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES	Yes	See “Minimize exposed attack surfaces”
SC-7-5	BOUNDARY PROTECTION | DENY BY DEFAULT — ALLOW BY EXCEPTION	Yes	See “Minimize exposed attack surfaces”
SC-7-7	BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES	No	
SC-7-8	BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS	Yes	This needs to be the functionality of the servers designed for this UC.
SC-7-9	BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC	Yes	This needs to be the functionality of the servers designed for this UC.
SC-7-10	BOUNDARY PROTECTION | PREVENT EXFILTRATION	Yes	This needs to be the functionality of the servers designed for this UC.
SC-7-11	BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC	Yes	This needs to be the functionality of the servers designed for this UC.
SC-7-12	BOUNDARY PROTECTION | HOST-BASED PROTECTION	No	
SC-7-13	BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS	No	

SC-7-14	BOUNDARY PROTECTION | PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS	No	
SC-7-15	BOUNDARY PROTECTION | NETWORKED PRIVILEGED ACCESSES	Yes	The proxy server implements enforcing the privileged access and performs the narrowing of the access for the data that passes through the proxy.
SC-7-16	BOUNDARY PROTECTION | PREVENT DISCOVERY OF SYSTEM COMPONENTS	No	
SC-7-17	BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS	Yes	The servers need to perform protocol formatting.
SC-7-18	BOUNDARY PROTECTION | FAIL SECURE	Yes	The servers need to fail secure and prevent access in case of failures.
SC-7-19	BOUNDARY PROTECTION | BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS	No	
SC-7-20	BOUNDARY PROTECTION | DYNAMIC ISOLATION AND SEGREGATION	Yes	
SC-7-21	BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS	No	
SC-7-22	BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS	Yes	
SC-7-23	BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE	Yes	
SC-7-24	BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION	Yes	
SC-7-25	BOUNDARY PROTECTION | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	No	The remote driving scenario does not connect to such systems.
SC-7-26	BOUNDARY PROTECTION | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	No	The remote driving scenario does not connect to such systems.

SC-7-27	BOUNDARY PROTECTION | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	No	The remote driving scenario does not connect to such systems.
SC-7-28	BOUNDARY PROTECTION | CONNECTIONS TO PUBLIC NETWORKS	Yes	
SC-7-29	BOUNDARY PROTECTION | SEPARATE SUBNETS TO ISOLATE FUNCTIONS	Yes	

Table 4: Security practises in NIST SP800-53 to Remote driving use case

9.1.4 Security, privacy and trust traceability and control concept for remote driving

The analysis of the critical elements, actors, physical entities, information/functional operation, and critical interactions including data exchanges revealed serious risks, problems and challenges for security, privacy, and trust in the remote driving operation. There are huge number of potential threats against the safety of the operation. The described security, privacy and trust requirements are basically only snapshots of the wide set of the requirements that trustworthy operations on streets demand in reality.

In the next step of this research, the aim is to proceed towards the security, privacy and trust traceability and control concepts that could support the remote driving of autonomous vehicles in urban context at least in some extent. Especially, the application of wireless communication channels in dynamic urban context where multiple stakeholders are present in mobile way, makes the case very demanding. In addition, there are high variety of road users, human (including VRUs) and non-human, multiple different kinds of IoT assets and their service providers' systems.

When comparing the analysed requirements, it can be estimated that the targeted concepts are related quite much to the potential architectural patterns e.g., to accountability, identity and access control, and data confidentiality/integrity/availability visualized in the Figure 40. The plan is to continue this research by focusing into targeted security, privacy and trust traceability and control concept(s) during the rest of task 3.2 and especially in task 3.4 so that the key resulting contributions will be described in D3.4.

