Grant Agreement No.: 871808
Research and Innovation action
Call Topic: ICT-20-2019-2020: 5G Long Term Evolution

INSPIRE-5Gplus

INtelligent Security and PervasIve tRust for 5G and Beyond

D4.4: Liability management in a 5G environment

Version: v1.0

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	30/06/2022
Submission date	04/08/2022
Lead editor	Chrystel Gaber (Orange)
Authors	Vincent Lefebvre (Tages), Vinh Hoa La (Montimage), Edgardo Montes de Oca (Montimage), Ghada Arfaoui (Orange), Christèle Tarnec (Orange), Luisa Rossi (Orange), Pauline Derez (Orange), Vincent Lefebvre (TAGES), Noelia Pérez Palma (UMU), Orestis Mavropoulos (CLS)
Reviewers	Chafika Benzaid (Aalto), Gianni Santinelli (TAGES)
Work package, Task	WP4 T4.4
Keywords	Liability, accountability, responsibility, management

Abstract

Based on the outcomes of T4.1, T4.2, T4.3 and T4.4, this document presents the results of T4.3 Liability management. The task provides a perspective on the regulation of specific Vertical and Telecom industries that are involved in the complex 5G environment. It demonstrates that it is not possible to define specific set of requirements (safety, availability, security, QoS) that would fit all use cases. And that providing on-demand security services with a 'convention of proof' i.e., an on-demand level of transparency, accountability and liability, is a key driver for the development of 5G Services. The deliverable defines some metrics to negotiate such a convention of proof. It also defines the goals of a liability management system and investigates how they are covered by the enablers developed in INSPIRE-5GPlus.

Document revision history

Version	Date	Description of change	List of contributor(s)
v0.1	23/01/22	Table Of Content	Chrystel Gaber
V0.2	27/06/22	Introduction, Section 2, Section 3, Section 4, Section 5	Chrystel Gaber, Luisa Rossi, Pauline Derez, Christèle Tarnec, Edgardo Montedesca, Vinh Hoa La, Vincent Lefebvre, Onur Kalignac, Gürkan Gür, Yannick Carlinet, Jose Sanchez, Ghada Arfaoui, Yacine Anser, Noelia Pérez Palma
V0.3	30/06/22	Section 4, proof-reading	Morgan Chopin, Jose Sanchez, Chrystel Gaber
V0.4	30/06/22	Corrections throughout the document after WP4 internal review	Chrystel Gaber after internal review by Rafal Artych, Aleksandra Podleska, Edith Felix
V0.5	05/07/2022	Abstract, executive summary, conclusion	Chrystel Gaber
V0.6	13/07/2022	Review	Gianni Santinelli, Chafika Benzaid
V0.7	26/07/2022	Corrections following review	Chrystel Gaber
V0.9	27/07/2022	Final editing	Uwe Herzog, Anja Köhler
V1.0	04/08/2022	Submit Deliverable	Uwe Herzog

List of contributing partners, per section

Section number	Short name of partner organisations contributing
Section 1	Chrystel Gaber (Orange)
Section 2	Chrystel Gaber (Orange), Gürkan Gür (ZHAW)
Section 3	Chrystel Gaber (Orange), Luisa Rossi (Orange), Pauline Derez (Orange), Christèle Tarnec (Orange)
Section 4	Chrystel Gaber (Orange), Yacine Anser (Orange), Noelia Pérez Palma (UMU)
Section 5	Noelia Pérez Palma (UMU),
Section 6	Chrystel Gaber (Orange)

Disclaimer

Acknowledgement

The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement No 871808. The European Commission has no responsibility for the content of this document.

[1] http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US

Executive Summary

The deliverable D4.4 builds upon the definitions of trust, accountability and liability that were provided by D4.3 to introduce the concept of duality between liability and trust. Liability represents a legal entity's commitment (in a contract for example) to deliver a set of negotiated KPIs and to provide evidence that can be monitored by its customers or auditors. Trust represents the belief formed by a trustor (typically the contractor) that a trustee (typically the contracted) will perform a task as previously agreed by both parties. Trust and liability cannot exist without one another, given that an entity would not enter in contract with another entity that it does not trust at all; and that trust is built on the level of controls and evidences that the contracted can provide to the contractor.

As a result, and in accordance with Deliverable D4.2, we propose to dedicate the concept of Trust within a Domain. The owner of the Domain manages its resources and operates services requested by external entities. The Domain owner is responsible for complying with the convention of objectives, KPIs and evidence that were negotiated with the external entities to demonstrate Trust (Trust metrics were investigated in D4.2) while optimizing its resources usage (e.g., cost, performance). The deliverable D4.4 presents a technical framework for liability and accountability management in the context of 5G environment. Based on an overview of the European legal and standards framework, we gather the requirements of several vertical use cases for security services and highlight that the 5G use cases needs cannot be addressed by a single security level overall the 5G infrastructure but that it is necessary to provide on-demand security services as well as on-demand accountability. Key enablers detailed in D4.4 to achieve this goal are the manifests which register the SLA operated by each entity contributing to the Lifecycle of a component, the attestation framework which collects evidence of SLA compliancy or violation, and the Root Cause Analysis which investigates origins of an issue or SLA violation.

We have reproduced the approach detailed in this deliverable in our Demo2 proposal, in which we resolve the strong issue of components isolations through an orchestration of container optimized to resolve placement under constraints of components. The interesting part of WP4 is to investigate approaches which have mathematical results that deliver formal evidence if the proposed algorithms converge to a solution. In this case we know that constraint have been covered and we have just to collect evidence of this orchestration on sensitive nodes to demonstrate the complete realization of the isolation SLA.

However, the second Workshop on Accountability, Liability and Trust organized by INSPIRE-5Gplus highlighted that establishing an end-to-end chain of trust over heterogeneous domains linked together is one of the major challenges to be managed by ENISA for defining 5G certification scheme. Even under Common Criteria evaluation scheme, the Assurance level, a scale between AVA-VAN1 and AVA_VAN5 which measures the capacity of attackers (from script kiddies to governmental labs), is the only Trust metric that is shared between legal entities and recognized by the signatories of the SOG-IS agreement. An emerging approach consists in combining certified Domains (e.g., CC or EUCS certification schemes), but even with this approach, the combinatory generated coupled with the complexity of this system of systems to be evaluated are out of reach. ENISA reduced the global problem to be resolved to a subset of around 10 business lines which hyperspecialized and focused on one service, for instance the "Access control procedure to a 5G network" or "the provisioning line of the Telecom Context in one eUICC" operated in multi-party contexts.

Then, we present the second Workshop on Accountability, Liability and Trust that was organized in July 2022. Finally, the Deliverables concludes with a discussion of results and an overview of perspectives.

Table of Contents

List of Figures

List of Tables

Abbreviations

5G-PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Authorization, Accounting
AI	Artificial Intelligence
IP	Intellectual Property
RFP	Request for Proposal
HLA	High Level Architecture
MEC	Multi-access Edge Computing
MNO	Mobile Network Operator
OES	Operator of Essential Services
SLA	Service Level Agreement
SSLA	Security Service Level Agreement

1 Introduction

5G networks aim to boost the development of digital services with anytime-anywhere connectivity. The Key Verticals expected to drive the wider adoption of 5G are the automotive industry, the smart city and public safety enablers, Industry 4.0, Healthcare, Energy and Entertainment. To fulfil the multiple use cases for these Verticals, which have very different requirements such as ultra-low latency or ultra-reliability, 5G networks are built to be extremely flexible and dynamic.

The safety and cybersecurity legal obligations that apply to some of these Verticals can be translated into requirements for underlying 5G End to End (E2E) services. Möllering defined that trust and control are dual concepts. They represent two sides of a same coin which contribute to each other to achieve the acceptation of risk [1]. Bearing in mind this principle, the ability to commit, deliver and demonstrate the fulfilment of these requirements is essential to develop trust among parties and demonstrate regulation compliance in a context where zero-risk cannot be achieved. Ultimately, we believe that this ability will be a driver for the adoption of 5G E2E Services.

However, the multi-party and multi-layer nature of 5G architecture makes it difficult to track and demonstrate responsibilities. Also, the strategy to implement the highest level of security is unrealistic as the cost required to maintain this security level would be prohibitive for most use cases which do not need such a configuration and would not use the associated services.

In this context, E2E Service Providers must find the balance between liability risk (i.e., risk that the slice provider does not deliver what he promised to his customer) and supply chain risk (i.e., risk that the supply chain does not provide services as committed to the slice provider), as illustrated in Figure 1. Liability management aims at assisting E2E Services in finding this balance to ensure an End-to-End assurance by identifying and collecting the requirements from the 5G Vertical Service and monitoring the cascade of responsibilities that result from the composition of services and that are potentially delegated to subcontractors.

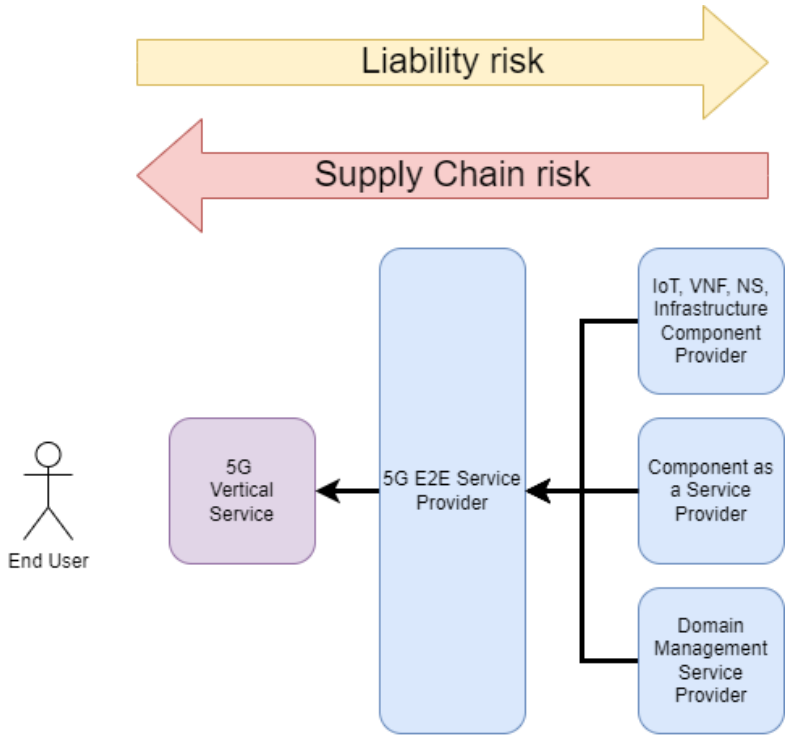


Figure 1. Management of liability risk and supply chain risk

This deliverable lists the needs related to liability in 5G, investigates the concept of liability management, and shows how INSPIRE-5GPlus enablers can serve this purpose. The definitions of trust,

accountability, liability have been thoroughly detailed in the deliverables D4.1 [30], D4.2 [42], D4.3 [40] and MS8 [43] and are not defined again here.

The deliverable is organised as follows. Section 2 provides an overview of regulation of 5GPP verticals in the European context. Section 3 provides a state of the art on liability modelling and handling. Section 4 defines how liability management can be achieved by decomposing it into functional blocks. Section 5 describes how INSPIRE-5GPlus enablers participate in liability management and section 6 details how INSPIRE-5GPlus demos illustrate liability management. Section 8 concludes this deliverable and provides some perspectives.

2 European Legal and Standards Framework for 5G Telecom Actors and 5GPP Verticals

This section gives an overview of the European legal and standards framework for 5G telecom actors and 5GPP verticals. First, we examine the legal and standards requirements applicable for 3 examples of 5GPP verticals and show that the diversity of requirements cannot be met by a unique security level for all use cases. It is necessary to propose services with on-demand level of security. Second, we provide an overview of the European legislation applicable to 5G telecom actors. Third, we provide a status on product defects legislation. Then, we detail how the evolution from SIM to eSIM ecosystem impact the trust and liability relationships in the ecosystem. We also provide a status on liability for AI. Finally, we discuss our findings and highlight what are the resulting challenges for liability management.

2.1 Legal or standard requirements for 5GPP Vertical use cases

Healthcare, transport, energy and water supply services are considered as Operators of Essential Services (OES) by the European Network and Information Security (NIS) Directive because their interruption would have a significant impact on the functioning of the economy or society. As such, they have to protect themselves against cyberattacks and can delegate or enrich some of these controls with services provided by 5G E2E Service Providers. Domain-specific regulation or standards like ISO 14971 [19] for Health or SEVESO [20] for industry also impose controls that can be translated into requirements for privacy, isolation of processing or network component certification levels.

ENISA has produced reports on the minimum security requirements for Digital Service Providers [24] and Baseline Security Measures for OESs [27] but they do not include any information on the differentiation of assurance levels, the creation of On-Demand security services and how 5G infrastructure can meet all security needs while optimizing costs. We complete this work by summarizing some standards and legal requirements applicable to 5GPP verticals. Based on this analysis, we highlight that providing on-demand security services with demonstrable SLAs is valuable for 5G Verticals Services and therefore a driver for the adoption of 5G services.

This section is organized as follows. First, we describe the methodology of our analysis. Then, we detail our observations for specific use cases in the automotive, industry and eHealth sectors. Finally, we synthesize and discuss our results.

2.1.1 Methodology

We analysed 9 use cases from 3 different sectors through a literature review and interviews of experts from French mobile operators. Table 1 compiles the results of this study.

Requirements were categorized by: Quality of Service; need to co-manage risks and responsibilities resulting from delegation of tasks or hosting of activities by a Third Party; support to demonstrate assurance of activities operated or hosted by a Third Party; security of communications; and services related to monitoring and reaction.

2.1.2 Automotive

In the automotive domain, infotainment use cases such as multimedia content streaming and online gaming have low criticality. Although such use cases are performance-demanding to reach acceptable QoS levels, priorities are usually lower than for emergency services [21], IP (Intellectual Property) and revenue streams should still be protected.

Use cases such as remote diagnostics are more safety-critical and security-sensitive and aim to maintain the vehicle in good operational conditions during its lifecycle, with auditability.

A safe and secure Over The Air (OTA) update process is pivotal to correct rapidly, regularly, and efficiently bugs and vulnerabilities in automotive software and hardware to avoid costly vehicle recalls. Malicious updates can threaten vehicle integrity or leak sensitive information such as proprietary vehicle data. The update protocol should therefore guarantee data authenticity, integrity, confidentiality, freshness, and privacy.

A high-criticality use case is *Anticipated Cooperative Collision Avoidance (ACCA)* to detect, localize dangerous events on the road, e.g. low visibility or short detection range, and respond accordingly [22]. Service guarantees (e.g., availability, low-latency) are key to distribute detected hazard information between heterogeneous infrastructure components (e.g., MECs hosted by multiple MNOs). Strong guarantees for network isolation, protection of data, and real-time anomaly detection and reaction are also expected for safe and secure processing of notifications.

2.1.3 Industry

In Industry 4.0 [25][26], preventive maintenance operations consist in planned routine operations to repair or upgrade industrial tools. Criticality is low and usually does not require high QoS. Threats are possible accidents which may cause damage to the production tools, physically harm workers, or entail theft of Intellectual Property or Know-How (e.g. blueprints, recipes or plans).

Since maintenance operations may require to lower some defences or remove some controls, the concerned perimeter should be isolated from the network of other components. All patches should also have been deployed during the downtime planned for maintenance.

The use case Collaborative Robots is a more sensitive use case because an issue may impact the safety of workers or the quality of production. The Crisis Management use case is demanding in terms of QoS and security level. A use case may also evolve over time in terms of criticality. For example, the Preventive Maintenance use case may evolve into Crisis Management if the situation becomes critical.

2.1.4 eHealth

Most eHealth use cases are associated to strong privacy requirements[27][28][29]. Low criticality use cases such as Remote Diagnostics and Smart Medication do not require specific security services: the basic level of network security levels are sufficient to cover their needs. On the other end of the spectrum, use cases such as Emergency Diagnostics and Remote Surgery [29] require very high Quality of Service (QoS.) Since issues can result in injuries or casualties, demonstrating that it is essential for eHealth services to operate on trusted and trustworthy systems. Moreover, safety requirements are very likely to be transposed into security requirements for the network infrastructure.

2.1.5 Summary

Table 1 regroups the requirements collected for each vertical and each use case described above. It highlights that verticals and even use cases within a vertical require different security services and various levels of security guarantees.

Ideally, to address all these requirements, 5G networks would need to implement the highest level of security throughout the infrastructure. This is not realistic given that this would require a huge amount of investment while representing less than 20% of the 5G infrastructure usage. Mainstream use cases stakeholders which represent 80% of the infrastructure usage may not accept to pay the costs of unnecessary high security levels. Even customers with high-security level needs would prefer to pay only for the services which are effectively useful for their use case.

The path for 5G services adoption by verticals is therefore to provide on-demand security services for their customers as well as some means to demonstrate their fulfilment. In this way, a baseline security service could be set up for mainstream services, advanced security services could be proposed for sensitive use cases. Finally, critical use cases would benefit from security services tailored specifically for them.

However, setting up such on-demand services requires 5G E2E Service Providers to put in place the management infrastructure which will allow them to provide differentiated security service and maintain the committed security level.

		AUTOMOTIVE			INDUSTRY 4.0			eHEALTH		
Category	Requirements	Entertain-ment	Remote diagnostics	Anticipated Cooperative Collision Avoidance	Preventive maintenance	Collaborative Robots	Crisis management	Remote diagnostics & smart medication	Emergency diagnostics	Remote surgery
Quality of Service	Network Reliability	Low	Low	High	Low	Low	High	Low	High	High
	Low Latency	Low	Low	High	Low	Medium	High	Low	High	High
	Availability	Low	Low	High	Low	Medium	High	Low	High	High
	Network Access Priority	Low	Low	High	Low	Low	High	Low	High	High
	Out of coverage services	Low	Low	High	Low	Low	Low	Low	High	Low
Third Party Trusted Operation & Responsibility Sharing	Protection of Human Safety	Low	Medium	High	Low	High	High	Low	High	High
	Protection of Intellectual Property & Know-How	Medium	Medium	Low	High	High	High	Low	Low	Low
	Protection of Revenue	Medium	Medium	Low	Medium	High	High	Low	High	High
Assurance Demonstration for Third Party Trusted Operation	Network isolation	Low	High	High	Medium	Medium	High	Low	High	High
	Network Components Certification Levels	Low	High	High	Low	Low	Low	Low	High	High
	Packet Processing Proof	Low	High	High	Low	Low	Low	Low	High	High
	Guaranteed Patch Management	Low	High	High	Medium	High	Medium	Medium	High	High
Communication Security	Confidentiality	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium
	Integrity	Low	High	High	Medium	Medium	High	Medium	High	High
	Authenticity	Low	High	High	Medium	Medium	High	Medium	High	High
	Anti-replay	Low	High	High	Medium	Medium	High	Medium	High	High
	Privacy	Low	Medium	Medium	Low	Low	Low	High	High	High
Monitoring & Reaction	Anomaly Detection Service	Low	Medium	High	High	High	High	Low	High	High
	Anomaly Prevention Service	Low	Medium	High	Low	Medium	High	Low	High	High
	Real-time Reaction	Low	Low	High	Medium	High	High	Low	High	High

Table 1. Summary of requirements for use cases in automotive, Industry 4.0 and eHealth Verticals

2.2 Legal or standard requirements for 5GPP Vertical use cases

In Europe, the directive 2018/1972 European Electronic Communications Code is applicable. It had to be transposed into national regulation in the EU countries by 21 December 2020. Article 40 requests Member States to ensure that Telecommunications Service Providers take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services with regards to the state of the art. Article 41 requires Member States to ensure that security incidents are notified without delay to competent entities and to provide a yearly report to the European Commission and ENISA. This directive also highlights the role of encryption. On its side, the directive 97/66 protects users of telecommunication services, their private data and the privacy of telecom users.