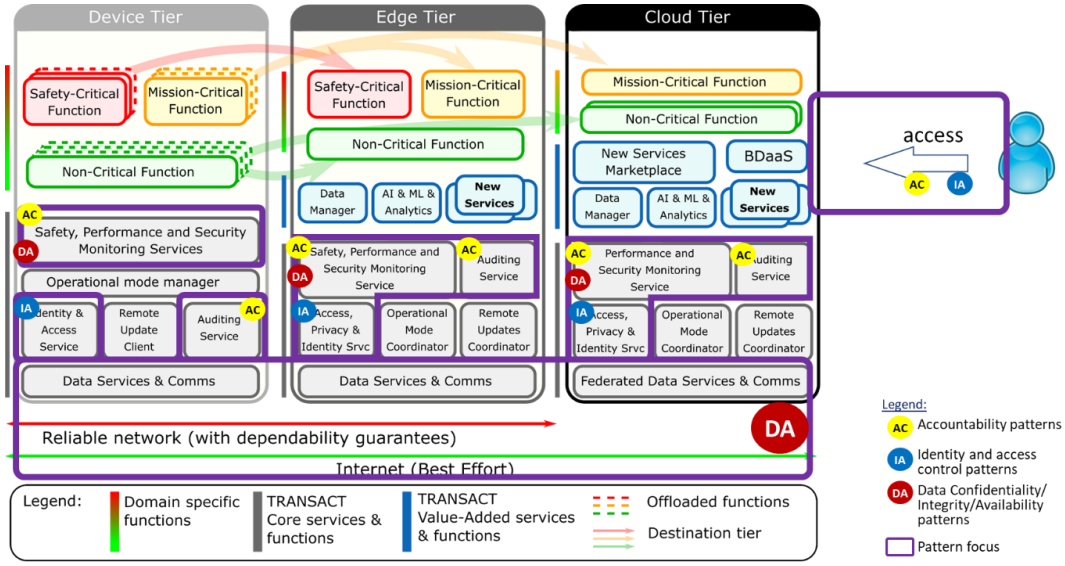

Figure 40. Targeted areas of the security, privacy and trust traceability and control concepts in the Transact architecture.

9.2 Security and privacy requirements and patterns for the healthcare DICOM data and applications

9.2.1 Overview

By moving safety-critical CPS architecture away from the centralized, on-device solution toward the distributed, cloud-based architecture significantly increases the attack surface of the new solution by making it more vulnerable for security attacks. Also, the data privacy concerns are growing significantly in such architecture as the user data, especially in automotive and healthcare domains, is highly sensitive and require special care not to be exposed due to being transfer over a public network or due to security attacks and software vulnerabilities.

The edge/cloud-based healthcare systems architectures should be designed such that the risks of security breaches and privacy violations are minimized. High level security and privacy requirements for healthcare (or other domains handling sensitive data) helps to focus the system design on relevant aspects to be addressed to provide sufficient security and privacy measures. This section presents high level security and privacy requirements and their impact on the TRANSACT architecture components.

9.2.2 Fit with concept TRANSACT reference architecture/components

Successful edge-cloud-based safety critical (healthcare) system has to address end-to-end security and privacy. Specifically, it needs to apply the security mechanisms to safeguard the regulatory requirements and prevent disclosure, compromise, or misuse the processed (healthcare) data. The TRANSACT's components implementing security and privacy related functionality need to be designed with security and privacy in-depth approaches to ensure adequate quality and protection of the processed data. The TRANSACT's components primarily impacted by the security and privacy functions are (also marked in Figure 41)

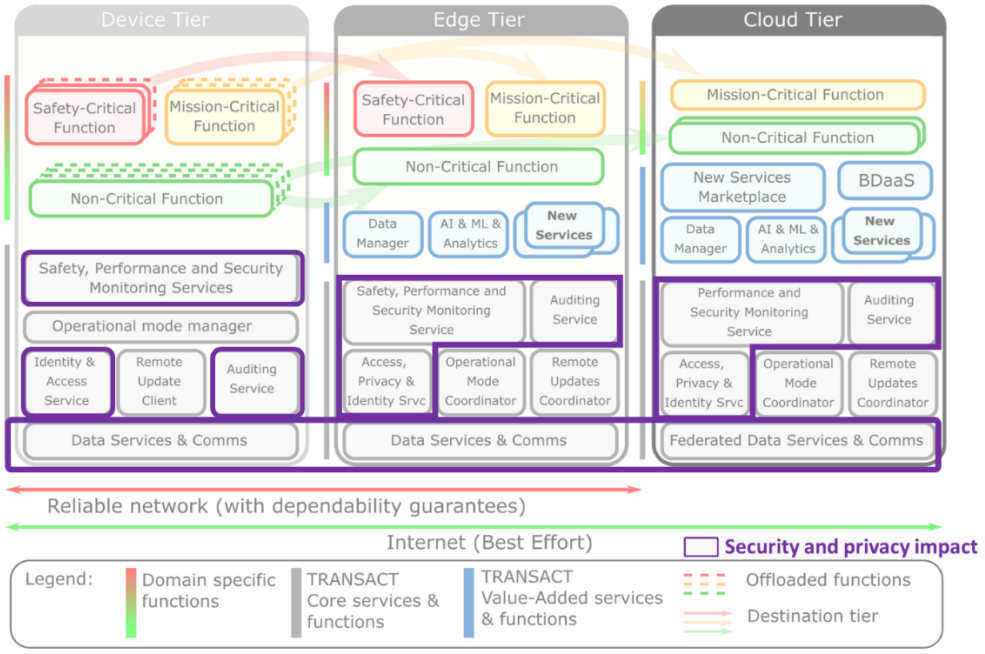

Figure 41: The security and privacy impact on the TRANSACT reference architecture.

- **Security monitoring services:** ensure monitoring and early detection of (data) security incidents.
- **Identity and access services:** responsible for granting/denying access to the system resources based on the policies defining who has what access (in which role) to the data and the services.
- **Auditing services:** collect information about accessing and using the system to help detecting the security policy violations (e.g., when the system is accessed by unauthorized users or in an unauthorized way) and provide information to comply with the required regulations.
- **Data Services and Communication services:** help in efficient and secured data handling, both, in transit and at rest.

9.2.3 Security and privacy requirements

9.2.3.1 Data confidentiality/integrity/availability (CIA)

The CIA triad ensures protection of the system managed data and its resources. *Confidentiality controls* ensure that only the right/authorized users/services can use the system and its data, while prevents sensitive information from reaching wrong/unauthorized users/services. *Integrity controls* ensure consistency, accuracy, and trustworthiness of data. *Availability controls* ensure that system data and resources are available to authorized users when need.

The high-level requirements for data confidentiality/integrity/availability are:

- **Secure-Data-Handling:** system shall guarantee that data may not get tampered and must be complete and correct
- **Secure-Data-Handling-at-Rest:** system shall guarantee that data cannot be interpretable when stored (at rest), covering: (edge/cloud) data storage services, file systems, and any storage solution used.
- **Secure-Data-Handling-in-Transit:** system shall guarantee that data cannot be interpretable in transit, i.e., the network transmission is encrypted to ensure confidentiality and integrity.
- **Secure-Data-Handling-Cryptography:** use state of the art cryptography solutions to encrypt data in-transit and at-rest.
- **Secure-Application-and-Services-Handling:** system shall ensure application and service integrity and secure execution so they cannot be tempered with, including the result of their processing. In healthcare domain failing to meet this requirement can result in misdiagnosis of patient state.
- **Security-Tenant-Isolation:** system shall guarantee strict separation of the tenants so it is not possible to steal or modify an execution environment state (e.g., in virtual machine, container) or data from the other tenants.

9.2.3.2 Identity and access control

The identity and access controls provide critical mechanisms for the data protection, such as user authentication, authorization, and role-based access control.

The high-level requirements for *identity and access control* are:

- **Secure-Resources-Access:** system shall ensure access to the system resources only for the authenticated user.
- **Secure-Resources-Authorized-Access:** system shall ensure access to the data and resources only in the scope of the granted permissions defined for the user or other services.

9.2.3.3 Accountability

Accountability serves two main purposes: to provide information about user activities in relation to the data (e.g., who accessed the data, when, and what action performed), and information helping to identify potential security incidents (that may impact the data). The accountability is critical to meet the (healthcare) regulatory requirements.