The NIS Directive creates a common framework for cybersecurity preparedness and response to be transposed to national regulations. It sets up a minimum set of cybersecurity measures to protect the OES (Operator of Essential Services) against cyberattacks involving major consequences and to report security incidents to national authorities. As telecom operators are identified as OES, they also have to comply with these measures.

The EU Cybersecurity Act defines that future certification schemes must distinguish three levels of assurance based on the level of risk, in terms of probability, impact of an incident and intended use. The Basic level is a self-assessment of compliance. The Substantial level requires a review of known vulnerabilities and to verify the proper implementation of security functions by an accredited third party. Finally, the High level adds penetration testing to evaluate the resistance against attacks performed by experienced attackers focusing on vulnerabilities identified in the Substantial level review. In some European countries, national agencies play a role in the process of certifying software in order to provide a panel of secure software. Nevertheless, the goal is not European autonomy in the development of self-certified software and products, but rather the ability to audit and control the security of products delivered by third parties.

The laws of contracts applicable in Europe and each country is applicable if there is a contract between a telecom operator and its customers for the purchase of an End-to-End service over 5G. For use cases,

where private data are used, such a telecom operator which provides an End-to-End service over 5G also has to comply with GDPR obligations.

Aside from these regulations, the standards (ETSI, GSMA) and assurance schemes (NESAS, SCAS) currently structure the technical and security requirements of telecommunications infrastructures.

2.3 Product defects

The Product Liability Directive 83/374/EEC (PLD), adopted in 1985, sets out the conditions under which an injured person can claim compensation for damages caused by defective products. It applies to all movable products but not to services. It applies to B2C relations. The PLD introduced **strict liability of the producers** for damages caused by a defect in their products.

The PLD:

- **defines a product as "all movables**, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable" (article 2)
- **covers software embedded in products** and provides the ability for injured parties to be compensated. Notably, article 1 of the Directive already makes the producer liable for damage caused from a defect in his product, thereby covering compensation of damages of erroneous products irrespective whether said product is or possesses AI.
- **defines the producer as "the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part"** (article 3)
- **does not** specify when exactly software is considered as a product

A product is defective "when it does not provide the safety which a person is entitled to expect" (article 6). The eligible damage covers: death, personal injury, and damage to consumer property. If a defective product causes personal injury or material damage above €500, the producer is liable.

The victim has to prove the defect, the damage and the causal link between the two (burden of proof - article 4). However, the injured person does not need to prove the producer's fault. In situations where two or more persons are liable for the same damage, "they shall be liable jointly and severally" (article 5). The injured person should be able to claim full compensation for the damage from any one of them.

However, **the PLD offers certain limitations to producers' liability**, in case producers prove that:

- producers did not put the product into circulation;
- the defect did not exist when the product was put into the market; or
- the product was neither manufactured by him for sale or any form of distribution
- the defect is due to compliance with regulations; or
- **the state of technical knowledge at the time of putting the product into the market made it impossible to discover the defect**;
- in the case of a manufacturer of a component, that the defect is attributable to the design of the product

There is a limitation period of **three years for the victim to claim damage** from the day on which the plaintiff became aware of the damage (article 10).

The current PLD does not harmonise all the aspects of product liability. National liability regimes in some EU member *states are fault-based, so the victims need to prove the damage and the causality between fault and damage, and also the fault of the* liable person.

The Commission started the PDL revision process. As a first step the EC published an evaluation in 2018 [13], as well as the 2019 Expert Group report on Liability for Emerging technologies [14], concluded that the Product Liability Directive (PLD) is generally **fit-for-purpose**. Moreover, EC published an Inception Impact Assessment [14].

To conclude, the PDL is under revision, and it is very likely that the revised instrument will cover software products. Potential changes to liability rules will be discussed in parallel with the recently proposed AI Act (AIA) that introduces additional obligations on providers and users of high-risk AI applications intended to increase the safety and trustworthiness of AI systems put on the EU market.

Although not in Europe, it is worthwhile noting that in the United States, an executive order issued in May 2021 requires software vendors contracting with the federal government to provide a software bill of materials (SBOM) which record the code, either proprietary or open source, which compose the software product. The SBOM can also be used to disclose known vulnerabilities and their remediation. This measure was taken in the wake of the Log4Shell vulnerability (CVE-2021-44228), as a way to improve supply chain security and encourage communication among stakeholders.

2.4 Evolution of the trust and reliability relationships in the eSIM ecosystem

Deliverable D4.1 [30] showed that the 3GPP Trust Scheme has evolved given that in the eSIM ecosystem, the UICC/USIM is not any more under the strict control of an Operator. and shifts under the control of device manufacturers. In the paper [31], we investigate further the impact of this evolution on liability and trust relationships. We show that the contractual relationship between operators and the SIM card manufacturers is replaced by the combination of the trust in actors involved in SOG-IS agreements (they coordinate the standardisation of Common Criteria protection profiles and certification policies) and the certifications performed by accredited laboratories.

Through an example of incident which occurred on the SIM card of an operator, this paper also highlights some challenges which emerge and that are not yet addressed. First of all, device manufacturers have little incentive to purchase high-quality eSIMs and there is no framework ensuring that operators will receive timely and high-quality support from device manufacturers. Second, the impact of anticipated churn increase on hardware performance and reliability has not been evaluated. Also, the current architecture of Security Domains does not preserve the context and data of a third-party application installed in the eSIM when there is a change of operator.

2.5 Status on liability for AI

The European Digital Single Market strategy, including the Data Act, Data Governance Act, Digital Markets Act, Digital Services and AI Act, is looking to not only protect personal data but also to create frameworks that allow for data flows, while aiming to mitigate hate speech and misinformation and protect from misuses of AI. Europe is at the forefront of AI regulation even if China is issuing a legal framework for ethical AI [32] and the USA at a federal level issued few months ago the Artificial intelligence Capabilities and Transparency (AICT) Act [34] and the Artificial Intelligence for the Military (AIM) Act [33].

The European legal framework dedicated to AI has to adapt to new technical risks and opportunities. For example, in network management, AI is very useful for capacity planning and optimization, for anomaly detection as well as for energy efficiency management. However, the risk of biased and unfair decisions exists if these are made based on black-box models without the possibility to have a clear understanding of AI model behaviour and without guarantee that the human stays in control.

More specifically, the purpose of the AI Act, one of the first set of legal frameworks for AI is to frame the legal use of AI in proportion to the risks that AI poses to fundamental human rights. Three

categories of AI are proposed (prohibited, high-risky and other) and a list of applications included in prohibited and high-risk AI has been proposed by the European Commission [35].

If classified as high-risk AI, a 3rd-party conformity assessment is needed before deployment. The requirements, mandatory for high-risky AI, will concern data, documentation and traceability, provision of information and transparency, human oversight, robustness and accuracy. Anticipating the regulation and answering the market and citizens' needs, companies are organizing themselves to create frameworks to define and implement responsible AI in order to be audited and recognized for their quality. A lot of initiatives are emerging [36], [37], [38] and they are mostly used as self-regulation and "conversation-starters" within and around the organization. In addition to labels, in the European approach of AI, an increasing role will be given to European standards to accompany and support practical implementation of AI regulation, through a set of technical and business guidelines and rules. As a matter of fact, conformity with specific standards will become mandatory for high-risk AI systems (to achieve conformed AI systems). Even if some of the solutions proposed by international standards (like the ones by ISO, IEEE) may be just adopted by European, some specific solutions may be required and will be required (for instance European personal rights and privacy protection may require providing some dedicated solutions in European standards). ISO/IEC JTC1 [39] is very active in the field of AI standardization, dealing with its development in a comprehensive manner (fairness, explainability, transparency, robustness, trust but also technical approach, governance and management of AI).

Although management & operation of critical infrastructures is qualified as high-risky AI, supply of communication services is currently not listed by the EC as high risky AI in its proposal. As of now, road traffic and supply of water, gas, heating and electricity are proposed to be in the high-risky AI list. Intense lobbying exists nowadays to avoid labelling network management/communication services supply as a high-risk activity. However, operators could possibly be submitted to high-risk requirements when providing technical component to manage critical infrastructure (for example an AI-based service provided by an operator on 5G network to detect security threat on the electrical network). Even though details are still in debate, operators should prepare to face high-risk requirements.

3 State of the art on Liability Modelling and Handling

In this section, we examine existing and related works on liability modelling and handling. First, we explore existing tools for liability management. Then, we list existing mathematical models used to represent liabilities and metrics that can be used to characterize various aspects related to liability. Finally, we show how we adapted these metrics to our context and how the INSPIRE-5GPlus project contributed to Security SLAs.

3.1 Liability management

To the best of our knowledge, there is limited work on liability management systems for 5G E2E service management. Most existing solutions either do not cover liability or are not adapted for 5G use case.

Contract management tools (e.g., Contractworks [1], hyperlex[5][4], Cobblestone[3], ContractPodAICloud[4]) assist legal departments to negotiate, sign, store and analyse contracts. Some tools such as hyperlex leave a lot of margin to users to perform their own analysis and mostly provide them tools to store, summarize and research a database of contracts. Others such as ContractPodAI give the possibility to fully automate contracts reviews and their risk assessments, evaluate vendor compliance in a Request For Proposal (RFP) process, automate approval processes. Cobblestone tool also has a feature that freezes records in case of legal disputes or litigations. The sectors which mainly make use of such tools are related to healthcare, technology, manufacturing, government[1],[6]. To our knowledge, such tools concentrate on risks prevention and do not monitor ICT products or services to collect evidence and investigate technical violations.

Hatzivasilis et al [17] proposed a cyber insurance tool which calculates insurance fees, alerts customers on potential violations and applies penalties to the entities at the origin of the violation. Given that this tool is aimed at insurers who hedge risks, it does not cover some concerns that are relevant for 5G E2E Service Providers. In contrast, an E2E Service Provider does not only seek to pinpoint the responsible party and calculate penalties. Its objective is also to operate its service in a way that minimizes its SLA violations, insurance fees and penalties.

3.2 Liability modelling

In software engineering, a design pattern is a general, reusable solution to a commonly occurring problem in a given context. Although design patterns [7] are not related to liability, some patterns model how a task is shared among multiple components and therefore can be used to model how responsibilities are shared. For example, the responsibility chain help developers define how a series of handlers to process a request. Figure 2 illustrates the corresponding sequence diagram. With this design, an event is propagated along a branch of an object tree and is processed by the first element of the chain that is capable of handling it, as illustrated in Figure 3. This design pattern only defines how a task (responsibility) is shared and does not deal with default/anomalies.

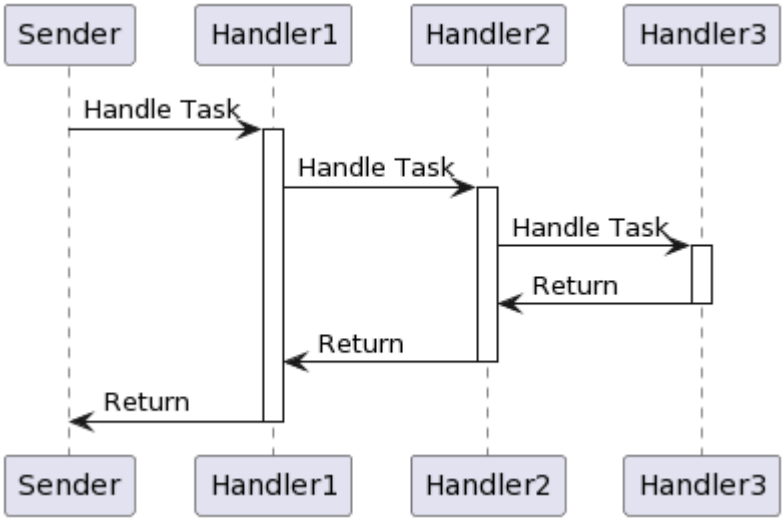


Figure 2. Sequence diagrams of the responsibility chain pattern, source [7]

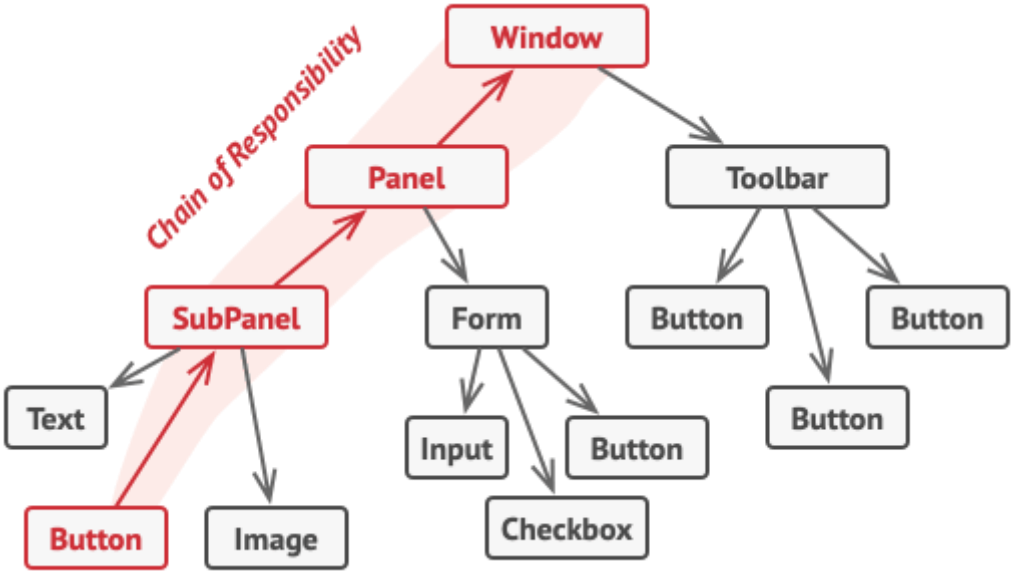


Figure 3. Example of a chain responsibility in a tree representing the components of a UI, source [8]

Relationships between actors or contracts can also be modelled by a tree. For example, the Contract Management Tool Cobblestone displays for each of the managed contracts their relationships with other contracts in the form of a graph [6].

One related work is [9], where a call graph of requests is generated for each time period by processing the traces supplied by application services on a regular basis. Root cause analysis (RCA) algorithm begins with the frontend service and traverses the graph by taking a random walk with a predetermined number of steps. Each neighbour's pickup probability is proportionate to its relevance to the anomaly, as determined by the correlation between its performance metrics and those of the frontend service. In [10], alternatively creates the topology based on the traces produced in a particular time window, which terminates at the moment when a service experienced the performance anomaly. The generated graph is explored through a breadth-first search (BFS). In anomaly propagation chain analysis, they apply a pruning technique to reduce irrelevant service calls and uses tailored models based on machine learning and statistical methods to discover different types of service anomalies (i.e., performance, reliability, traffic).

Wu et al. [11] creates a topology graph with vertices representing running application services and the node that hosts them, and oriented arcs representing service interactions and hosting. Each vertex of the topology graph is associated with the time series of KPIs monitored on the relevant service or node.

MicroRCA then creates a "anomalous subgraph" by selecting the vertices of the topology graph that correspond to the services where anomalies were discovered by including the vertices and arcs corresponding to the interactions to/from the anomalous services, and adding other vertices and arcs from the topology graph to create a connected subgraph.

Instead of identifying the application topology automatically, DLA [12] requires the application operator to give it as input. The input includes data about the services forming an application, the containers that run them, and the VMs that host the containers, as well as their communication and hosting relationships. DLA automatically determines the likelihood of an anomaly impacting a service, container, or VM being caused by the components it corresponds to by transforming the input topology into a Hierarchical Hidden Markov Model (HHMM).

3.3 Liability and Accountability KPIs and metrics

Table 2 regroups the metrics proposed by A4Cloud to measure several concepts relevant for liability management. The first column describes the characteristic which is measured by the combination of metrics detailed in columns 2 and 3. The last column is a summary of the metric adapted to the context of INSPIRE5G-Plus.

Attribute	ID	Dimension	Adaptation in the context of INSPIRE5G-Plus
Transparency	T1	Accessibility	Measures how easy it is to obtain data that are relevant to analyse security issues
	T2	Effectiveness	Measures how easy it is to process the collected information in order to retrieve relevant information
	T3	Timing	Measures quantitatively the time elapsed between an event of incident and the time after which the alert was raised or the time elapsed between a report was requested and the time after which the report was produced.
	T4	Overall evaluation of transparency	This metric combines T1, T2 and T3 to give an overview of the transparency
Responsibility	R1	Level of Authentication	The level of confidence in the authentication system which is used to authenticate the actions performed by administrators performing actions on the HLA.
	R2	Delegation of Responsibility	This metric is related to delegation chains. Responsibilities are less diluted in short delegation chains than in long ones.
	R3	Integrity	The level of confidence on the integrity of collected evidence. For example, the assurance level provided by an MD5 is lower than that of SHA-512 to protect logs collected by an HLA component
	R4	Duty/Role separation	This metric is related to delegation of

Attribute	ID	Dimension	Adaptation in the context of INSPIRE5G-Plus
			responsibility.
	R5	Overall Responsibility Level	This metric combines R1, R2, R3 and R4 to give an overview of responsibility
Attributability	A1	Attributability	This metric measures the degree of certainty with which an action or event can be attributed to an entity. It is based on the ability to produce evidence that are non-repudiable.
Liability	L1	Penalty	The goal of A4Cloud's liability metrics is to measure the consequences faced by an entity if it is found responsible for not fulfilling its legal obligations or for violating its commitments in a contract. Generally, these consequences are measured as financial losses.

Table 2. Summary of metrics proposed by the A4Cloud project

3.4 Adaptation of Liability and Accountability KPIs and metrics to INSPIRE-5Gplus context

In the project, we defined several metrics that can be used either to build a 'convention of proof' i.e., an agreement on the level of proof that is required by a customer and the provider of a service or to evaluate a level of responsibility / liability.

3.4.1 Transparency

We propose to measure accessibility by a scale which identifies different levels of information accessibility.

Accessibility level	Description
1	The data is accessible on demand physically on-premises or posted
2	The data is sent by e-mail after request
3	The data can be retrieved through an API on demand after an authentication and authorization
4	The data can be retrieved through an API publicly

Table 3. Accessibility metric

We propose to measure effectiveness by a scale which identifies different types of processing which are more or less readable by a machine.

Effectiveness level	Description
1	The data is available in paper format
2	The data is available in digital format but non-machine-readable
3	The data is available in digital format and is machine-readable

Table 4. Effectiveness metric

Timing can be measured by the Mean Time To Report (MTTRep). This indicator is interesting for transparency as it measures how rapidly incidents are reported to customers. The lower the timing value, the better. It can either be measured by calculating the average time necessary to generate a report on-demand (MTTRep1) or the average time necessary to generate a report after an incident occurred (MTTRep2).

$$MTTRep_1 = \frac{\sum(Time\ when\ report\ was\ received - Time\ when\ report\ was\ requested)}{number\ of\ reports\ generated}$$

$$MTTRep_2 = \frac{\sum(Time\ when\ report\ was\ received - Time\ when\ incident\ occurred)}{number\ of\ reports\ generated}$$

Overall evaluation of transparency (OET) is obtained by multiplying the scores of timing, accessibility and effectiveness. The lower the value is, the most transparent the system is.

$$OET = Timing\ \times Effectiveness\ \times Accessibility$$

3.4.2 Responsibility

We evaluate the level of authentication thanks to a scale which discriminates several scenarios based on whether system users are authenticated, their actions are traced and authorized. With this scale, it is possible to evaluate whether users can be individually identified, which can be useful for cases where individual responsibility is involved.

Authentication level	Description
0	Users are not authenticated; their actions are not traced and there is no access right management
1	Users are authenticated; their actions are traced and there is no access right management
2	Users are authenticated; their actions are traced and an access right management system is used to grant authorizations to perform actions

Table 5.Level of Authentication metric:

If we consider that a system can be represented in the form of a tree as illustrated in Figure 3, delegation of responsibility is the inverse of the length of the longest delegation chain of the system:

$$DR = \frac{1}{length\ of\ longest\ delegation\ chain\ in\ the\ system}$$

We propose to use a scale between 0 and 5 to evaluate the level of integrity of the logs produced by the system. With this scale, we can evaluate how hard it is to tamper with evidence and therefore the

level of trust that can be placed in it.