The high-level requirements for *accountability* are:

- **System-Audit:** System shall support auditing to monitor access to personal data and system usage.
- **System-Audit-in-Healthcare:** Auditing shall be defined in accordance with Audit Trail and Node Authentication (ATNA) Profile [ATNA (International)].
- **System-Audit-Integrity:** The audit data shall be secured to ensure their integrity after creation.
- **Security-Monitoring:** system shall provide logging information of access to the storage, data migration, data backup, and related activities.
- **Security-Monitoring-Incident-Alerting:** system shall be able to monitor and react to security incidents/events (e.g., by sending alerts). The monitoring should scan critical activities and to log scanning and probing activities, or patterns that appear to be attempts at unauthorized access to the services and/or data.

9.2.3.4 Processes and framework

Next to the technical security controls, it is critical to employ the relevant security processes and frameworks during system development to ensure secure system design and its release in the edge/cloud deployment.

The high-level requirements for *processes and framework* are:

- **Privacy-Information-Handling-by-Product:** system shall ensure that all privacy-sensitive information (e.g. patient name, date of birth, physician, etc.) is not exposed (e.g., via logging).
- **System-Security-by-Design:** system shall be designed by following the best security practices and realizes “defence in depth” approach which does not rely on a one single security control but places security controls at various levels, ranging from the application security, computing security, data security, information security, network security, to the administrative and operational safeguards. (IEC 80001-1:2010, ISO 27001/27002/27018 and NIST SP 800-53).
- **Establish-Secure-Defaults:** applicable security features shall be enabled by default throughout the system.
- **System-Security-Updates:** shall ensure means for proper security patch management to ensure quick actions against any security breaches without jeopardizing any security and privacy domain rules.
- **Secure-DICOM-Data-Processing** (DICOM Standards Committee, 2022)**:** DICOM Part 15 “Security and System Management Profiles” [DICOM] should be used for interoperable secure implementation of DICOM data exchange and ensure proper handling of privacy-sensitive DICOM attributes.

9.2.3.5 Generic privacy requirements

Since healthcare data is very sensitive data it is paramount to ensure proper handling, processing, storage, and usage of such data.

The high-level requirements for *healthcare data privacy* are:

- **Applicable-Privacy-Data-Protection-Regulations:** system shall ensure storage and processing the data accordance with the applicable laws, i.e., national laws, privacy and data protection laws (such as GDPR (EU, 2016) or HIPAA (HIPPA)), or domain specific regulations (e.g., in healthcare: IHE Audit Trail and Node Authentication (ATNA) profile (ATNA, 2021).

- **Data-Localization:** the system shall ensure that the correct handling of (country/region) location constrains imposed by the handled (healthcare/personal) data. The same location guarantees shall apply to storing data and to processing/accessing data. This requirement is typically imposed by: local laws, privacy and data protection laws (such as the GDPR or HIPAA), or the healthcare organization using the system.
- **System-Adequate-Data-Privacy-Protection:** the system shall ensure technical and organizational measures to protect the data and enable compliance with legal requirements (e.g., pseudonymization, sensitive data to be kept in a separate database, services to be provided from within the Customer's group of companies by means of seconded personnel). The used solutions and platform should ensure realization legal requirements around data (e.g., GDPR (GDPR, 2018), HIPAA (HIPPA)).
- **System-Privacy-by-Design:** system shall embed privacy and data protection controls throughout the entire development lifecycle, from the system design to system deployment, when collecting and using the data, till ultimate data disposal. This also involves having data privacy experts to assess risk of bridging data protection throughout the entire development lifecycle.
- **Data-Protection-Impact-Assessment (DPIA):** it is an activity required by GDPR regulation and it aims to detail the nature and extent of personal information processing and provides means for determining the best way to manage significant risks and protect individuals' privacy. DPIA should be integral part of System-Privacy-by-Design approach so that all services and their capabilities that process personal information are subject to the DPIA process.

9.2.3.6 Security Patterns

Due to CPS inherent complexity and safety nature using the security and privacy pattern during the system development can strengthen the core security principles around user/patient data confidentiality, integrity, and availability. In addition, they can also improve handling of user identity, services and data access control, and accountability for the performed actions on the system. There are broad set of the security and privacy patterns that support requirements presented in Section 9.2.2 and Section 9.2.3.5—majority of those are presented in [D2.1].

9.2.4 Phase considerations

Phases: design, development, deployment, operation, maintenance, decommission.

9.2.5 Participate components/ entity

The impacted components of the TRANSACT's architecture are presented in Figure 40 (see Section 9.2.2).

9.2.6 Example in context of a Use case

Use Case 4: Edge-cloud-based clinical applications platform for Image Guided Therapy and diagnostic imaging systems.

Applicability: Any system processing healthcare data requires to fulfil the healthcare regulation on personal data privacy rules such as General Data Protection Regulation in Europe, or Health Insurance Portability and Accountability Act [HIPAA] in United States. When considering cloud-based solution in healthcare context the patient data security and privacy are the critical aspects to consider.

9.2.7 Challenge for application within TRANSACT context

While extending the local, on-device safety critical healthcare systems to the edge-cloud continuum it is paramount to ensure patient data security and privacy. The TRANSACT's components implementing security and privacy related functionality need to be design with security and privacy in-depth approaches to ensure

adequate quality and protection of the processed data. The security and privacy measures designed into the system and its environment should prevent unprivileged access to data, not only during processing, but also while data is at rest regarding defined policies. Therefore, successful edge-cloud-based safety critical (healthcare) system must address end-to-end security and privacy, i.e., it needs to apply the security mechanisms ensuring proper safeguards to comply with the regulatory requirements and preventing disclosure, compromise, or misuse the stored and processed (healthcare) data.

In the context of the TRANSACT project the impact on data security and privacy of the on-device safety critical system when deployed in the device-edge-cloud continuum needs to be evaluated. Which security and privacy patterns are applicable and are the most effective?

10 Summary

This deliverable has presented selected concepts for end-to-end security and privacy for distributed CPS solutions. The selection of concepts has been made based on the TRANSACT use cases and their needs (see Section 3) and the technical requirements stemming from the TRANSACT WP1 analysis.

The selected concepts' applicability as per Device, Edge, and Cloud Continuum are mapped into four main categories (as shown in Table 5)

1. Security & Privacy Concepts for Transact Core Services & Functions
2. Security & Privacy Concepts for Transact Value-added Services & Functions
3. Security & Privacy Concepts for Domain-Specific Functions
4. Application-Specific Security and Privacy Concepts

Several concept classes have been identified for each of these categories. Within each concept class, then the selected concepts and methods are described. Individual Concept mapping on Device, Edge, and Cloud Continuum is shown in Table 6. Furthermore, mapping of individual concept as per the TRANSACT reference architecture's components is shown in Table 7. Table 8 contains mapping of technical security requirements with D9 (D3.2) Concepts.

The specific concepts in such a class can describe a further sub-division of the overall concept. Each concept is described using a homogenous structure. First, the concept overview is presented, followed by how the particular concepts fit in the TRANSACT reference architecture. The security risks and Threats are discussed, focusing on generic security requirements with specific concepts. Then an example of application of the concept is given (in the context of a particular use case), and lastly, the challenges for the application of the concept in the TRANSACT device-edge-cloud continuum type of systems are listed. The phase considerations like design, development deployment, operation, and maintenance are also considered for each concept while focusing on participant components such as CPS and Devices/ Edge servers/ Cloud Facilities/Services and Solution Providers. These form the basis of further investigation in the scope of the TRANSACT project.

One of the objectives of TRANSACT project is to ensure security and privacy from an end-user perspective. This requires a thorough selection and evaluation of end-to-end security and privacy concepts for distributed safety-critical CPS solutions. Only when these concepts meet this TRANSACT objective can they be elaborated into solutions, which may be more specific to various domains and realizations of device-edge-cloud continuum systems and demonstrators.