Integrity level	Description
0	There is no integrity-control mechanism in place
1	A simple integrity mechanism is in place without authentication. Typically, this means that logs are hashed but not signed.
2	Logs are hashed and signed with a symmetric-key based mechanism (e.g., HMAC)
3	Logs are hashed and signed with an asymmetric-key based mechanism (e.g., Digital Signature Algorithm or RSA)
4	Logs are hashed, signed with a symmetric-key based mechanism. The logs are crash- or fault-tolerant (meaning that an administrator can tell apart a real crash or fault from an attack)
5	Logs are hashed, signed with an asymmetric-key based mechanism. The logs are crash- or fault-tolerant (meaning that an administrator can tell apart a real crash or fault from an attack)

Table 6. Integrity metric

We define the Duty/role separation as the ratio of the number of tasks or functional blocks with regards to the number of actors which participate in the system

$$DS = \frac{number\ of\ functional\ blocks\ in\ the\ system}{total\ number\ of\ actors\ in\ the\ system}$$

The overall responsibility can be obtained by combining all the above-mentioned indicators related to responsibility:

$$ORL = Level\ of\ authentication\ \times level\ of\ integrity\ \times DR\ \times DS$$

3.4.3 Attributability

In INSPIRE5G+, this indicator is typically provided by Root Cause Analysis modules calculates a confidence score of the results they produce which corresponds to the precision (probability).

3.4.4 Liability

Liability can be measured by the penalties declared in the SLA and the risk exposure.

$$Risk\ exposure = Probability\ to\ violate\ SLA\ \times Penalties\ if\ SLA\ is\ violated$$

3.5 Status of SSLA

Service-level agreements (SLAs), have been investigated and adapted for network slicing, telecom and cloud infrastructure [44]. They represent contracts between service providers (SPs) and their customers to define services to be provided and the metrics by which their service standards are met. As different SPs differentiate security requirements on a vertical basis, especially in 5G contexts, security SLAs (SSLAs) plays indeed an important role for slice security assessment to declare the security level granted by SPs to verticals/end-users and the security constraints that should be fulfilled.

In this context, the main challenge is to provide an automated end-to-end management of the security constraints specified in SSLAs during the full lifecycle of a slice. We first need to collect security requirements of the verticals/end-users to configure the provided services and deploy the necessary

security controls to enforce the SSLAs. As SSLAs and even high/medium level policy descriptions only provide what to monitor in general (e.g., protocol, port, IP address), they do not contain any specific technical details on how to monitor and measure security requirements. Thus, producing monitoring rules and algorithms corresponding to the agreed SSLAs that allow specific monitoring tools to assess them in real-time is indeed necessary. If any violation is detected in security provisioning level, we notify both parties including SPs and end-users, and then apply reaction methods in real-time for triggering proper mitigation actions. Therefore, the INSPIRE5G-plus framework aims at allowing slice providers to offer tailored security features and deliver slices controlled by SSLAs to the verticals/end-users. It also specifies the security grants offered and continuously monitors the preservation of specific properties in order to support the satisfaction of the specified SSLAs at all times in each provided slice. We summarise some advances of SSLAs in both high and low levels in the next paragraphs.

Firstly, dynamic selection of enablers based on SSLAs provides a high-level of abstraction layer by using SSLAs which are independent to the underlying infrastructure, decoupling the security requirements of the specific implementations to deal with problems like heterogeneity and vendor-locking. This is especially useful in slicing environments where services including security must be adapted to available resources and constraints. Since the metrics can be associated with three different priority levels (“HIGH”, “MEDIUM” or “LOW”), for each capability described in the SSLAs, we identify a list of available enablers supporting all the metrics marked with a "HIGH" priority. It is logical as we favour first enablers that supports all the metrics with the highest priority level. Furthermore, we have chosen to classify the enablers according to the other supported metrics, favouring the greatest number of metrics with “MEDIUM” priority implemented, then the greatest number of metrics with “LOW” priority. Overall, this selection strategy is effective, as only the enablers that comply correctly with the critical points are chosen without becoming too drastic. Indeed, we avoid cases where our selection strategy would return an empty set of enablers.

Secondly, real-time monitoring of SSLAs (RT-SSLAs) and their continued assessment is of great added value for both end-users and service providers since it improves the trustworthiness of the services. RT-SSLAs can facilitate the ability to gain more insight concerning which system modules are responsible for any detected faults and problems, or the poor performance of a running component. The aim is providing an automated SSLA-based monitoring framework that requires a minimum amount of input from the users. First, we produce the security rules of the monitoring tools from the specified set of high-level security specifications, such as SSLAs, or from different levels of security policies. The deployment of the security monitoring tools allows us to detect anomalies or attacks in real-time and consequently generate security reports that will be used by other enablers (e.g., Decision Engine) to perform the necessary mitigation actions. Finally, we configure the monitoring tools to dynamically adapt to the runtime changes in the execution environment by enforcing, as quickly as possible, the configurations generated for the enforcement of new or modified network topologies and security policies. RT-SSLA rule templates can be predefined using the type of security policies (e.g., related to filtering, anomaly detection, IoT network behaviour) and crucial information extracted from security policies.

4 Liability Management Functional Blocks

The deliverables D4.1 and D4.3 identify and explore the duality between trust and liability. Both deliverables highlight that as zero-risk security cannot be achieved, defining liability and responsibilities when security breaches occur is of paramount importance to support confidence between parties and compliance with regulation. As a result, we identified three functional blocks (FB) which are necessary to achieve liability management. Each enabler is mapped with at least one of these functional blocks and with the INSPIRE5G+ HLA in section 4.

FB.1: Defining accountability and liability relationships. This functional block consists in identifying the governance required to set up the E2E or Domain service, the evidence required to demonstrate compliance to regulation and contractual agreements and the liability relationships among actors (customers, E2E or domain service providers and subcontractors). Concretely, this functional block consists in knowledge models which describe the responsibilities, the associated commitments and accepted evidence defined in contracts and regulation, as well as translation tools to configure the components of the functional blocks FB2 and FB3.

FB.2: Monitoring for accountability evidence. Security agents collect the evidence from the infrastructure as identified by the first functional block. The first objective is to demonstrate compliance with legal obligations or contractual agreements by using Remote Attestations, Path Proof Protocol or by collecting logs. The second objective is to identify and trace events or incidents for example by setting up anomaly detection of Security Information & Event Management systems.

FB.3: Analyse, resolve & identify liabilities. FB.3 analyses the evidence of events/incidents collected by FB.2. Based on the liability relationships identified by FB.1, FB.3 can qualify compliance or potential violations and resolve responsibilities. FB.3 then provides reports to administrators or jurists to support further forensic investigations or negotiations to settle disputes.

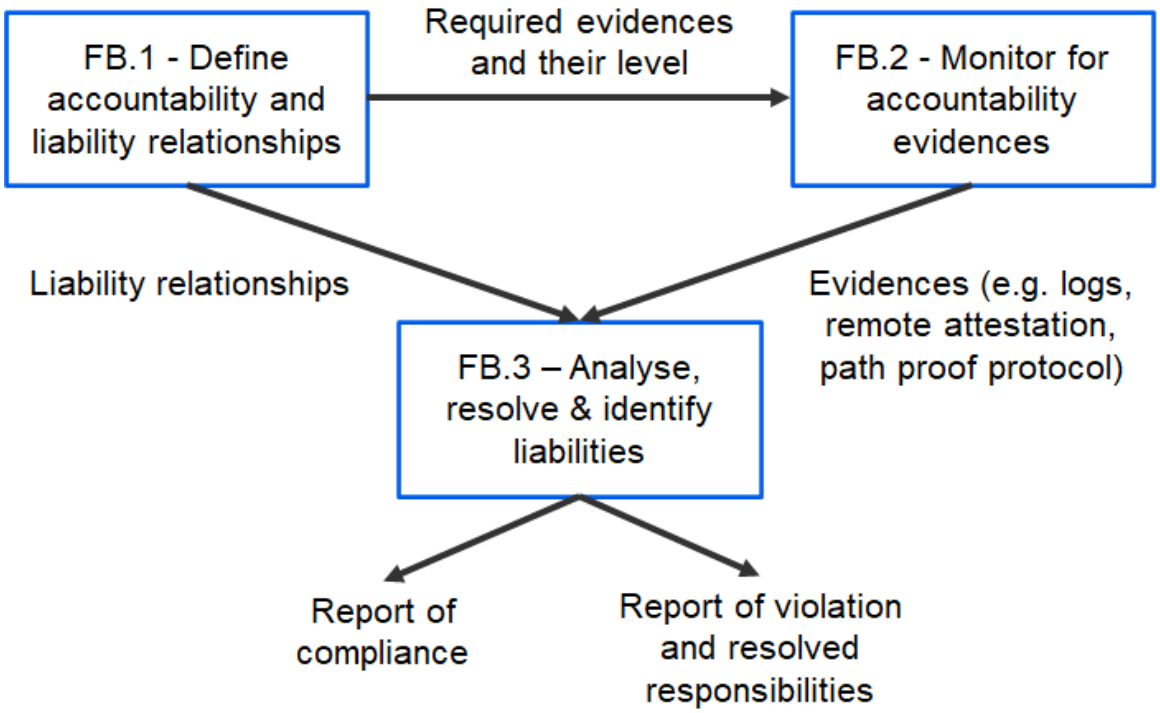


Figure 4. Liability management functional blocks

5 Enablers Status

This section gives an overview of how INSPIRE5G-Plus enablers contribute to liability management. First, this deliverable describes how the functional blocks of a liability management system can be mapped with the INSPIRE-5GPlus High Level Architecture (HLA). Second, this deliverable describes where the enabler is described in detail. Then, the enabler is mapped within the HLA and a sequence diagram illustrates how the enabler interacts with other HLA components. Finally, the enabler is mapped with the functional blocks of a liability management system and with the various sets of KPIs that have been proposed in the scope of INSPIRE-5GPlus.

5.1 Mapping of liability management system functional blocks and HLA

We mapped the liability management system functional blocks described in section 4 with the HLA architecture components and show the results in Table 7.

The Policy and SSLA management component, whether at E2E or Domain level, cover the function dedicated to the definition of accountability and liability relationships (FB.1). Indeed, at E2E level, this component is configured with data which emanate from the contract binding the E2E Service Provider to the 5G Vertical customer or the contract binding the E2E Service Provider and its suppliers, the Domain Service Providers. At Domain level, the Policy and SSLA management component is configured with data from the contract binding the Domain Service Provider and its customer, the E2E Service Provider. It is also configured with data from contracts binding the Domain Service Provider and its suppliers.

All the other components of the HLA, namely the Security Orchestration, the Decision engine, the Trust management, the Security Analytics Service collect data which can demonstrate whether for a task the commitment is fulfilled or not. Therefore, they all contribute to the second functional block of a liability management system.

The E2E or Domain Security Analytics Services aim at analysing anomalies and incidents thus covering the third functional block of a liability management system.

HLA Component	Mapping with HSL functional block
E2E or Domain Policy and SSLA management	FB.1 – Define accountability and liability relationships
E2E or Domain Security Orchestration	FB.2 – Monitor for accountability evidence
E2E or Domain Decision engine	FB.2 – Monitor for accountability evidence
E2E or Domain Trust management	FB.2 – Monitor for accountability evidence
E2E or Domain Security Analytics Service	FB.2 – Monitor for accountability evidence FB.3 – Analyse, resolve and identify liabilities

Table 7. Mapping of HLA and liability functional blocks

5.2 Trust enablers status and mapping

This section gives an overview of the contribution of the Liability enablers in INSPIRE-5Gplus project. First, we list in Table 8, the enablers and potential earlier complete description. Second, the enabler is placed in the context of the HLA. A UML sequence diagram details the interaction with the main HLA components. Finally, each enabler is mapped with a liability functional block.

Enabler Name	Owner	Latest published description
Manifest	ORA	D4.3
Liability-Aware Service Management (LASM)	ORA	MS8
Similarity-based Root Cause Analysis (RCA)	MI	MS7
Root Cause Analysis (RCA-VNF)	ORA	D4.2
Path Proof Protocol (PPP)	ORA	MS8
Risk Analysis Graphs	ORA	D4.1
Behavioural profile	UMU	D4.2
Security-by-Orchestration	ORA	MS8
GRALAF	ZHAW	MS8
Systemic	TAGES	D4.2
DiscØvery	CLS	D3.4

Table 8. List of T4.4 enablers

5.2.1 TRAILS Manifest

5.2.1.1 Description

As described in D4.3 [40], TRAILS manifests are descriptors which keep track of the responsibilities and usage conditions throughout a network component's lifecycle. For a thorough description of the TRAILS manifest, please refer to D4.3 [40].

5.2.1.2 Mapping with HLA

TRAILS manifests are typically used within the E2E or Domain Policy & SSLA management modules. It is used by the Liability-Aware Service Manager enabler.

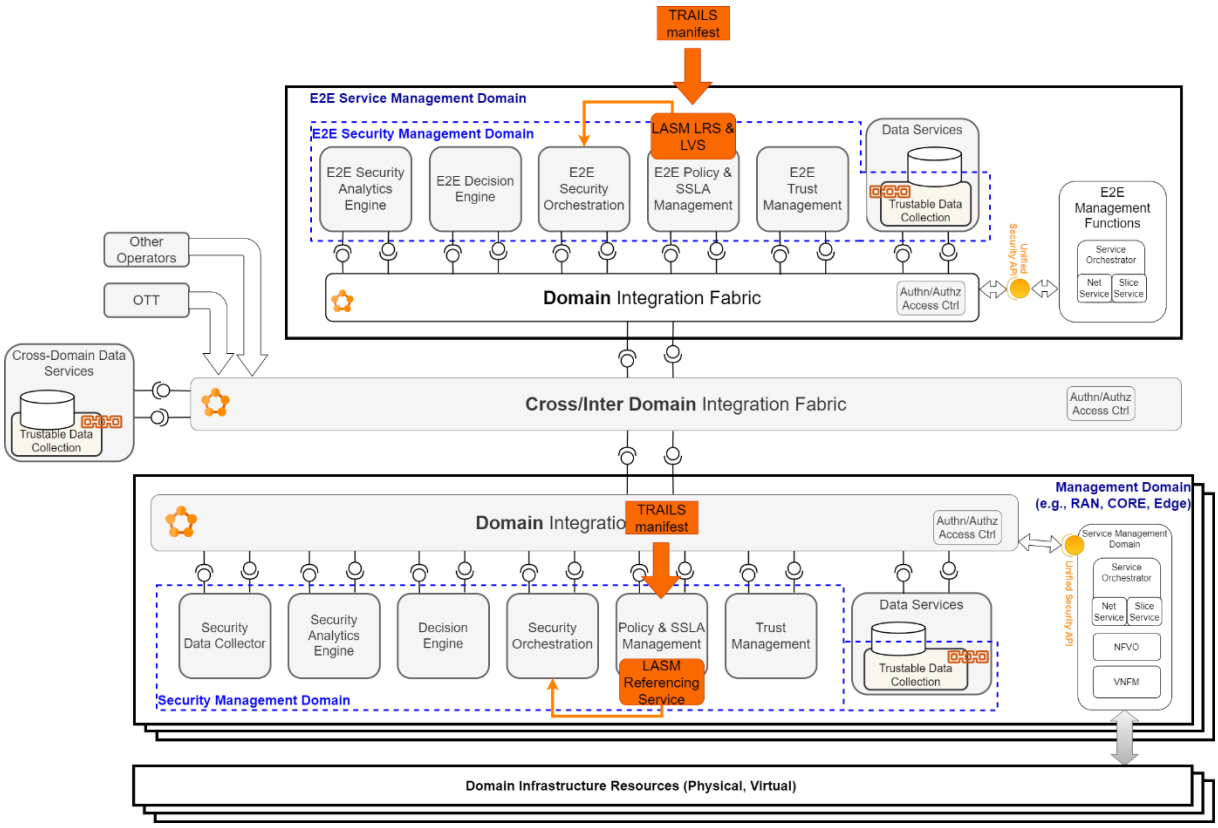


Figure 5. Mapping of the TRAILS manifest with HAL architecture

5.2.1.3 UML sequence diagram

This diagram represents the sequence to reference the TRAILS manifest of a network component in the LASM Referencing module. When the administrator requests to reference a new network component with its TRAILS to the LASM, the LASM applies a referencing policy to the content of the TRAILS. This referencing policy is expressed thanks to an ontology. Depending on the result of the reasoning, the manifest is either accepted and referenced or accepted but its TRAILS manifest is modified to express operational constraints before being referenced or rejected.

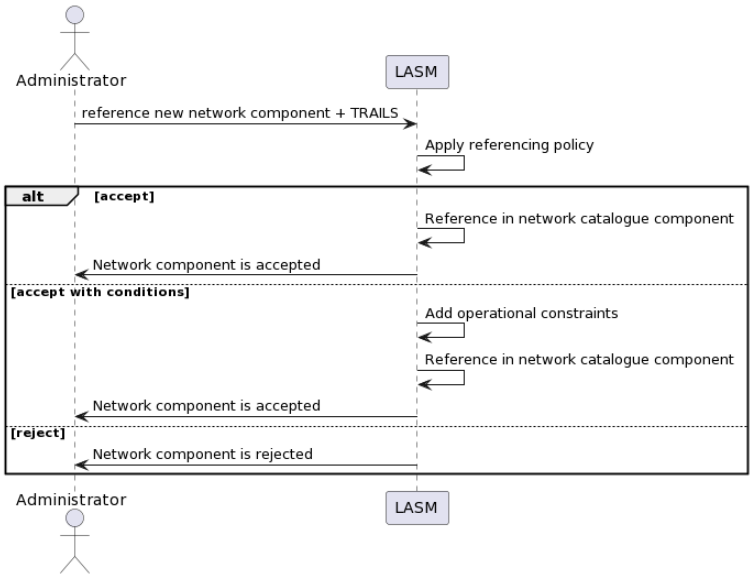


Figure 6. Sequence diagram of the referencing of a new network component.

5.2.1.4 Mapping with Liability Functional Blocks

Manifests are part of the first functional block "Define accountability and liability relationships" because they contain information which allows to identify commitments (SLA) and responsibilities (endorsed with signatures).

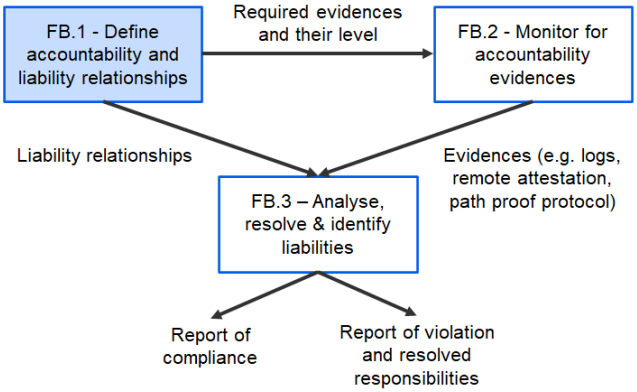


Figure 7. Mapping of manifests with liability-aware management functional blocks

5.2.1.5 Mapping with metrics

5.2.1.5.1 MS9 metrics

All MS9 metrics can be used to express SLAs that are referenced in the TRAILS manifest.