The TRANSACT project task T3.2 has undertaken this selection and evaluation of concepts. The selected concepts are reported in this deliverable D3.2. The review has reflected relevant security and privacy concerns, the TRANSACT reference architecture, and needs stemming from the use cases and WP1 analysis. This report covers:

- Security and privacy requirements for distributed application with identification of security and privacy risks and threats, as well as the regulatory aspects;
- End-to-end security and privacy concepts for distributed safety-critical edge/cloud applications taking into account security and privacy protection, intrusion detection, and attestation;
- Applicability of state-of-the-art methods from related projects (e.g., Secredas, CyberSec4Europe), e.g., securing communication in distributed architectures, security by contract for CPS;
- Specification of the trust assumptions that are inherent to environments comprising heterogeneous CPSs, running mixed-criticality applications, and are necessary towards defining and modelling the trusted activities between them and with the back-end infrastructure that has to be supported by the provided attestation enablers;

Final validation of both these concepts and further TRANSACT developed solutions will be based on selected TRANSACT use case demonstrators created in TRANSACT WP5. These demonstrators will incorporate the selected concepts and solutions for validation.

Table 5 : Mapping of concept classes as per the TRANSACT reference architecture.

Device, Edge, and Cloud Continuum	Security & Privacy Concepts for Transact Core Services & Functions	Security & Privacy Concepts for Transact Value added Services & Functions	Security & Privacy Concepts for Domain Specific Functions	Application Specific Security and Privacy Concepts
	1. Concept for risk analysis and management 2. Runtime Verification 3. TPM2.0-based edge and device security 4. Role-based access control rules at the business/design level 5. Anonymization: prevent personal data leak 6. Security and privacy concepts for communication 7. PKI Infrastructure	1. Centralized Machine Learning with Decentralized Data 2. Security and privacy concepts for cloud-based applications 3. Multi-cloud concept for cloud security posture management (CSPM) 4. User and entity behavioural analytics (UEBA) concept for cloud security 5. Cloud Detection & Response (Cloud DR) orchestration for multiple clouds	1. Safety and privacy of off-the-shelf components, including MQTT, non-doubled 4G networks, open IP networks, Unity3D	1. Security and privacy concepts for secure remote driving operation 2. Security and privacy requirements and patterns for the healthcare DICOM data and applications

Table 6: Concept mapping on Device, Edge, and Cloud Continuum.

Concepts	Device	Edge	Cloud
1. Relevant Regulations and Standards	✓	✓	✓
2. PKI Infrastructure	✓	✓	✓
3. Concept for risk analysis and management	✓	✓	✓
4. Runtime Verification	✓	✓	✓
5. TPM2.0-based edge and device security	✓	✓	✓
6. Role-based access control rules at the business/design level	✓	✓	✓
7. Anonymization: prevent personal data leak		✓	
8. Security and privacy concepts for communication	✓	✓	
9. Centralized Machine Learning with Decentralized Data	✓	✓	✓
10. Multi-cloud concept for cloud security posture management (CSPM)			✓
11. User and entity behavioural analytics (UEBA) concept for cloud security			✓
12. Cloud Detection & Response (Cloud DR) orchestration for multiple clouds			✓
13. Security and privacy concepts for cloud-based applications			✓
14. Safety and privacy of off-the-shelf components, including MQTT, non-doubled 4G networks, open IP networks, Unity3D			✓
15. Security and privacy concepts for secure remote driving operation	✓	✓	✓
16. Security and privacy requirements and patterns for the healthcare DICOM data and applications	✓	✓	✓

Table 7: Mapping of individual concept as per the TRANSACT reference architecture's components.

Concepts	A	B	C	D	E	F	G	H	I	J	K	L
1. Concept for risk analysis and management									✓			
2. Runtime Verification							✓					
3. TPM2.0-based edge and device security							✓		✓			
4. Role-based access control rules at the business/design level									✓			
5. Anonymization: prevent personal data leak									✓			
6. Security and privacy concepts for communication							✓					
7. Centralized Machine Learning with Decentralized Data					✓						✓	✓
8. Multi-cloud concept for cloud security posture management (CSPM)					✓		✓					
9. User and entity behavioural analytics (UEBA) concept for cloud security							✓					
10. Cloud Detection & Response (Cloud DR) orchestration for multiple clouds							✓					
11. Security and privacy concepts for cloud-based applications						✓			✓			
12. Safety and privacy of off-the-shelf components, including MQTT, non-doubled 4G networks, open IP networks, Unity3D		✓	✓									
13. Security and privacy concepts for secure remote driving operation							✓	✓	✓	✓	✓	✓
14. Security and privacy requirements and patterns for the healthcare DICOM data and applications							✓	✓	✓			✓

A: Safety- Critical Function, B: Mission- Critical Function, C: Non-Critical Function, D: Data Manager, E: AI-ML & Analytics, F: New Services, G: Safety Performance and Security Monitoring Services, H: Auditing Services, I: Identity Access and Privacy, J: Operational Mode Coordinator, K: Remote Update Coordinator, L: Data Service and Communication

Table 8: Mapping of Technical Security Requirements with D9 (D3.2) Concepts.

TSR No	Descriptions	Covering Concepts
TSR 1	The TRANSACT system architecture should include protection and recovery mechanisms for data and centers for cloud services, and continuously protect data involved in transfers or transmissions	C2, C6-C15
TSR 2	The architecture should be protected against most attacks on edge computing infrastructures. This protection is mainly supposed to be against the following four categories: DDoS attacks, side-channel attacks, malware injection attacks, and authentication and authorization attacks.	C1, C5, C7, C14
TSR 3	The architecture should be protected against DDoS attacks.	C7, C14
TSR 4	The architecture should include effective solutions against flooding attacks and support the technique of detection and filtering.	C2, C7, C14, C15
TSR 5	The architecture should support packet-based detection aims to detect flooding-based attacks.	C2, C14
TSR 6	The architecture will support statistics-based approaches to detect DDoS attacks	C14
TSR 7	The architecture will be protected against Zero-Day Attacks.	C14
TSR 8	The architecture should be protected against Side Channel attacks.	C7, C14
TSR 9	The architecture will include components of a defence protection mechanisms suitable for data perturbation and differential privacy.	C5, C6, C12, C13, C14, C15
TSR 10	The architecture should be protected against Malware Injection Attacks.	C3, C4, C14
TSR 11	To counter the server-side injection attacks, the architecture will include detect-and-filter technique.	C14
TSR 12	The architecture will include components for defence against Device-Side Injections.	C3, C4
TSR 13	The architecture should be protected against Authentication and Authorization Attacks.	C1, C5, C6, C12, C15
TSR 14	The architecture will be protected against threats to Membership Inference Attacks.	C1, C4, C5, C6, C12
TSR 15	The architecture will be protected against Data Poisoning.	C1, C4, C5, C6, C12
TSR 16	The architecture will include components for defence against evasion attacks.	C1, C4, C6, C7, C12
TSR 17	The architecture will ensure the following security requirements: the confidentiality of permanently stored elements, executed-code authenticity, and run-time state integrity. The security architecture consists of four security mechanisms: security by separation, secure boot, secure key storage, and secure interdomain communication.	C4, C15
TSR 18	The cloud systems when used by the architecture should provide the details of how Use Case data will be handled, what types of security they already apply to the cloud infrastructure, what happens in case the system was compromised, if and how they will participate in the investigation and prosecution.	C5, C6, C9, C10, C11, C12, C15
TSR 19	The cloud systems used by the architecture should ensure that the data from the Use Cases is not shared with any third party.	C6, C8, C9, C10, C11, C12, C15

TSR 20	The cloud systems and their provider when used by the architecture should establish trust in the service offered to the Use Cases.	C8, C9, C10, C11, C12, C15
TSR 22	If used in the Use Case, an edge device in the architecture, will be secured on the basis of two factors: (1) root of trust (RoT), in which the edge device is unclonable in addition to the integrity, nonrepudiation, and authenticity of the running software at edge devices; and (2) chain of trust (CoT), in which the edge device is designed to boot up only if cryptographically signed software by a trusted entity is first executed using public-key cryptography. In addition, the keys are stored in specialized secure hardware; this hardware is also responsible for verification and RoT processes.	C1, C4, C5

C1: PKI Infrastructure, C2: Concept for risk analysis and management, C3: Runtime Verification, C4: TPM2.0-based edge and device security, C5: Role-based access control rules at the business/design level, C6: Anonymization: prevent personal data leak, C7: Security and privacy concepts for communication, C8: Centralized Machine Learning with Decentralized Data, C9: Multi-cloud concept for cloud security posture management (CSPM), C10: User and entity behavioural analytics (UEBA) concept for cloud security, C11: Cloud Detection & Response (Cloud DR) orchestration for multiple clouds, C12: Security and privacy concepts for cloud-based applications, C13: Safety and privacy of off-the-shelf components, including MQTT, non-doubled 4G networks, open IP networks, Unity3D, C14: Security and privacy concepts for secure remote driving operation, C15: Security and privacy requirements and patterns for the healthcare DICOM data and applications.