Generic KPIs	Mapping
Mean Time To Detect	This metric can be used to express an SLA in the TRAILS
Mean Time to Contain	This metric can be used to express an SLA in the TRAILS
Mean Time to Resolve	This metric can be used to express an SLA in the TRAILS
Transaction speed	This metric can be used to express an SLA in the TRAILS
Packet Loss Ratio	This metric can be used to express an SLA in the TRAILS
Number of False positives	This metric can be used to express an SLA in the TRAILS
Number of False negatives	This metric can be used to express an SLA in the TRAILS
Initial time	This metric can be used to express an SLA in the TRAILS
Migration time	This metric can be used to express an SLA in the TRAILS
Service response time	This metric can be used to express an SLA in the TRAILS
Service downtime	This metric can be used to express an SLA in the TRAILS

Generic KPIs	Mapping
SSLA enforcement	This metric can be used to express an SLA in the TRAILS

Table 9. Mapping with MS9 Generic KPIs

Test-Case-Specific KPIs	Mapping
Blocked adversarial examples rate	This metric can be used to express an SLA in the TRAILS
Ratio of allowed malicious scale-up	This metric can be used to express an SLA in the TRAILS
Automated vulnerability assessment	This metric can be used to express an SLA in the TRAILS
Automated model generation	This metric can be used to express an SLA in the TRAILS
Threat assessment	This metric can be used to express an SLA in the TRAILS
Cyber-security insights assessment	This metric can be used to express an SLA in the TRAILS
Latency	This metric can be used to express an SLA in the TRAILS
Mean Time to implement the MTD action	This metric can be used to express an SLA in the TRAILS
MTD action cost	This metric can be used to express an SLA in the TRAILS
Protection gain of an MTD policy	This metric can be used to express an SLA in the TRAILS
Mean decision time for MTD action	This metric can be used to express an SLA in the TRAILS
QoS gain/loss of the protected resources	This metric can be used to express an SLA in the TRAILS

Table 10. Mapping of MS9 Test-case Specific KPIs

5.2.1.5.2 MS10 metrics

MS10 metrics can be used to express SLAs that are referenced in the TRAILS manifest

MS10 additional KPI	Mapping
Mean Time To Detect that a function has been tampered with or is in incorrect location	This metric can be used to express an SLA in the TRAILS
Mean Packet Loss Ratio during the switch between normal to critical mode	This metric can be used to express an SLA in the TRAILS
Mean Ratio of Time Functions are Not isolated In Critical mode	This metric can be used to express an SLA in the TRAILS

MS10 additional KPI	Mapping
Mean Observation Report Request Response Time corresponds to the mean time required to provide an observation report after it was requested	This metric can be used to express an SLA in the TRAILS

Table 11. Mapping of MS10 Additional KPIs

5.2.1.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

The responsibility dilution can be calculated based on TRAILS manifest

Liability KPIs	Mapping
Accessibility	This metric can be used to express an SLA in the TRAILS
Effectiveness	This metric can be used to express an SLA in the TRAILS
Timing (Mean Time To Report)	This metric can be used to express an SLA in the TRAILS
Overall Evaluation of Transparency	This metric can be used to express an SLA in the TRAILS
Level of Authentication	This metric can be used to express an SLA in the TRAILS
Integrity	This metric can be used to express an SLA in the TRAILS
Delegation of responsibility	Not relevant
Overall responsibility level	This metric can be used to express an SLA in the TRAILS
Precision of Root Cause Analysis	This metric can be used to express an SLA in the TRAILS
Penalties	This metric can be expressed within the expression of an SLA
Risk Exposure	Not Relevant

Table 12. Mapping with MS9 Generic KPIs

5.2.2 Liability-Aware Service Management

5.2.2.1 Description

The Liability-Aware Service Management (LASM) is a tool that help Infrastructure administrators in their management decision to achieve the commitments made by the different stakeholder in the service. As depicted in Figure 8, the LASM is a modular service where each module communicates through a Kafka bus.

The first service, LASM Visualization Service (LVS), deals with the presentation of services and data. The second one, LASM Referencing Service (LRS), catalogues the available network components and their TRAILS profiles. It provides tools to evaluate a new component's TRAILS with regards to a referencing policy or research for a profile with specific features. The fourth, LASM Analysis Service

(LAS), evaluates various metrics related to trust, responsibility or reputation of components and authors. Finally, the LASM Orchestration & Deployment Service (LODS) ensures the link with dedicated orchestrators or managers such as a MANO or an SD-IoT manager. Only the LRS and LVS modules have been developed in the scope of the project INSPIRE-5GPlus, therefore the rest of the document will concentrate on them both.

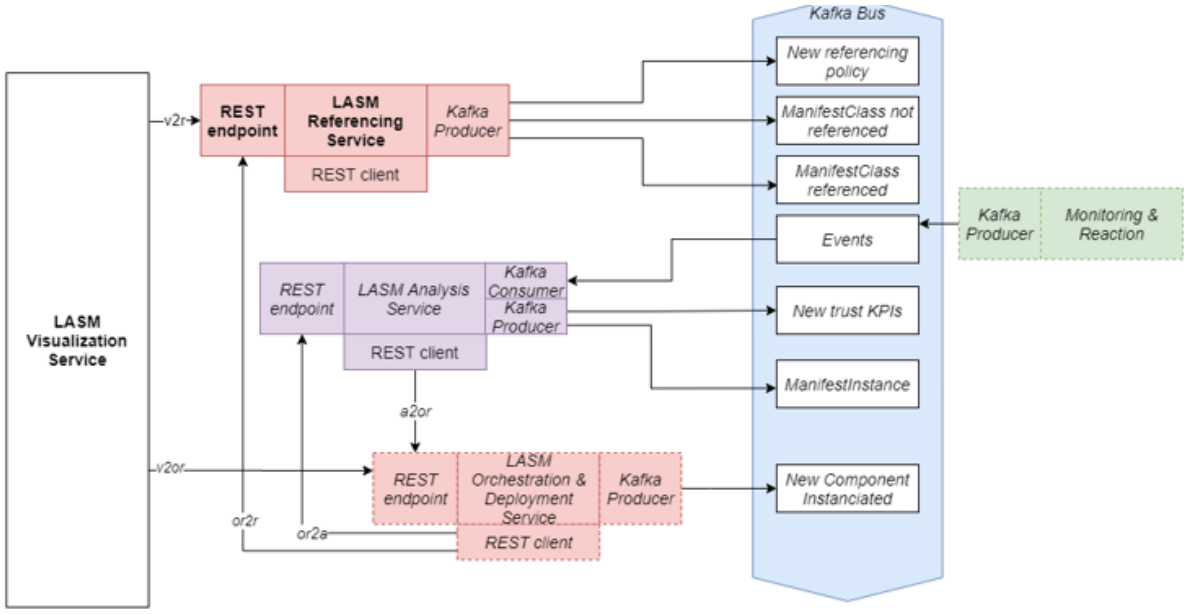


Figure 8. LASM architecture

5.2.2.2 Mapping with HLA

The Liability-Aware Service Manager enabler consumes TRAILS manifests. Then, the LASM Referencing Service can be used to find network components within a catalogue.

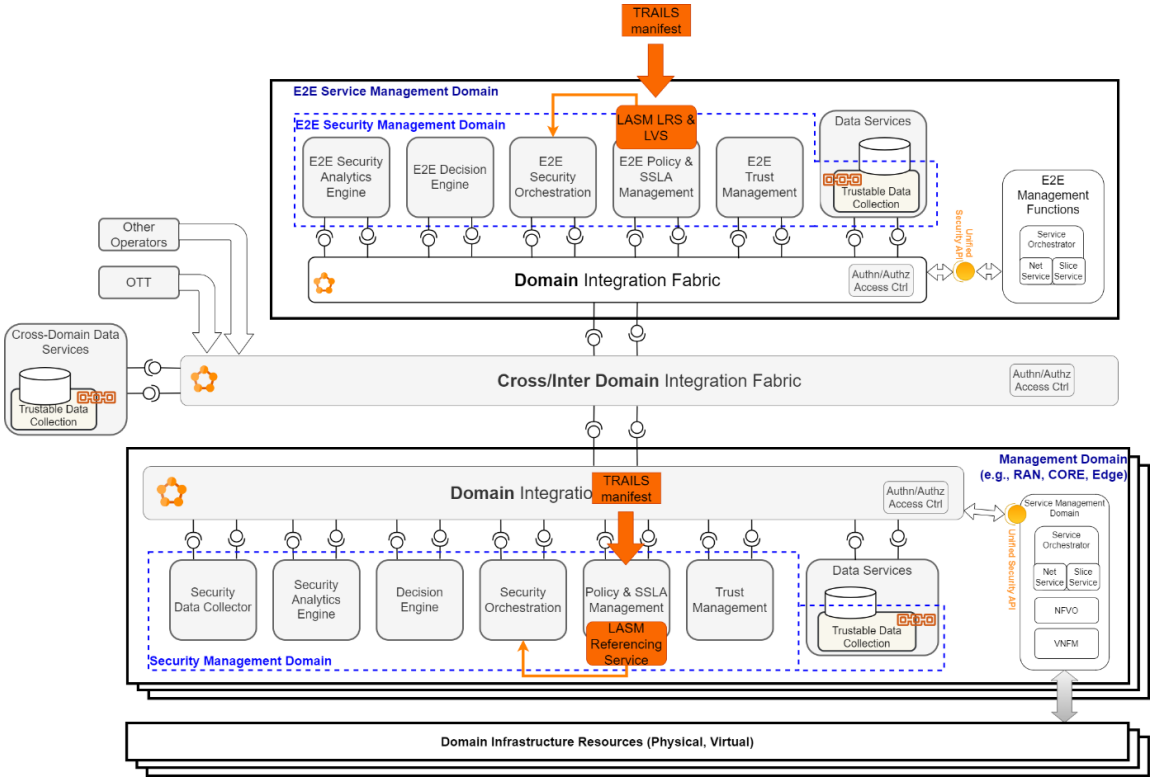


Figure 9. Mapping of the LASM Referencing Service with HLA architecture

5.2.2.3 UML sequence diagram

This sequence diagram represents how the LASM referencing service can retrieve from the catalogue a list of network components which match a description provided by the Security Orchestration.

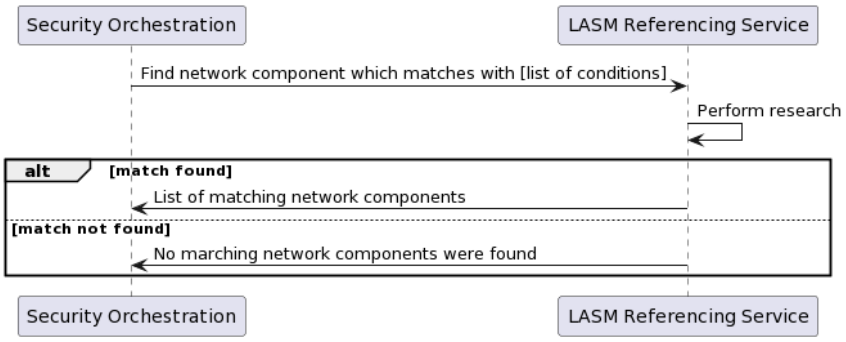


Figure 10. Sequence diagram to find network services which match a security orchestrator request.

5.2.2.4 Mapping with Liability Functional Blocks

The LASM is part of the FB.1 “Define accountability and liability relationships” because it contains an ontology which can be used to define a referencing policy to automate the decision to add a network component to the catalogue or not. The Security Orchestration module can then query the LASM in order to find a specific network component which complies with specific conditions on SLA or responsibilities.

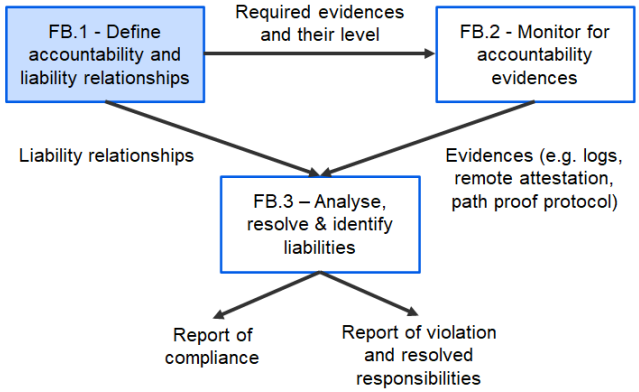


Figure 11. Mapping of LASM with liability-aware management functional blocks

5.2.2.5 Mapping with metrics

5.2.2.5.1 MS9 metrics

All MS9 metrics can be used to express SLAs. Then, an orchestrator can query the LASM referencing service to retrieve a list of network components which commit to specific SLAs.

5.2.2.5.2 MS10 metrics

All MS10 metrics can be used to express SLAs. Then, an orchestrator can query the LASM referencing service to retrieve a list of network components which commit to specific SLAs.

5.2.2.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

The current version of the LASM, does not support accountability / liability metrics.

5.2.3 Similarity-based Root Cause Analysis

5.2.3.1 Description

Security monitoring of 5G IoT networks requires not only the detection of failures or degraded performance but also determining and identifying the causes (e.g., intrusions, denial of services, compromised devices, etc. or just normal wear-and-tear) as a prerequisite for triggering corrective actions. For addressing this need, the enabler involves meaning from experience to determine the most probable cause of any detected malfunctioning. The RCA-M machine learning approach developed in INSPIRE-5Gplus considers highly granular monitoring indicators (e.g., statistics and data extracted from the logs, metrics, network traffic, and any data that could identify the system state) and performs deep analysis to assess the similarity of a newly observed event reflecting the current system status and each past experience recorded in the historical database. This RCA-M enables systematizing the experience in dealing with incidents to build a historical database and verify whether a newly detected incident is similar enough to an observed one with known causes. Thanks to the suggestions provided by the RCA-M, remediation actions could be timely and wisely taken to prevent or mitigate the damage of reoccurring similar problems.

5.2.3.2 Mapping with HLA

The RCA-M is part of the Decision Engine, as shown in Figure 12. It receives information from the Security Analytics Engine or the SSLA assessment module; historical root cause-related information from the Data Services and stores new information; and, finally it notifies the Security Orchestrator so that corrective actions can be taken.

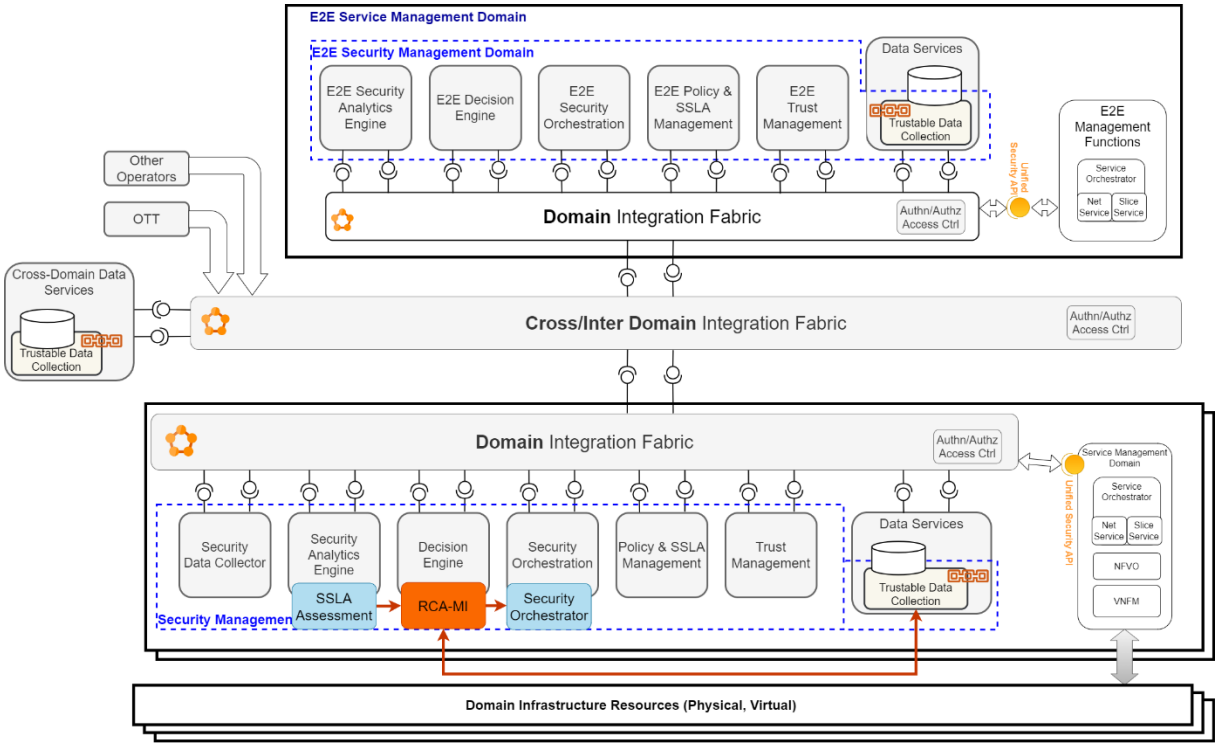


Figure 12. Mapping of RCA-MI in the INSPIRE-5Gplus HLA

5.2.3.3 UML sequence diagram

Figure 13 demonstrates the UML sequence diagram of RCA-MI which consists of two phases: (Supervised) Learning Phase and (Live) Monitoring Phase. The RCA-MI is capable of extracting the features characterizing the incidents and calculating the similarity to the learned ones to detect the recurrence with known causes.

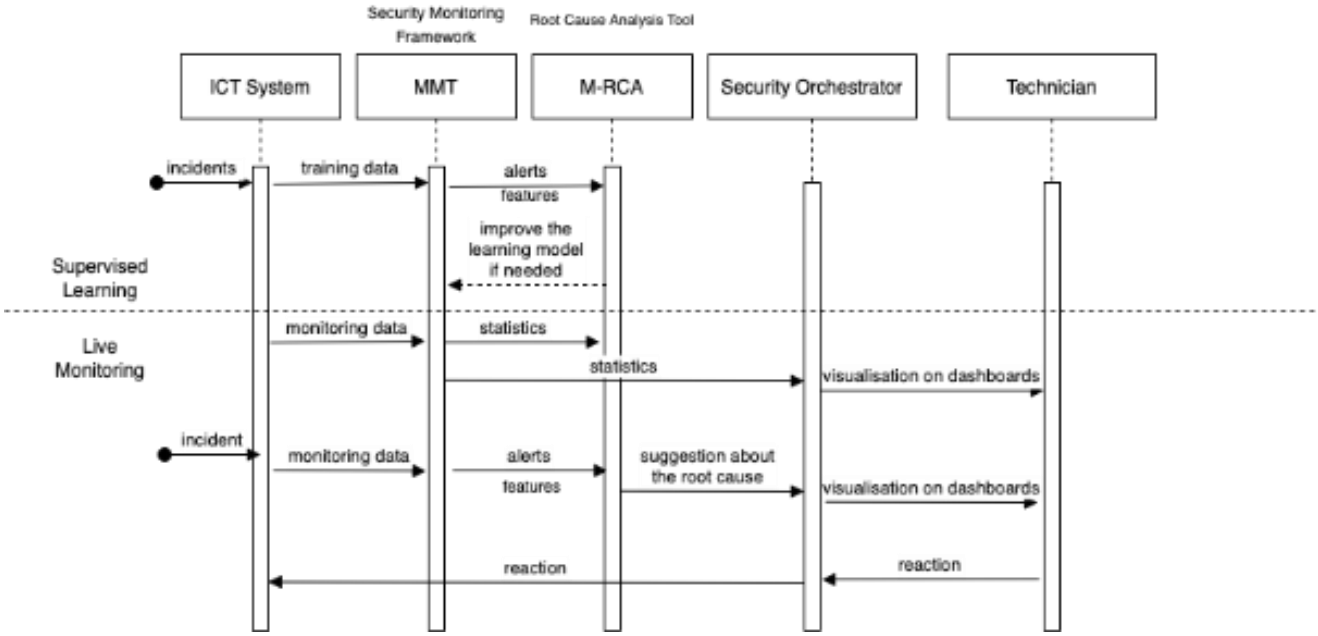


Figure 13. Sequence diagram of RCA-MI.

5.2.3.4 Mapping with Liability Functional Blocks

The RCA-M is part of the FB.2 and FB.3 as it consists of:

- One or several probes collecting the evidence (logs, network traffic, exchanged messages) from the infrastructure to identify and trace events or incidents
- A Security Analytic and a Machine Learning-based Root-cause Analysis module analysing the evidence of events/incidents collected to qualify compliance or potential violations and resolve responsibilities. Reports can be exported and provided to administrators or jurists to support further forensic investigations or negotiations to settle disputes.

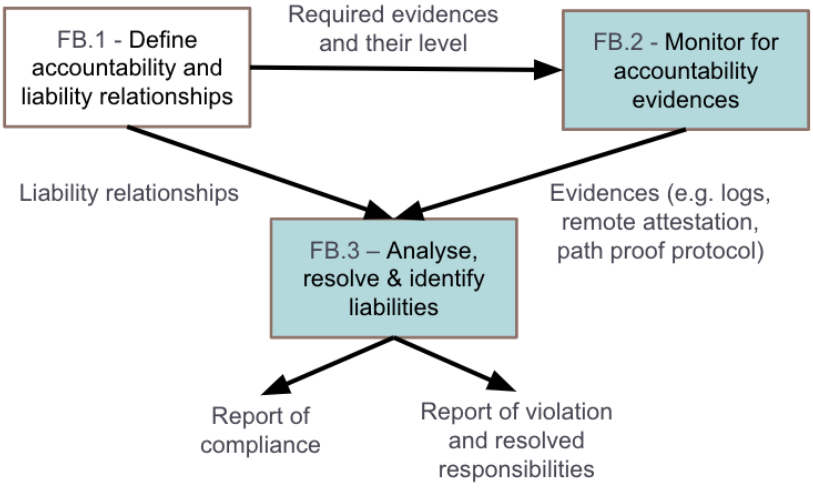


Figure 14. Mapping of RCA-M with liability management system functional blocks.

5.2.3.5 Mapping with metrics

5.2.3.5.1 MS9 metrics

Generic KPIs	Mapping
Mean Time To Detect	The average length of time between the start of an incident's recurrence and their discovery based on the similarity score.
Mean Time to Contain	Not Relevant
Mean Time to Resolve	Not Relevant
Transaction speed	Not Relevant
Packet Loss Ratio	The ratio of the number of data packets lost to the total number of packets that should have been received and processed by MMT.
Number of False positives	If the M-RCA detects a recurrence of an incident but it is actually not, this is considered as a false positive.
Number of False negatives	If an incident's recurrence takes place but M-RCA do not detect it, this is considered as a false negative.
Initial time	The delay needed so that M-RCA starts or restarts
Migration time	Not Relevant
Service response time	Not Relevant
Service downtime	Not Relevant
SSLA enforcement	Not Relevant

Table 13. Mapping with MS9 generic KPIs

5.2.3.5.2 MS10 metrics

M-RCA KPIs have been considered in MS 10 with the specific KPIs listed below:

- **% Packet lost**:
  - Number of packets processed by MMT/ Number of packets captured by the IoT Sniffer
  - Number of packets captured by the IoT Sniffer vs Number of packets exchange/ collected by the IoT Border Router.
- **Response time (real time / near real time):**
  - Anomaly detection delay
  - Root-cause determination delay
- **Confidence:**
  - Similarity score: The higher similarity score represents a higher confidence.
  - Number of supervised learning datasets: The bigger number of datasets represents a higher confidence.

5.2.3.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

Attribute	ID	Dimensions	Adaptation in the context of INSPIRE5G-Plus
Transparency	T1	Accessibility	Not Relevant
	T2	Effectiveness	Not Relevant

Attribute	ID	Dimensions	Adaptation in the context of INSPIRE5G-Plus
	T3	Timing	✓
	T4	Overall evaluation of transparency	Not Relevant
Responsibility	R1	Level of Authentication	✓
	R2	Delegation of Responsibility	✓
	R3	Integrity	Not Relevant
	R4	Duty/Role separation	Not Relevant
	R4	Overall Responsibility Level	Not Relevant
Attributability	A1	Attributability	✓
Liability	L1	Penalty	Not Relevant

Table 14. Mapping with accountability: liability metrics adapted from the state of the art of Inspire5G+

5.2.4 Root Cause Analysis for VNF

5.2.4.1 Description

The aim of RCA-VNF is to find the root cause dynamically concerning SDN networked topologies, where the network topology may evolve due to network reconfiguration and changes. It can detect new network elements when connected to the network topology and instantiate their inner dependencies and connect those to the network dependency graph by regenerating it every time there is a change. Overall, it can contribute to the resilience of 5G networks, as the RCA can identify those networked elements that are under failure and have to be replaced or disconnected from the network topology (quarantine).

The RCA is key for liability purposes, where there is need to know the identifier of those network elements whose performance is far from normal, due to operational misbehaviours, of intentional ones.

Further information on the inner functioning of the VNF-RCA is given in D4.6 deliverable.

5.2.4.2 Mapping with HLA

As far as the mapping with HLA is concerned, the RCA is highly related to the e-TRM, already described in deliverable D4.2.

To sum up, The RCA is embedded in the Security Analytics Engine, where it sends the network graph and probabilistic graph to the eTRM to compute reputation based on those probabilities. On the other hand, the TRM is located in the Trust Management, where it provides the reputation metrics as additional indicator to the security orchestrator to warn about risky networked elements, including the SDN controller. Those interactions are further described in he below figure:

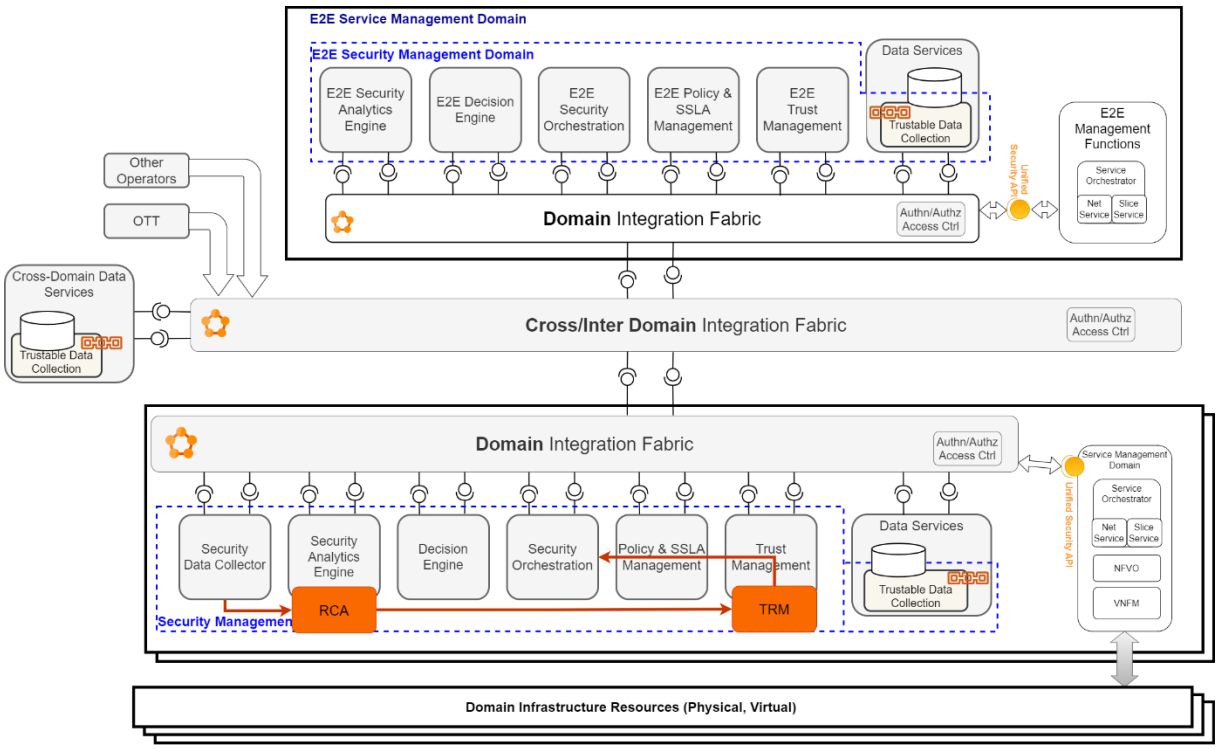


Figure 15. Mapping of manifests of RCA-VNF and e-TRM on the HLA

5.2.4.3 UML sequence diagram

Figure 18 shows the corresponding sequence diagram concerning the RCA-VNF. It works as follows:

- Firstly, the RCA gets the network topology (1) from the SDN controller.
- Secondly, the Root Cause Analysis enabler computes the probability of fault for each network equipment inside that domain and updates the network topology with those values (2). The network topology provided is given in the shape of network graph updated with the fault probabilities computed by means of Machine Learning (ML) algorithm based on Bayesian Networks.
- Finally, the RCA sends that information to the e-TRM which will convert those probability values to reputation ones to be send to the Security orchestration (3).

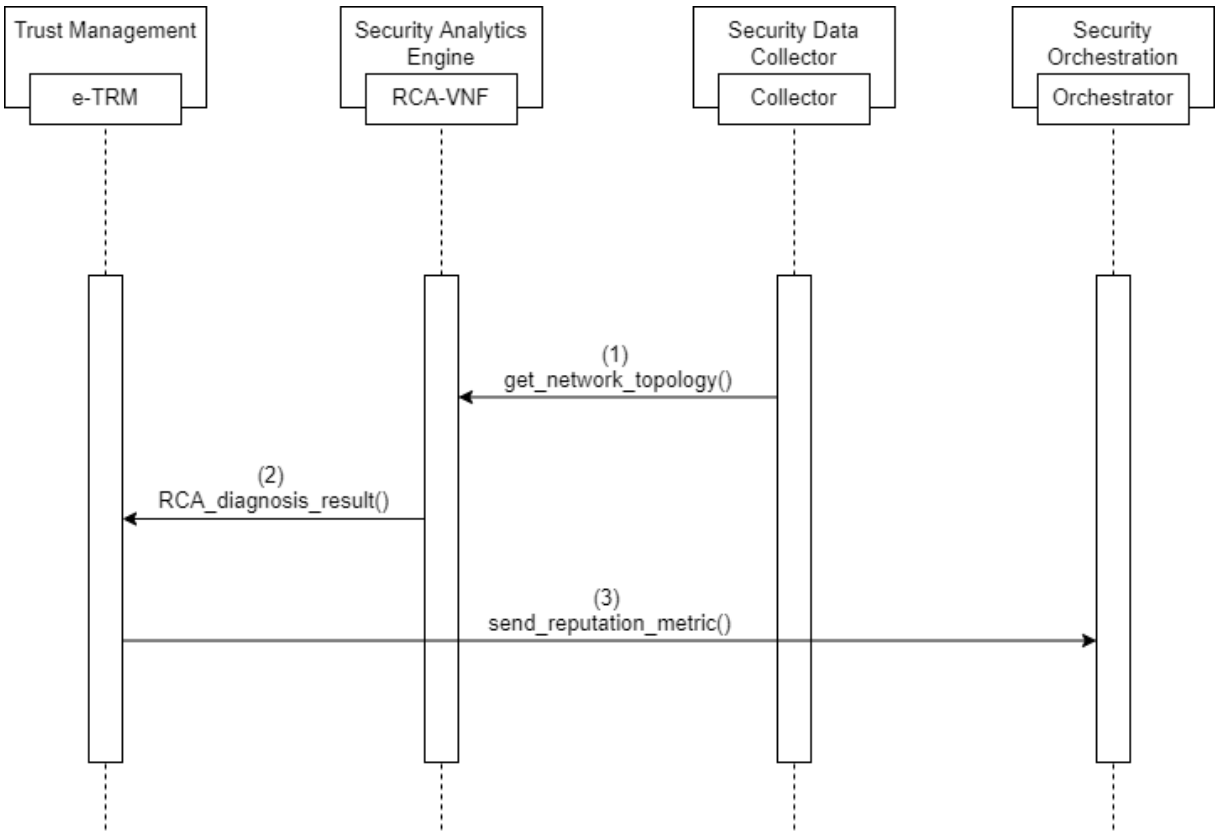


Figure 16. UML sequence diagram for the RCA-VNF

5.2.4.4 Mapping with Liability Functional Blocks

The RCA-VNF is part of the FB.2 "Monitor for accountability evidences" because the RCA-VNF can detect changes on the network topology and pinpoint those network elements being the root cause of malfunctions in services deployed over a SDN infrastructure.

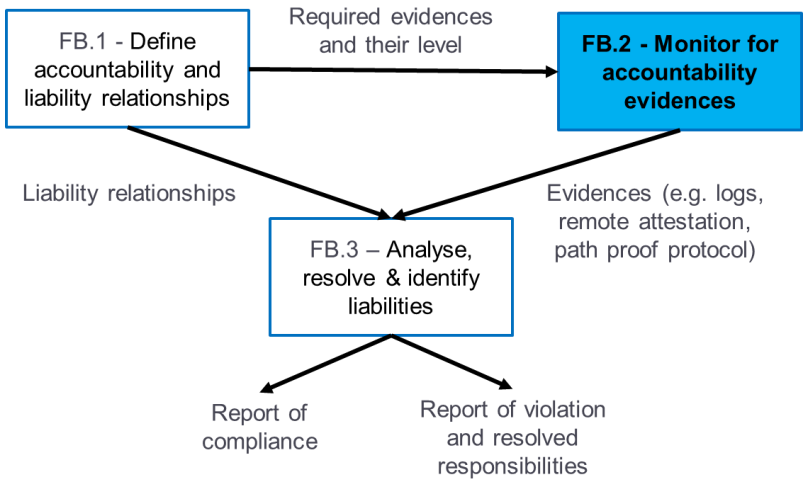


Figure 17. Mapping of RCA-VNF with liability-aware management functional blocks

5.2.4.5 Mapping with metrics

5.2.4.5.1 MS9 metrics

Those metrics identified to be mapped with the RCA-VNF enabler are on one hand the generic KPI service downtime metric and the test case specific KPI known as automated model generation. The former is by detecting when a service deployed on a SDN infrastructure becomes unavailable, the latter is by generating a model in the shape of network graph (dependency graph) corresponding to the current network topology at a given timeslot.

5.2.4.5.2 MS10 metrics

No MS10 metrics have been identified to be mapped with the RCA-VNF so far at this stage of the project.

5.2.4.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

The current version of the RCA-VNF, does not support accountability / liability metrics.

5.2.5 Path Proof Protocol

5.2.5.1 Description

Hijacking attacks have existed for a long time. On Internet, they consist in deviating the traffic on a given route to make it travel through unexpected nodes. The PP enabler addresses the hijacking attack without relying on the routing protocol specificities. Instead, we propose an original application-layer approach that relies on a two-party cryptographic-based anomaly detection protocol, which measures the communication time between users. It performs statistical analysis upon these measurements and a trusted sample.

5.2.5.2 Mapping with HLA

Path Proof enabler can be part of the Trust Management Block. A shown in Figure 18, Path Proof enabler can have input from “Domain Infrastructure resources”, “Security analytics Engine”, “Data Services”, “Service Management Domain” and its outputs can be used by the “Decision Engine” and the Security Management Domain”.

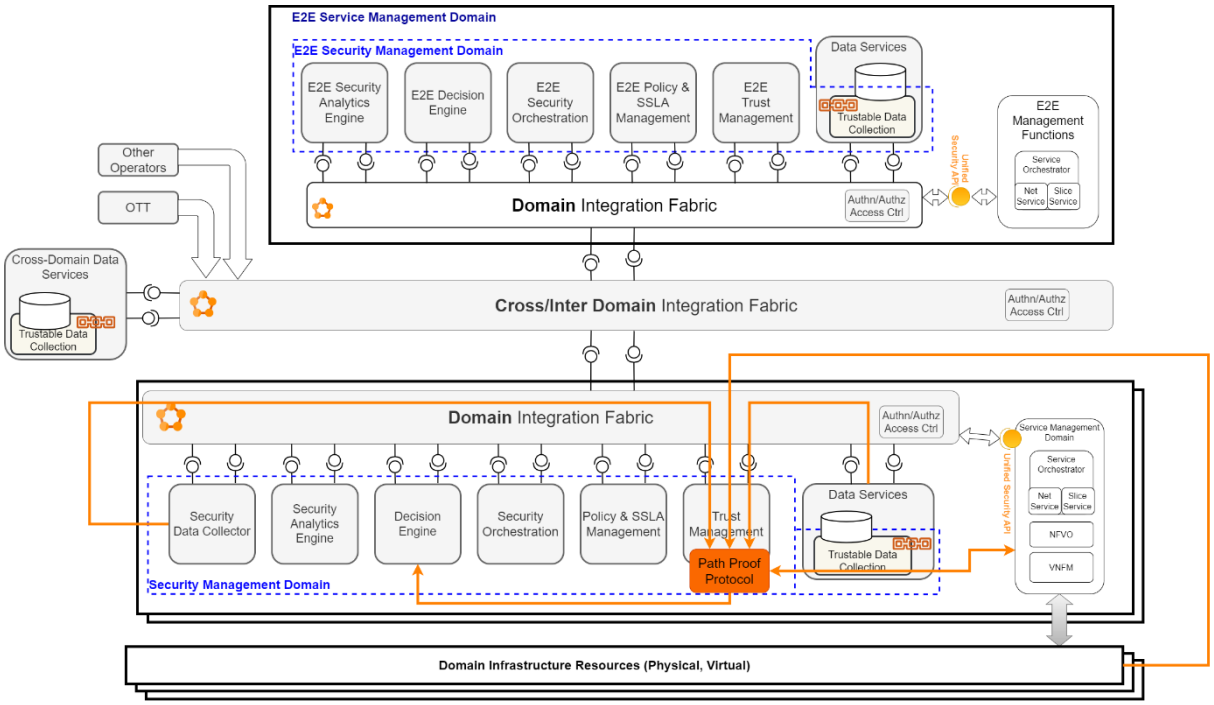


Figure 18: Path Proof Enabler Mapping with HLA

5.2.5.3 UML sequence diagram

In Figure 19, an administrator starts by registering the nodes that can be later involved in the Path Proof Protocol. A node can be identified for example by its IP address. Upon receiving the registration request, the PP Server registers the nodes (e.g., check that an Attestation Agent is correctly running in the node). The Administrator can then start the Path Proof Protocol between two registered nodes. At the end, the sender node sends the results (i.e., OK: no hijack detected; KO: a hijack has been detected)

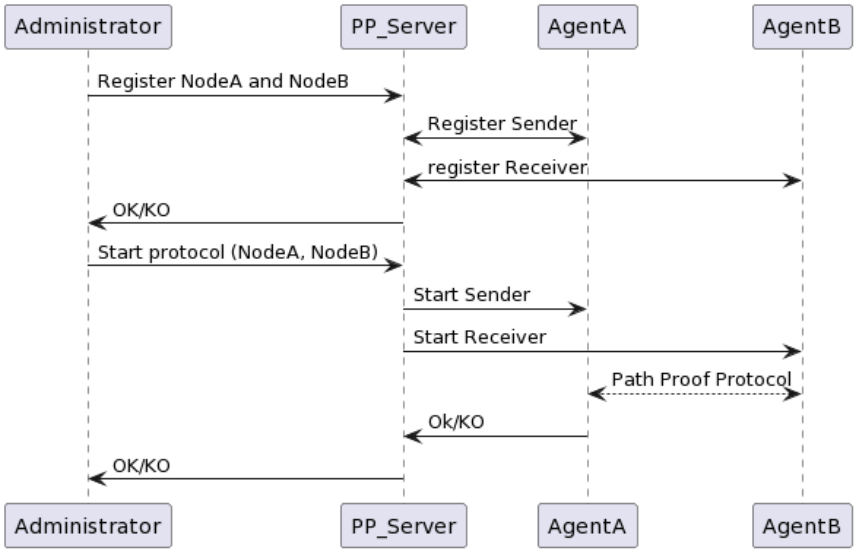


Figure 19: Path Proof - UML diagram

5.2.5.4 Mapping with Liability Functional Blocks

The Path Proof enabler is part of the second functional block as it enables to verify if a traffic between two endpoints has been hijacked or not.