11 References

Antonia M. Reina Quintero, S. M.-V. (2022). A domain-specific language for the specification of UCON policies. *Journal of Information Security and Applications.*

Anupam Chattopadhyay, K.-Y. L. (2021). Autonomous vehicle: Security by design. *IEEE Transactions on Intelligent Transportation Systems*.

ATNA. (2021). *Audit Trail and Node Authentication.* IHE.

Boyu Kuang, A. F. (2022). A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects. *Computers & Security*.

Chen Sun, A. H. (2004). Fast beamforming of electronically steerable parasitic array radiator antennas: theory and experiment. *IEEE Transactions on Antennas and Propagation*.

Czarnecki, K. (2004). Overview of generative software development. *International workshop on unconventional programming paradigms.* Springer.

DICOM Standards Committee. (2022). *DICOM PS3.15 2022a - Security and System Management Profiles.* NEMA.

Edlira Dushku, M. M. (2020). SARA: Secure asynchronous remote attestation for IoT systems. *IEEE Transactions on Information Forensics and Security*.

EU. (2016). *General Data Protection Regulation.* THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.

GDPR. (2018). *General Data Protection Regulation.* European Parliament and Council of the European Unio.

George Coker, J. G. (2011). Principles of remote attestation." International Journal of Information Security. *International Journal of Information Security* .

HIGHER COUNCIL FOR ELECTRONIC GOVERNMENT. (n.d.). *PORTAL ADMINISTRACIÓN ELECTRÓNICA.* Retrieved from https://administracionelectronica.gob.es/pae_Home/dam/jcr:80b16a91-75b1-432d-ab23-844a12aab5fc/MAGERIT_v_3_book_1_method_PDF_NIPO_630-14-162-0.pdf

HIPPA. (n.d.). *Health Insurance Portability and Accountability Act.*

Hoepman, J.-H. (2014). Privacy Design Strategies. *IFIP International Information Security Conference.* Springer.

International, I. (n.d.). *IHE Audit Trail and Node Authentication (ATNA) Profile.* IHE International .

Koen Tange, M. D. (2020). A systematic survey of industrial internet of things security: requirements and fog computing opportunities. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, .*

MAGERIT. (2005). Retrieved from European Union Agency for Cybersecurity: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html

Marco Brambilla, J. C. (2017). Model-driven software engineering in practice. *Synthesis Lectures on Software Engineering.*

McKinney, D. (August, 2001). Impact of Commercial Off-The-Shelf (COTS) Software and Technology on Systems Engineering. *INCOSE Chapters*, (pp. 1--19).

Michal Tarkowski, M. R. (2017). Improved jamming resistance using electronically steerable parasitic antenna radiator. *IEEE EUROCON 2017-17th International Conference on Smart Technologies.*

Paul Vanhaesebrouck, A. B. (2017). Decentralized collaborative learning of personalized models over networks. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics,*, 509-517.

Peter Kairouz, H. B. (2021). Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning*.

Salvador Martínez, A. F. (2018). Automatic generation of security compliant (virtual) model views. *International Conference on Conceptual Modeling* (pp. 109-117). Springer.

Santiago Hernández Ramos, M. T. (2018). Mqtt security: A novel fuzzing approach. *Wireless Communications and Mobile Computing*, 1-12.

UN Regulation No. 155. (2021). *UN Regulation No. 155 - Cyber security and cyber security management system.* UNITED NATION.

UN Regulation No. 156. (2021). *UN Regulation No. 156 - Software update and software update management system.* UNITED NATIONS.

Y. Sheffer, R. H.-A. (2015). *Summarizing known attacks on transport layer security (TLS) and datagram TLS (DTLS).* IETF.