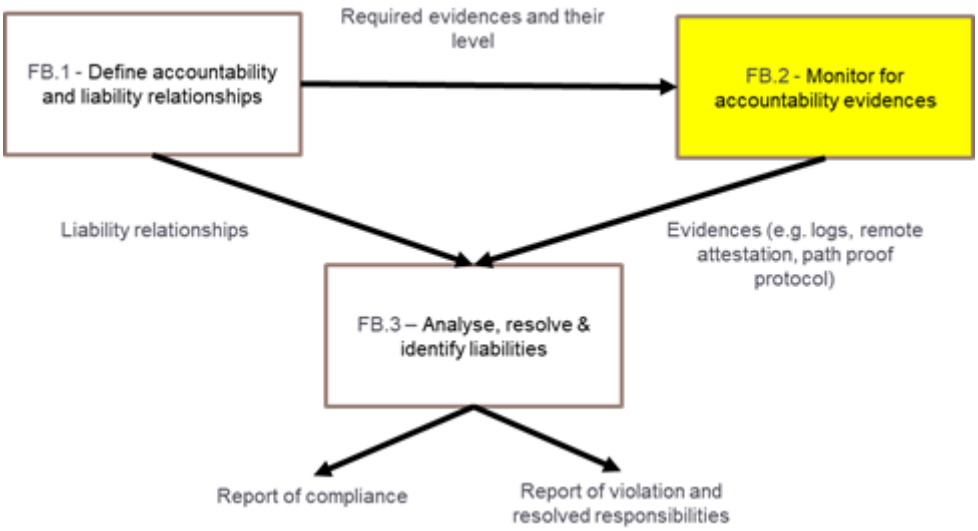


Figure 20: Path Proof enabler - Mapping with Liability Functional Blocks

5.2.5.5 Mapping with metrics

5.2.5.5.1 MS9 metrics

Generic KPIs	Mapping
Mean Time To Detect	Not Relevant
Mean Time to Contain	Not Relevant
Mean Time to Resolve	Not Relevant
Transaction speed	Not Relevant
Packet Loss Ratio	Not Relevant
Number of False positives	We made analysis to choose the right parameters to have 0% of false positives (A false positive is when the PP enabler detects a hijack however this is not the case.)
Number of False negatives	We made analysis to choose the right parameters to have 0% of false negatives (a false negative is when the PP enabler does not detect a hijack of the traffic.)
Initial time	Not Relevant
Migration time	Not Relevant
Service response time	Not Relevant
Service downtime	Not Relevant
SSLA enforcement	Not Relevant

Table 15. Mapping with MS9 generic KPIs

Test-Case-Specific KPIs	Mapping
Blocked adversarial examples rate	Not Relevant
Ratio of allowed malicious scale-up	Not Relevant
Automated vulnerability assessment	Not Relevant
Automated model generation	Not Relevant
Threat assessment	Not Relevant
Cyber-security insights assessment	Not Relevant
Latency	We analysed the impact of our PP protocol when sending a file between two endpoints. We also have analysis of the impact of the number of packets, the number of sessions and the packet size.
Mean Time to implement the MTD action	Not Relevant
MTD action cost	Not Relevant
Protection gain of an MTD policy	Not Relevant
Mean decision time for MTD action	Not Relevant

Test-Case-Specific KPIs	Mapping
QoS gain/loss of the protected resources	Not Relevant

Table 16. Mapping with MS9 test-case-specific KPIs

5.2.5.5.2 MS10 metrics

MS10 metrics are not relevant.

5.2.5.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

Liability KPIs	Mapping
Accessibility	Not Relevant
Effectiveness	Not Relevant
Timing (Mean Time To Report)	We provide analysis about the impact of our protocol when sending a file between two endpoints. We also analyse the impact of the number of packets, the number of sessions and the packet size.
Overall Evaluation of Transparency	Not Relevant
Level of Authentication	Our enabler allows to authenticate the receiver.
Integrity	Our enabler allows the sender to verify if the sent packet has been correctly received by the receiver.
Delegation of responsibility Overall responsibility level	Not Relevant Not Relevant
Precision of Root Cause Analysis	Not Relevant
Penalties	Not Relevant
Risk Exposure	Not Relevant

Table 17. Mapping with accountability / liability metrics

5.2.6 Risk Analysis Graphs

5.2.6.1 Description

As described in D4.1, the concept of RAGs provides a new framework that captures simultaneously the topology of a system, the vulnerabilities, the accessibility between the components, their external exposure, and the way all these elements may evolve over the time. Thus, RAGs provide a framework for fine qualitative and quantitative risk assessment approaches to assess the impact of the exploitation of the vulnerabilities and their exposition surface throughout the nodes of the graph; to compute risk indicator metrics; and to observe their evolution over several time periods. Based on this model, this enabler can compute and determine the best strategies to secure the system. More precisely, given a set of available countermeasures associated with known vulnerabilities (ranging from firmware updates or patches to VNF deployments), the enabler computes the best placement strategies at minimum cost to increase the security up to a provided acceptance level.

5.2.6.2 Mapping with HLA

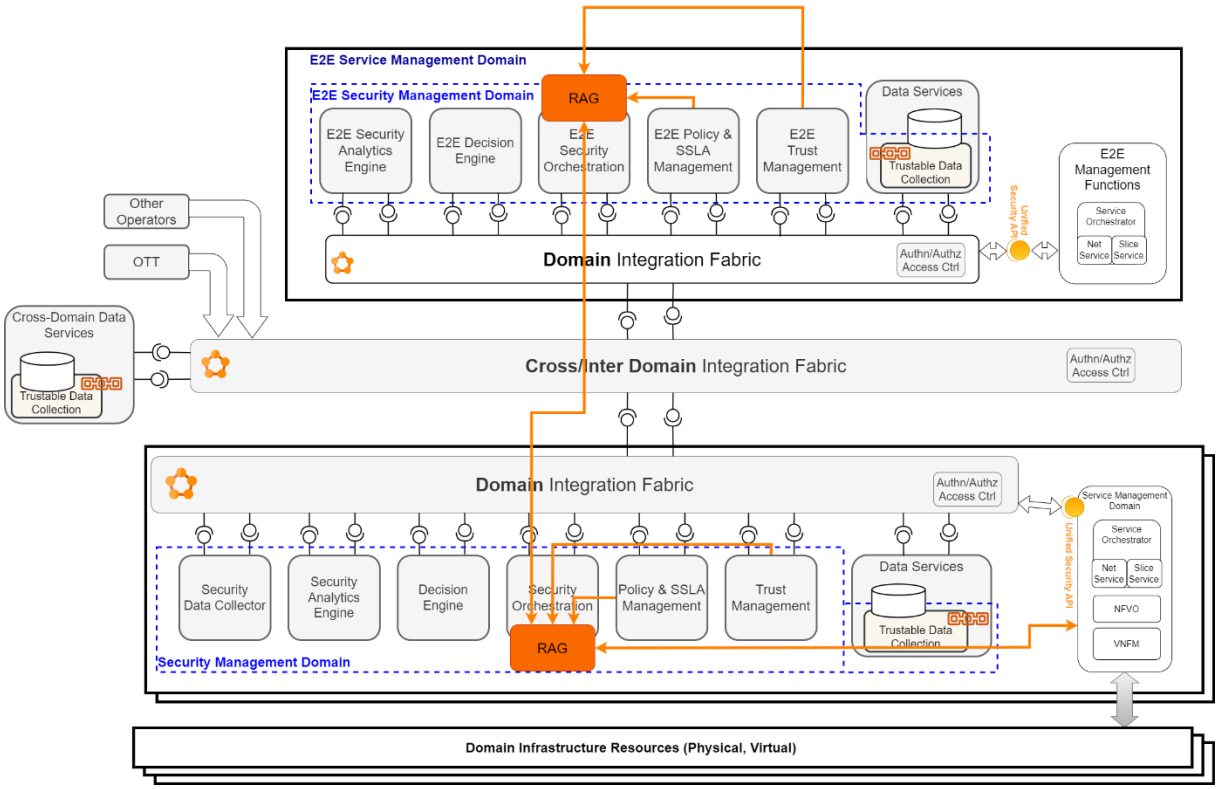


Figure 21. RAG enabler within the HLA

Figure 21 presents the description of the RAG enabler within the HLA:

- RAG – RAG: hierarchical interaction between several vision of topologies.
- RAG – Trust Management: collection of targeted security levels per sub-domain.
- RAG – Security Orchestrator: optimized placement strategy (for Vertical's VNF and counter measures) with respect to Policy, SSLA and trust management constraints.
- RAG – Policy and SSLA management: topology of connectivity between components and available countermeasures at this level of topology.

5.2.6.3 UML sequence diagram

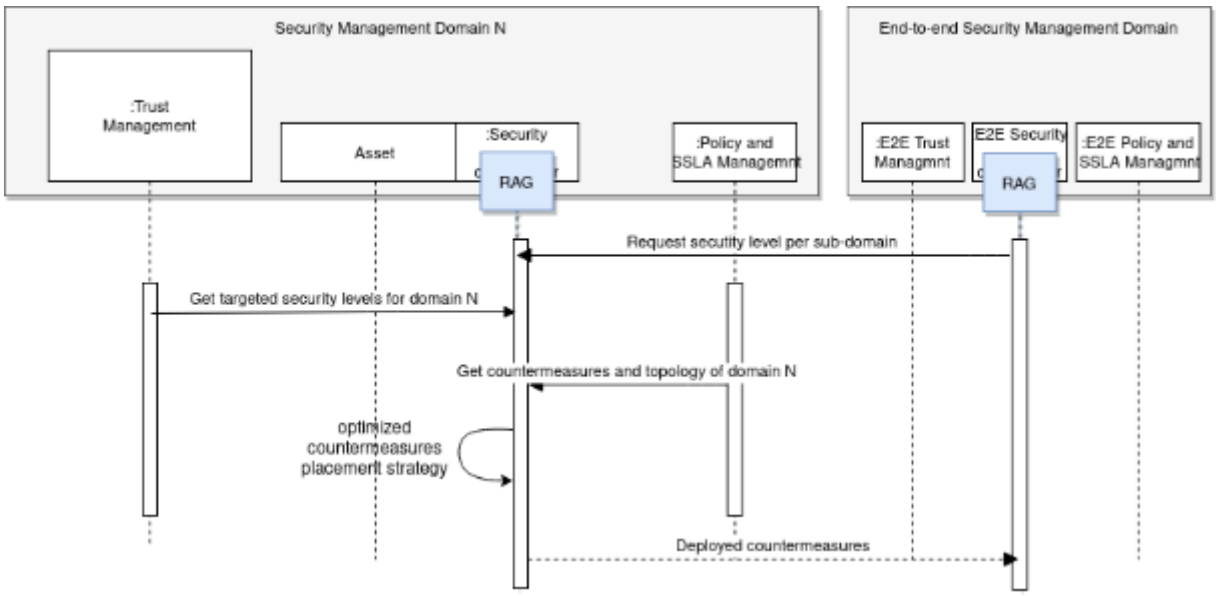


Figure 22. Sequence diagram for the enabler RAG

Figure 22 presents the sequence diagram for the RAG enabler. At end-to-end level, a request may be initiated to poll the security level at the sub-domain level. Within a domain, the Trust Management gets targeted security levels from RAG. The Policy and SSLA Management on its side gets countermeasures and topology of the domain. RAG computes optimized countermeasures placement strategy. It also advertises the deployed countermeasures to the end-to-end Management Domain.

5.2.6.4 Mapping with Liability Functional Blocks

The RAG enabler is located in the functional block “FB.2 - Monitor for accountability evidences” since it can detect security issues based on the network topology and a vulnerability database and then provide a strategy to mitigate the risk.

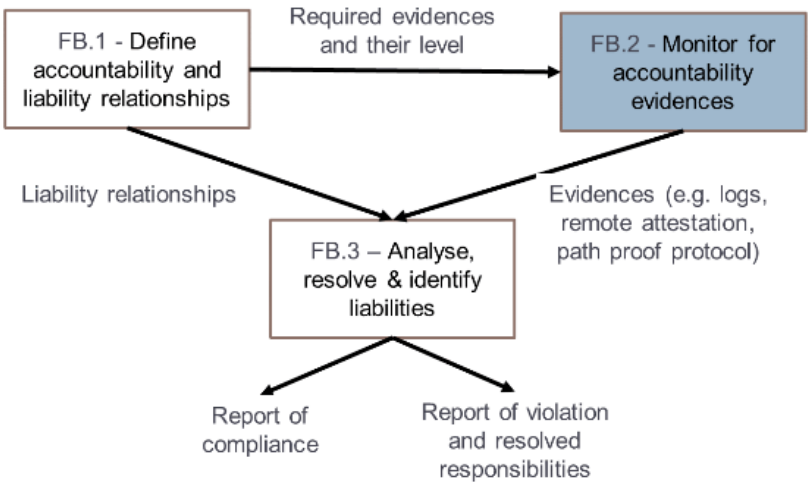


Figure 23. Mapping with Liability management system functional blocks.

5.2.6.5 Mapping with metrics

5.2.6.5.1 MS9 metrics

Service response time: time to compute the optimal placement of countermeasures to reach the requested level of security.

5.2.6.5.2 MS10 metrics

Mean Observation Report Request Response Time: corresponds to the time taken to compute the most risky element in the network, generate and send the report.

5.2.6.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

The RAG module provides a risk assessment of the system. It can compute the chain of vulnerabilities (attack path) that an attacker is likely to use to access the system.

5.2.7 Behavioural profiles

5.2.7.1 Description

As described in D4.2, the Manufacturer Usage Description (MUD) is an Internet Engineering Task Force (IETF) standard aimed to define the intended behaviour of the device through Access Control Lists (ACLs), in order to restrict the communication to/from a certain device. For a thorough description of the MUD (Behavioural Profile), please refer to D4.2.

5.2.7.2 Mapping with HLA

In Figure 24 we can observe the mapping of the Behavioural profile enabler, named MUD, into the High-Level Architecture. In the first place, and in order to retrieve the MUD file, a device will attempt to access the infrastructure by providing its MUD URL. This MUD file will contain information to restrict the device communications. Next the MUD Manager, which is located at the Security Orchestrator, uses the previously obtained MUD URL to retrieve the MUD file from the corresponding MUD File Server.

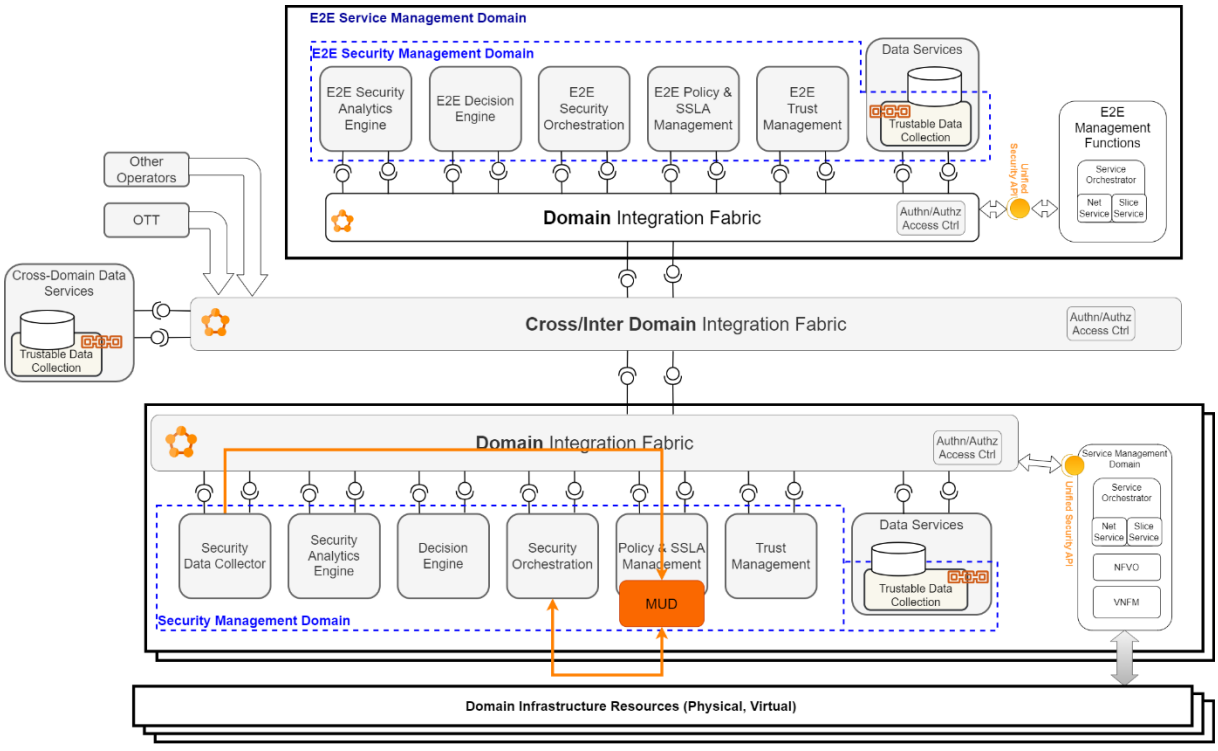


Figure 24. MUD file within the HLA.

5.2.7.3 UML sequence diagram

Figure 25 shows MUD sequence diagram:

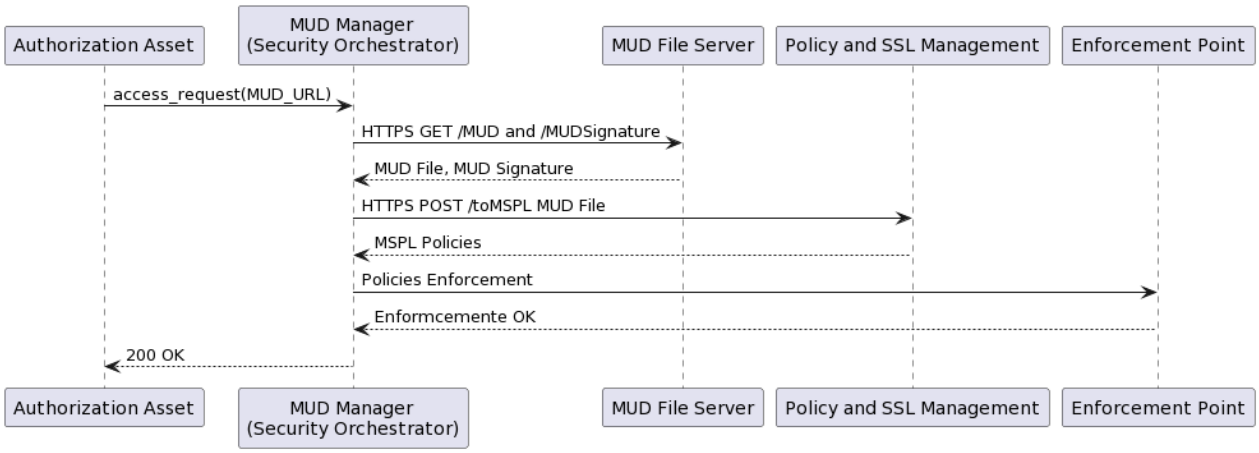


Figure 25. MUD sequence diagram.

As mentioned before, we assume that an external device willing to access the network sends its associated MUD URL through an Authorization Asset, which is in turn received at the MUD Manager (located at the Security Orchestrator). The MUD Manager asks the MUD File Server, through the Integration Fabric, for both the MUD file and the MUD file signature using the previously obtained MUD URL. Then, the MUD Manager sends the collected MUD File which contains the communication restrictions for the external device to a Policy Interpreter. The latter will be in charge of translating the MUD policies to MSPL intermediate language which will be, finally, enforced as a new configuration by the Security Orchestrator enforcement point.

5.2.7.4 Mapping with Liability Functional Blocks

As described in Figure 26, MUD is part of the first functional block (FB.1 - Define accountability and liability relationships) because MUD files are used to deliver policy requirements for a device joining the network, and then translated to network access specific policies. In fact, MUD files are collected during the bootstrapping process in order to obtain the security policies before the device has access to the network. MUD file provides Access Control List (ACL) requirements for each device type so it is possible to identify a well-known regular behaviour for them.

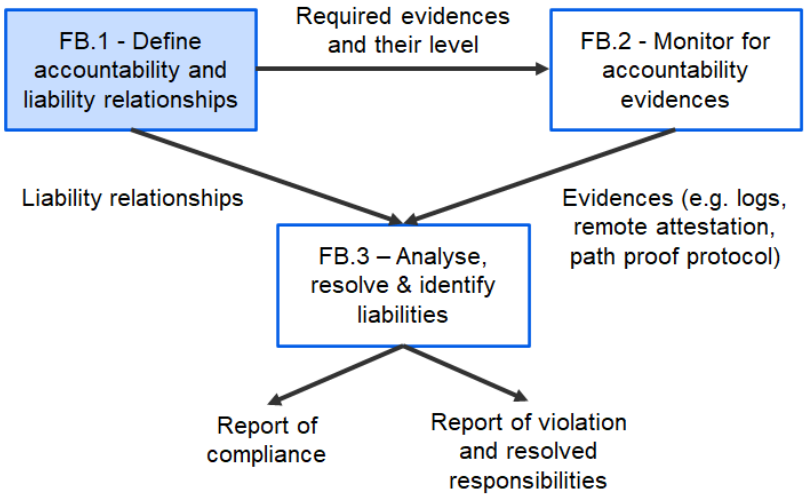


Figure 26. Mapping of MUD with liability-aware management functional blocks

5.2.7.5 Mapping with metrics

5.2.7.5.1 MS9 metrics

Generic KPIs	Mapping
SSLA enforcement	MUD file information can be used to define SSLAs.

Table 18. Mapping with MS9 Generic KPIs

Test-Case-Specific KPIs	Mapping
Automated vulnerability assessment	MUD file information can be used to derive which threat can target the system
Threat assessment	MUD file information can be used to derive which threat can target the system
Cyber-security insights assessment	MUD file information can be used to improve the security posture of the system

Table 19. Mapping with MS9 test-case-specific KPIs

5.2.7.5.2 MS10 metrics

MS10 metrics are not relevant for MUD.

5.2.7.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

From accountability and liability metrics only the Level of Authentication can be affected by MUD.

MUD file can be used to authenticate the device accessing the infrastructure with the information provided by the manufacturer.

5.2.8 Security-by-Orchestration Kubernetes (SBO-K8S)

5.2.8.1 Description

The aim of this module is to provide a more sophisticated algorithm for placement of functions (or pods, in the Kubernetes terminology) to the orchestrator of Kubernetes. In particular, the algorithm provides physical isolation to functions, depending on their security isolation requirements. The algorithm also ensures that latency-sensitive services have an end-to-end latency meeting their requirements.

5.2.8.2 Mapping with HLA

As described in Figure 27, the module 'Security-by-Orchestration for Kubernetes' (SBO-K8S) takes as input the function chain descriptions from the SSLA End-To-End Policy and Management functional block. These descriptions include the Security level of each function, their isolation requirement, how they are chained together in order to provide a service, their end-to-end latency requirement, and so on.

Then, the module performs the computation for the placement that will meet all the function requirements, while minimizing a relevant KPI chosen by the administrator of the module, such as the number of nodes used, or the total latency for instance.

Afterwards, the module contacts the end-to-end service orchestration and instructs the latter to deploy the functions according to the determined placement.

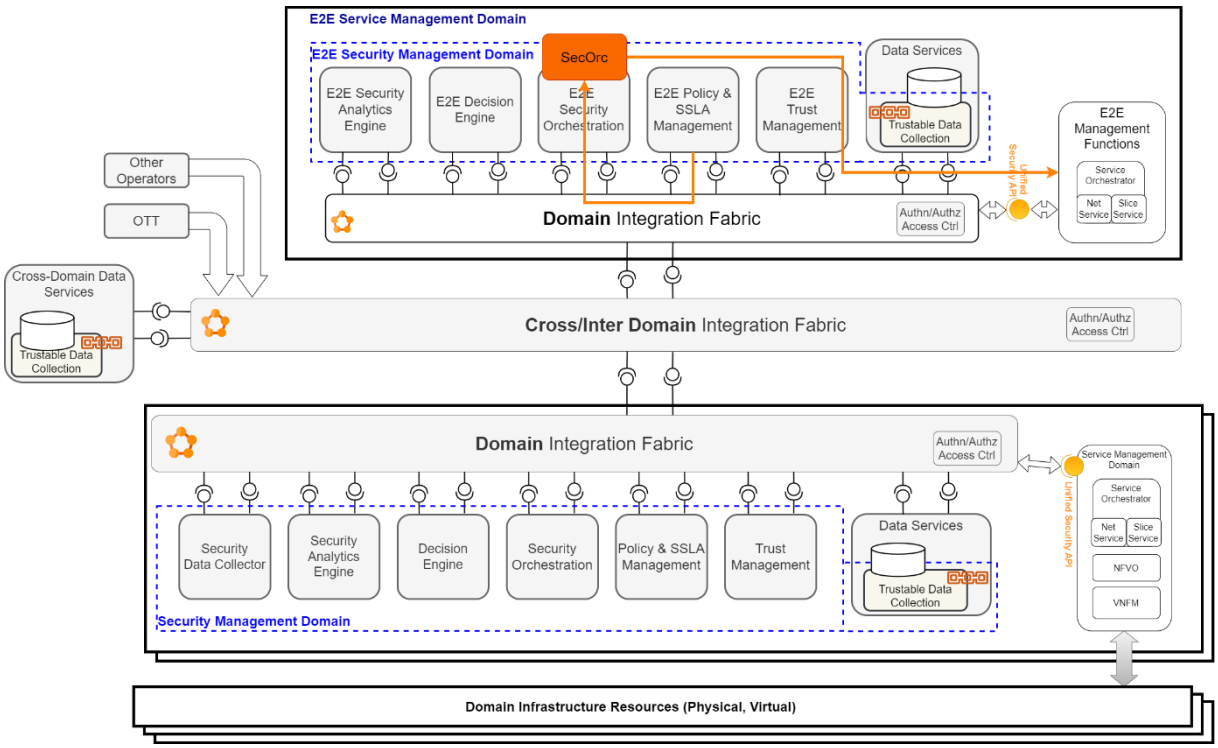


Figure 27. Module 'Security-by-Orchestration for Kubernetes', mapping with HLA

5.2.8.3 UML sequence diagram

The 'SBO-K8S' module receives the function description from the SSLA. In particular, the SSLA specifies the Security level of the functions, along with their Isolation requirements. It also specifies the maximum acceptable end-to-end latency for the function chains. The computation then determines how the functions can be placed in order to account for all the constraints and requirements. The output of the algorithm is a file that can be used by the Service Orchestration for the function deployment.

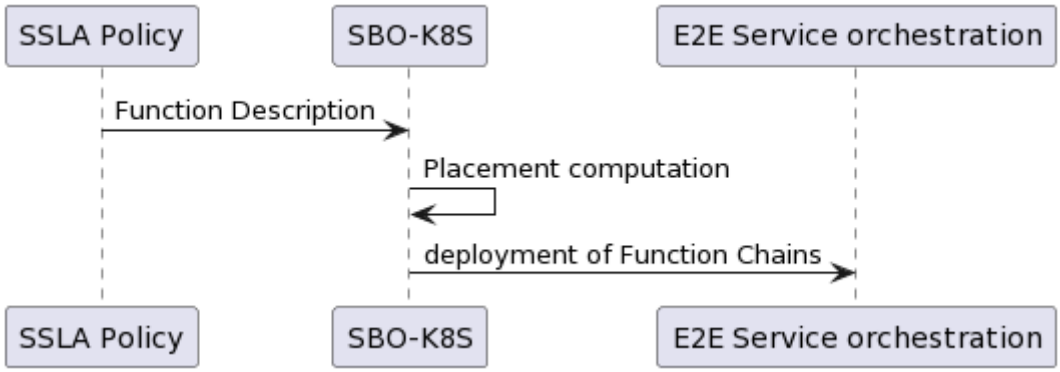


Figure 28. Simplified Sequence Diagram for the module 'SBO-K8S'

5.2.8.4 Mapping with Liability Functional Blocks

The SBO-K8S module provides evidence of the presence of all the functions that are deployed on a physical node. It also provides evidence of the isolation requirements of each function and check that they are effectively met.

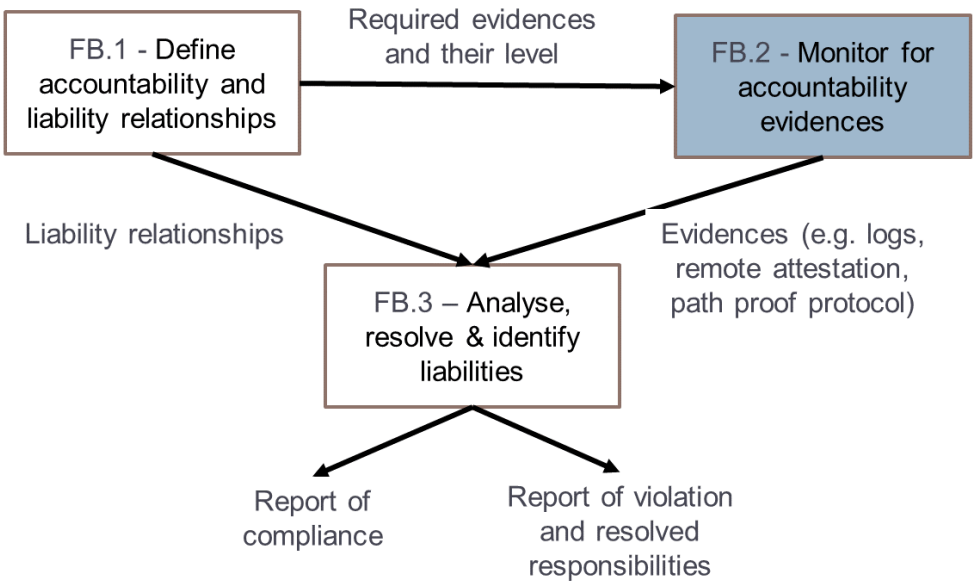


Figure 29. Mapping with Liability Functional Blocks of the module 'Security-by-Orchestration for Kubernetes'

5.2.8.5 Mapping with metrics

5.2.8.5.1 MS9 metrics

Service response time (time to compute the optimal placement of functions while meeting isolation, latency, and capacity constraints, and function deployment).

5.2.8.5.2 MS10 metrics

Mean Observation Report Request Response Time (corresponds to the mean time required to provide an observation report after it was requested).

5.2.8.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

The only metric measured or used by the enabler is "Mean Time To Report" which is correlated to MS10 Mean Observation Report Response Time.

5.2.9 GRALAF

5.2.9.1 Description

GRALAF uses graph-theoretic analysis to identify liability based on liability formulations and responsibilities of various actors in the microservice-architecture-based network. It extracts the network model from traffic monitoring tools. From the SSLA Management Service (LASM), GRALAF receives TRAILS data which include information about the committed behaviour of the components. GRALAF periodically gets the monitoring data of services and nodes where it detects anomalies and SLA commitment violations. A Causal Bayesian network (CBN) is used to model the network assets and their metrics, in which each node represents a variable and the arcs in the graph represent causal relations; that is, the relation A → B represents some physical mechanism such that the value of B is directly affected by the value of A. The multiple RCA algorithms process the graphical model and determine a list of liable entities with a likelihood score and liability value. GRALAF sends to the LASM the results which include the root cause list and the traces related to the incidents that triggered the root cause. In Figure 30, you may see how the system components of GRALAF interacts with each other in our test environment.

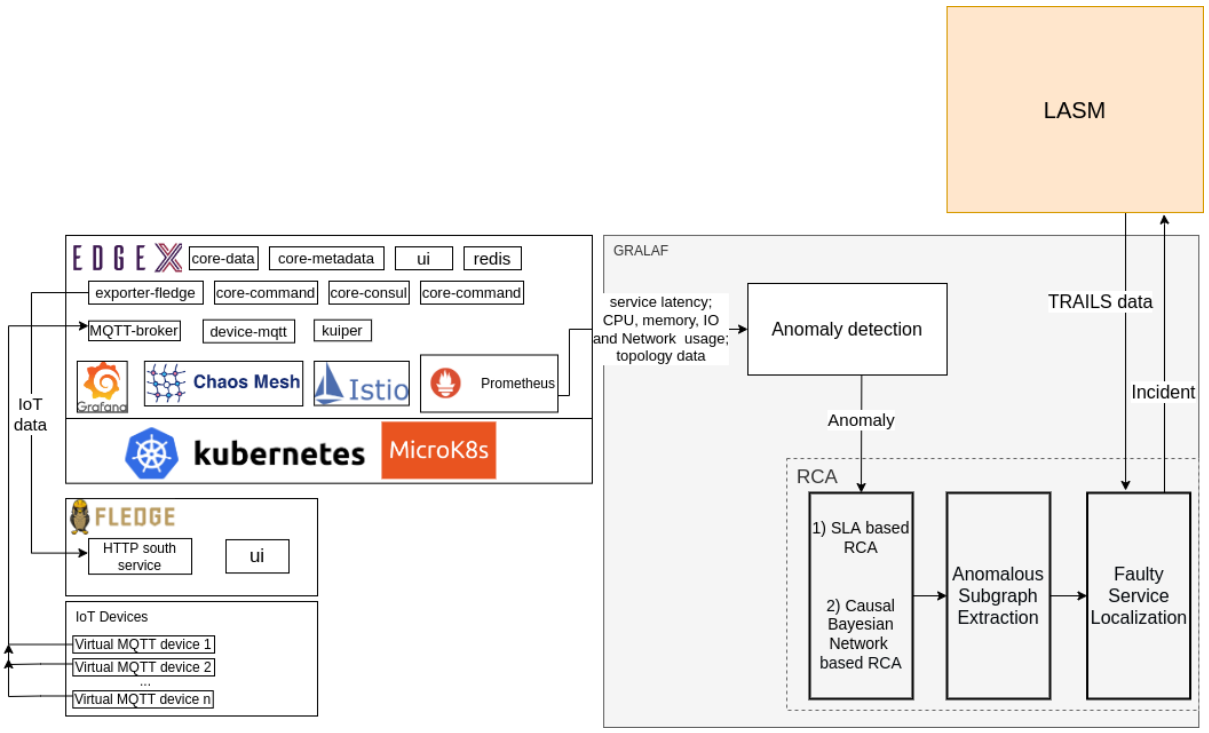


Figure 30. GRALAF system block diagram

5.2.9.2 Mapping with HLA

GRALAF provides anomaly detection and RCA services so it can be located under Security Analytics Engine as can be seen in Figure 31.

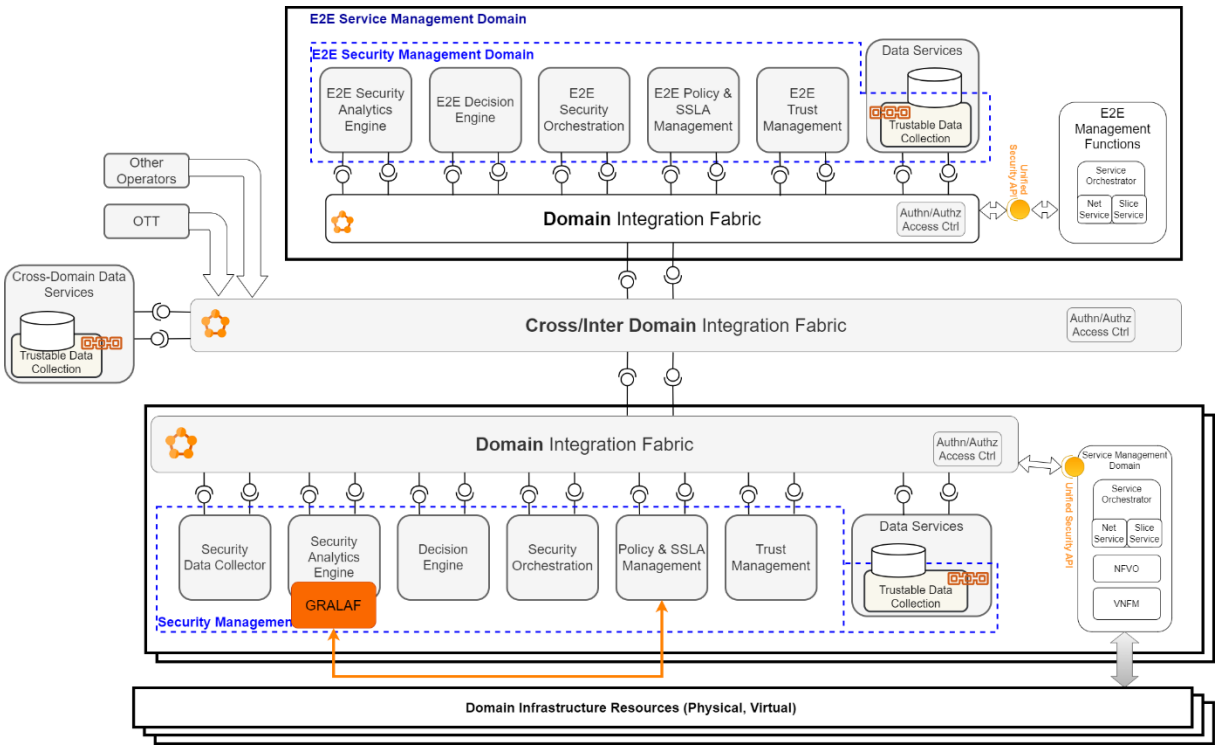


Figure 31. Mapping of the GRALAF service with HLA architecture

5.2.9.3 UML sequence diagram

In Figure 32, a sequence diagram is given to represent initialization of GRALAF, anomaly detection, RCA and its incident reporting processes.

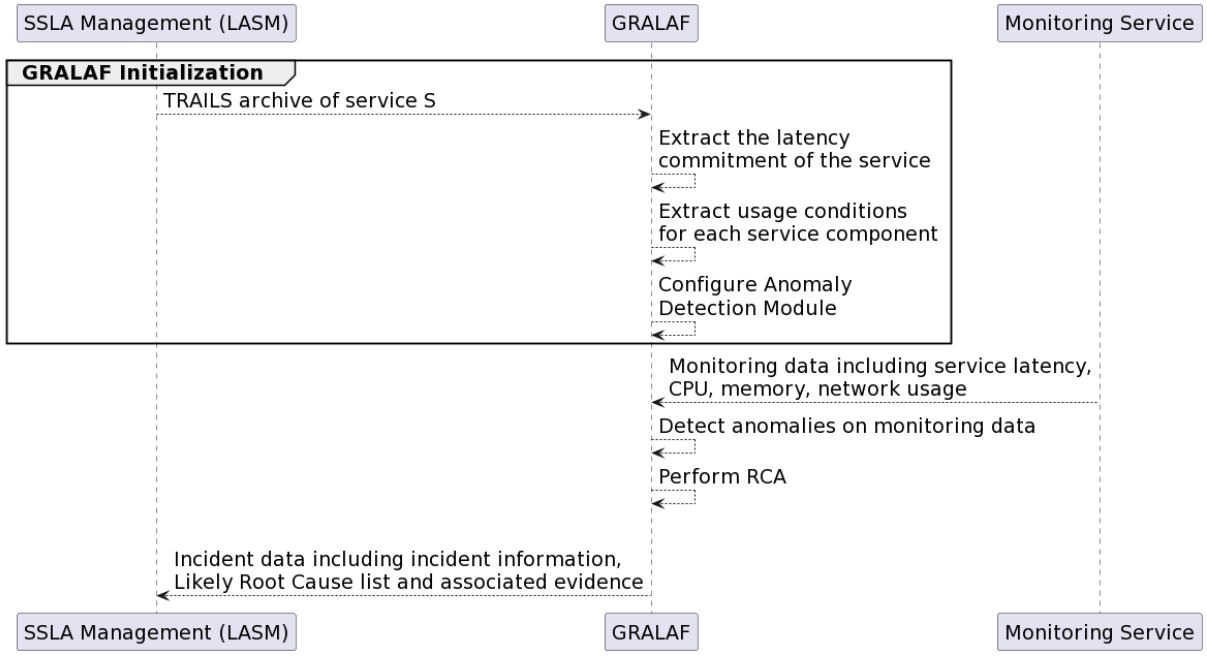
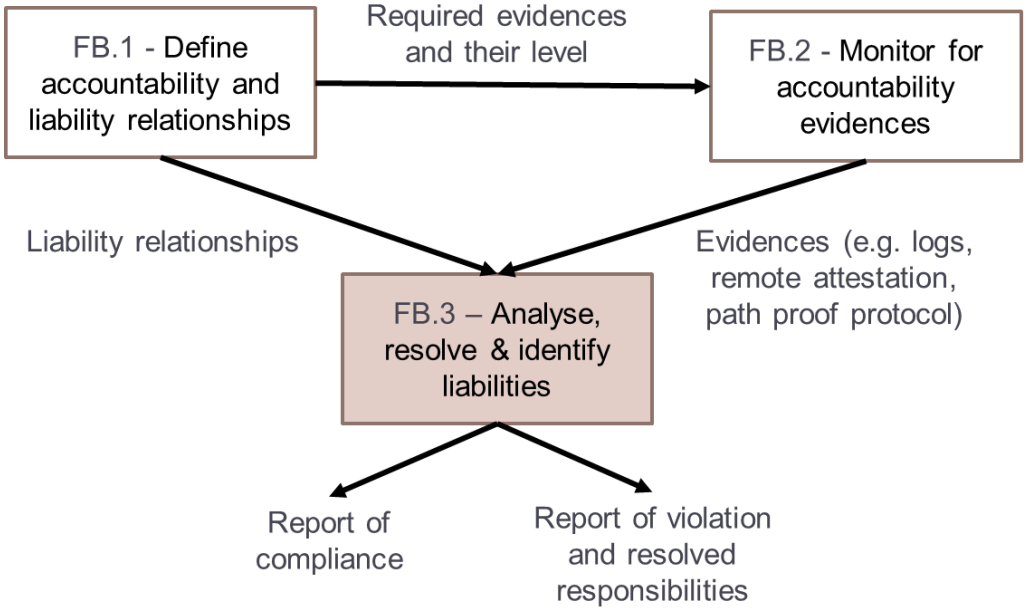


Figure 32. Sequence diagram for GRALAF initialization and reporting incidents to LASM

5.2.9.4 Mapping with Liability Functional Blocks

As given in Figure 33, GRALAF is a part of the FB.3 “Analyse, resolve & identify liabilities” because it performs anomaly detection and root cause analysis by using monitoring data and SLA.



1

Figure 33. Mapping of GRALAF with liability-aware management functional blocks

5.2.9.5 Mapping with metrics

5.2.9.5.1 MS9 metrics

Generic KPIs	Mapping
Mean Time To Detect	The MTTD is used to evaluate how quickly system anomalies can be detected following an occurrence of an anomaly.
Mean Time to Contain	Not Relevant
Mean Time to Resolve	Not Relevant
Transaction speed	Not Relevant
Packet Loss Ratio	Not Relevant
Number of False positives	CBN-based RCA depends on probability and could produce incorrect results.
Number of False negatives	Same as above
Initial time	GRALAF retrieves data for initialization. This metric is used for the enabler evaluation.
Migration time	Not Relevant
Service response time	Not Relevant
Service downtime	Not Relevant
SSLA enforcement	Not Relevant

Table 20. Mapping of MS9 Generic KPIs

Test-Case-Specific KPIs	Mapping
Blocked adversarial examples rate	Not Relevant
Ratio of allowed malicious scale-up	Not Relevant
Automated vulnerability assessment	Not Relevant
Automated model generation	A system model is generated from service latency metrics
Threat assessment	Not Relevant
Cyber-security insights assessment	Not Relevant
Latency	Service latency metrics are used to detect anomalies
Mean Time to implement the MTD action	Not Relevant
MTD action cost	Not Relevant
Protection gain of an MTD policy	Not Relevant
Mean decision time for MTD action	Not Relevant
QoS gain/loss of the protected resources	Not Relevant

Table 21. Mapping of MS9 Test-Case-Specific KPIs

5.2.9.5.2 MS10 metrics

The metrics from MS10 are not relevant to GRALAF.

5.2.9.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

Liability KPIs	Mapping
Accessibility	Not Relevant
Effectiveness	Not Relevant
Timing (Mean Time To Report)	The time from the retrieval of system metrics with anomaly to incident report submission is measured and used to evaluate the enabler.
Overall Evaluation of Transparency	Not Relevant
Level of Authentication	Not Relevant
Integrity	Not Relevant
Delegation of responsibility	Not Relevant
Overall responsibility level	Not Relevant
Precision of Root Cause Analysis	Precisions are obtained for the performed RCAs.
Penalties	Not Relevant
Risk Exposure	Not Relevant

Table 22. Mapping of MS9 Test-Case-Specific KPIs

5.2.10 Software monitoring by Systemic

5.2.10.1 Description

Systemic description in former deliverables D4.1 and D4.2 were exclusively focused on the security and trust properties delivered by Systemic on protected software. Security and trust are brought in the form of confidentiality, authentication and integrity verification all worked out by the protected code itself against itself and without any additional dependency (hardware or software), as shown in Figure 34. In addition, and as a result of INSPIRE-5Gplus, proven evidences of such properties can be generated and transmitted to a remote central monitoring utility. These proven evidences bring a novel type of real time functioning status of the software. In particular, in a telecom industry context, the very first security property which states that the code is effectively executing is of great significance for liability and accountability reasons. Signs of activity can certainly be existing in the software source code, but if they are not present, Systemic palliates to this situation in all cases.

Additionally, to discern unambiguously the instance among a plurality of running instances, the solution appends an identification marker. Each instance is identified and its execution conditions monitored by means of regular and signed heartbeats. The content of the heartbeats is given in the following Table 23.

Instance identifier: The different instances of the code are **identified** and distinguished with an appended identifier. This identifier enables to monitor each instances unambiguously. The signed heartbeats contain the identifier	
Security property	**Measured element. Method**
P1. The protected code **executes**	By construction of Systemic Control Flow Obfuscation technique, Systemic appended security routine collects the control flow activity (e.g., jumps to next code block). These transitions in **reflect the activity** of the software as a sleeping or terminated software will not go through these internal code block transitions.
P2. The protected code is **integrated** and authenticated at load time and during execution.	The security routine produces the authentication verification and integrity check during runtime. The **test results** are appended in the heartbeats.
P3. The protected code **executes at the right location**	The security routine decrypts the code file text section (after a validated authentication test) with a AES key provisioned on the machine. The correct decryption is followed by the process memory load and execution of the code and attests the presence of the correct key on the machine, therefore that the code executes on **the correct (key provisioned) machine**.
P4. The protected code execution does not **deviate from the "normal" execution profile.**	This is an evolution of the current Systemic implementation. It is presented here as a relevant possible extension considered as relevant and feasible and delivering the mean to create pre-alerts (as bearing a positive False alarm rate and cannot constitute a firm attack detection per-se). By averaging of several runs on the same machines or from different similar nodes, a normal execution profile is composed. The profile corresponds to a typical normal CFG pattern, enabling to discern anomalies and deviations, suggesting a control flow attacks (which may be confirmed). Time and frequency elements associated extracted per code blocks are collected locally in systemic security routine appended on the protected instances and possibly transmitted in a central monitoring unit.

Table 23. Proven evidence heartbeat message structure

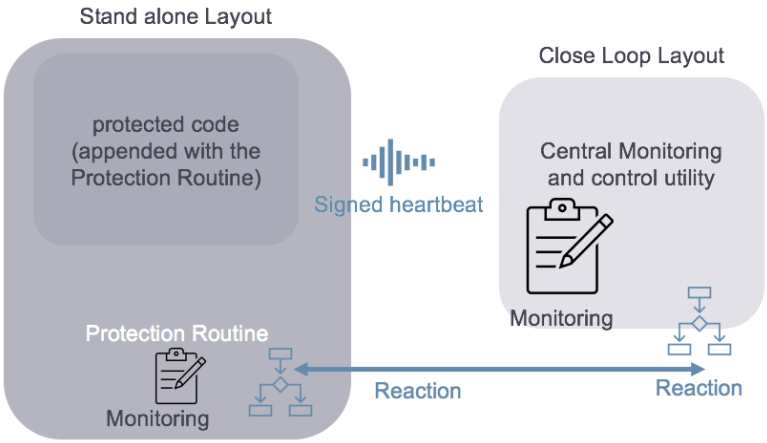


Figure 34. Systemic protection routine sending heartbeat messages to Central Monitoring utility

5.2.10.2 Mapping with HLA

D4.2 already describes the interaction of Systemic for its software security function. The mapping with the HLA produced here only reflects the interaction of Systemic routine with central monitoring units collecting the heartbeats and potentially reverts a modified protection pattern. Therefore, Figure 35 highlights the monitoring function of Systemic.

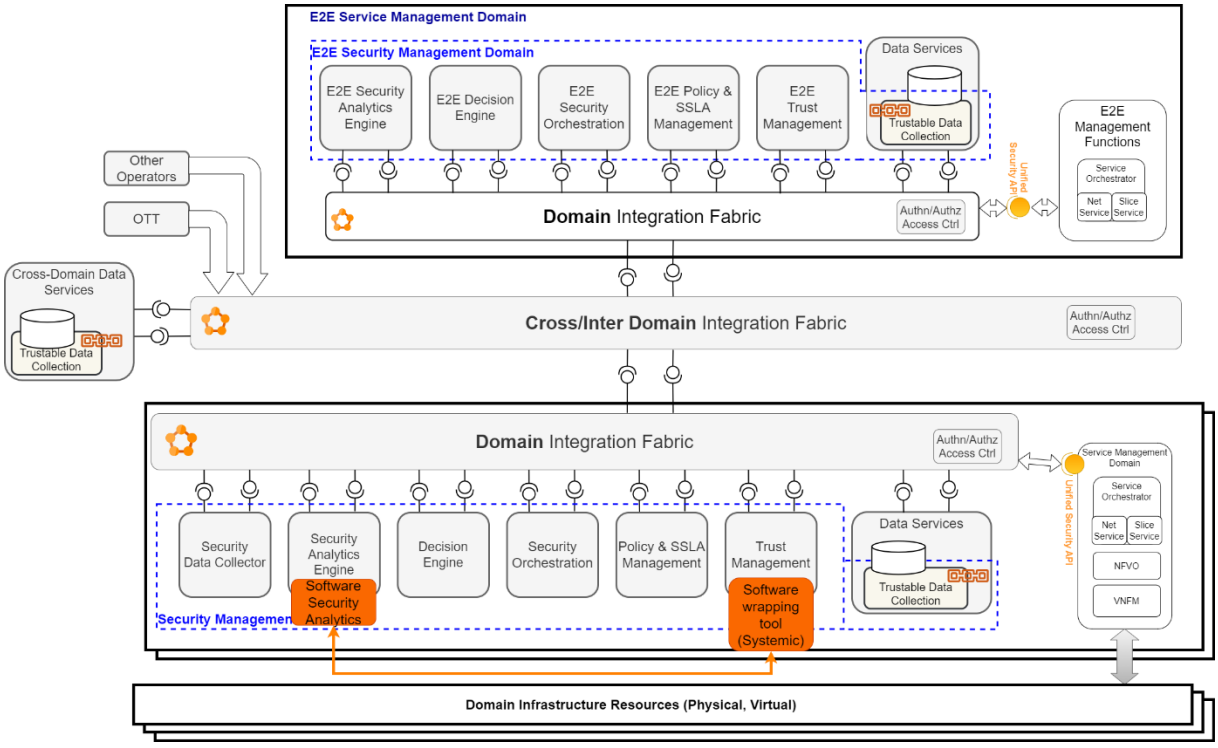


Figure 35. Systemic interaction with Security Analytics Engine

Systemic security routine interacts with the Security Analytics Engine as the collector of generated heartbeats carrying the correct functioning status of the protected software (i.e., security properties P1-4 as stated above).

The security analytics engine can derive a normal control flow profile by integrating various executions at the same locations or at different locations. This is needed to detect attacks by the deviations they create on the CFG.

The security analytics engine will be completed with the Software Security Analytics Engine, able to collect signed heartbeats, to interpret them and to adjust the security profile accordingly.

5.2.10.3 UML sequence diagram

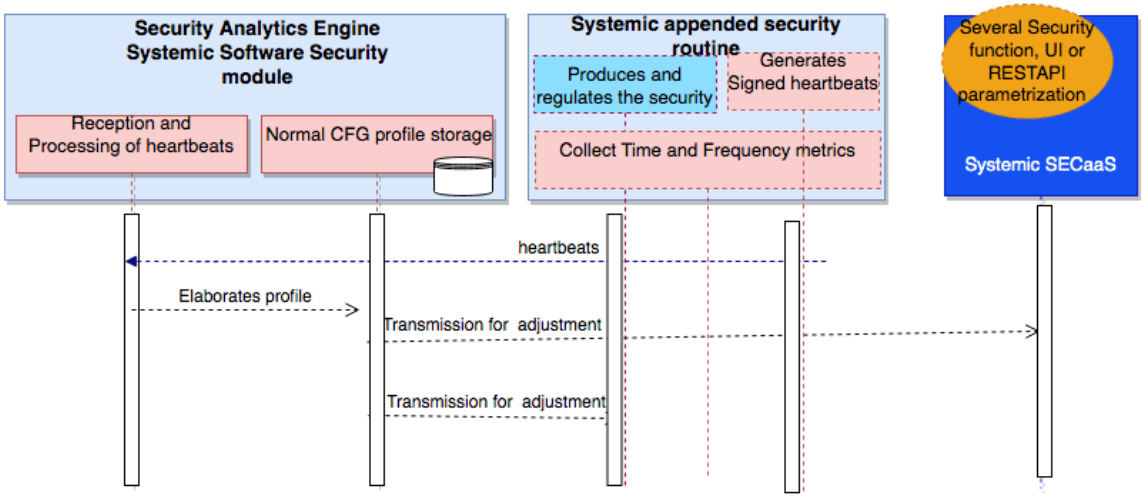


Figure 36. Systemic sequence diagram

The sequence diagram in Figure 36 shows the generation of heartbeats within the security routine located in the protected software, their collection at the Security Analytics Engine and the generation of a modified protection profile, either processed at SECaaS for its future protection job or directly by the security routine. On the right hand, the user defines first the initial security pattern and configuration for the protected software. This configuration integrates the optional "monitoring" function in order to append the associated heartbeats generation module into the Systemic routine. Provisions shall also be taken to install the Security Analytics Engine module capable to collect, interpret and generate the normal CFG pattern from the different running instances. Derived from this execution profile, the SECaaS can adjust and improve its security profile to elevate the protection level and to reduce the overhead impact. This adjustment can also be worked out directly on the running instance by an exchange between the SAE and Systemic appended routine.

5.2.10.4 Mapping with Liability Functional Blocks

As given in Figure 37, Systemic is a part of the FB.2 "Monitor for accountability evidences" because it collects runtime monitoring information useful for accountability.

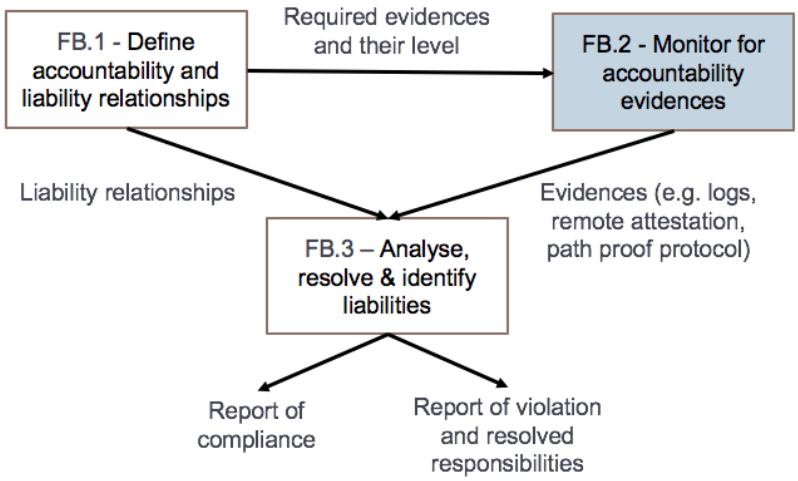


Figure 37. Mapping of Systemic with liability-aware management functional blocks

5.2.10.5 Mapping with metrics

5.2.10.5.1 MS9 metrics

Generic KPIs	Information
Mean Time To Detect	The MTTD is derived from the frequency of the heartbeats. A 5 second period shall be considered as offering a sufficient refreshing rate without bearing a significant computational cost overhead.
Mean Time to Contain	The complete cycle depends actually in the policy in the reaction time. Two layouts are considered. The reaction can be triggered directly at the protection routine at the time of the detection or at a remote centralized monitoring unit. In a security perspective, the reception of security alert shall not be followed by an instant reaction as it would indicate that the attack has been detected to the attacker. We would probably consider that a reaction into 1 to 5 minutes is the correct balance in addition to an extension of the software package (e.g., complete container or VM) to create opacity on the reaction.
Mean Time to Resolve	Same as above.
Transaction speed	Not relevant
Packet Loss Ratio	Not relevant
Number of False positives	0% for the tampering alerts. All tampering detection are valid without exception as resulting from a crypto-proven primitive and asymmetric encryption principle. Deep CFG monitoring could lead to the detection of false positive (to be defined)
Number of False negatives	0% for the tampering alerts, any tampering of the software (still present at the time of the measure) will result in a tampering detection with a 100% probability. Deep CFG monitoring could result in the non -detection of carefully crafted discrete control flow attacks
Initial time	Not relevant
Migration time	Not relevant
Service response time	Not relevant
Service downtime	If the tampering alert reaction is the termination of the software (and the reinstallation of an integrated original version), the service downtime is defined by the time needed by the orchestrator to produce the reinstallation
SSLA enforcement	Not relevant

Table 24. MS9 metrics

Test-Case-Specific KPIs	Information
Blocked adversarial examples rate	Not relevant
Ratio of allowed malicious scale-up	Not relevant
Automated vulnerability assessment	Not relevant
Automated model generation	Not relevant
Threat assessment	The detection of a deviation to the normal control flow graph constitutes a threat assessment. This is not implemented in the current version.
Cyber-security insights assessment	Same as above
Latency	Not relevant
Mean Time to implement the MTD action	Not relevant
MTD action cost	Not relevant
Protection gain of an MTD policy	Not relevant
Mean decision time for MTD action	Not relevant
QoS gain/loss of the protected resources	Not relevant

Table 25. Mapping of MS9 Generic KPIs

5.2.10.5.2 MS10 metrics

Systemic KPIs have been considered in MS 10 with the specific KPI listed below:

- *Mean Time To Detect that a function has been tampered with or is in incorrect location*

5.2.10.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

Transparency is a compounded KPI integrating Accessibility, Effectiveness and Mean Time to Detect.

One special consideration shall be recalled here: The transparency associated to Systemic Tampering detection can be viewed as very high but only if the software is (1) protected and (2) with the monitoring feature. This reminder is simply to restate that the security solution must be applied before the code is deployed and cannot offer any alert service nowhere (accessible or not) if not. If the code is protected, it then turns to be fully accessible and the tampering detection is also unambiguous. If the code is not protected, the accountability is null.

The other metrics of responsibility, attributability and Liability are not relevant with Systemic software security.

5.2.11 DiscØvery

5.2.11.1 Description

DiscØvery as presented in WP3 is a graph-based security and trust analysis tool for complex systems and networks. The tool uses a domain-specific language to express systems based on their unique requirements. The models that are created are dynamic and can evolve based on input by users or software agents. A security engineer will be able to define assets, identify threats and vulnerabilities, and receive insights on how to improve security and privacy, in a software aided analysis.

5.2.11.2 Mapping with HLA

DiscØvery is a component of the E2E Policy and SSL Management of the E2E Security Management Domain as shown in Figure 38.

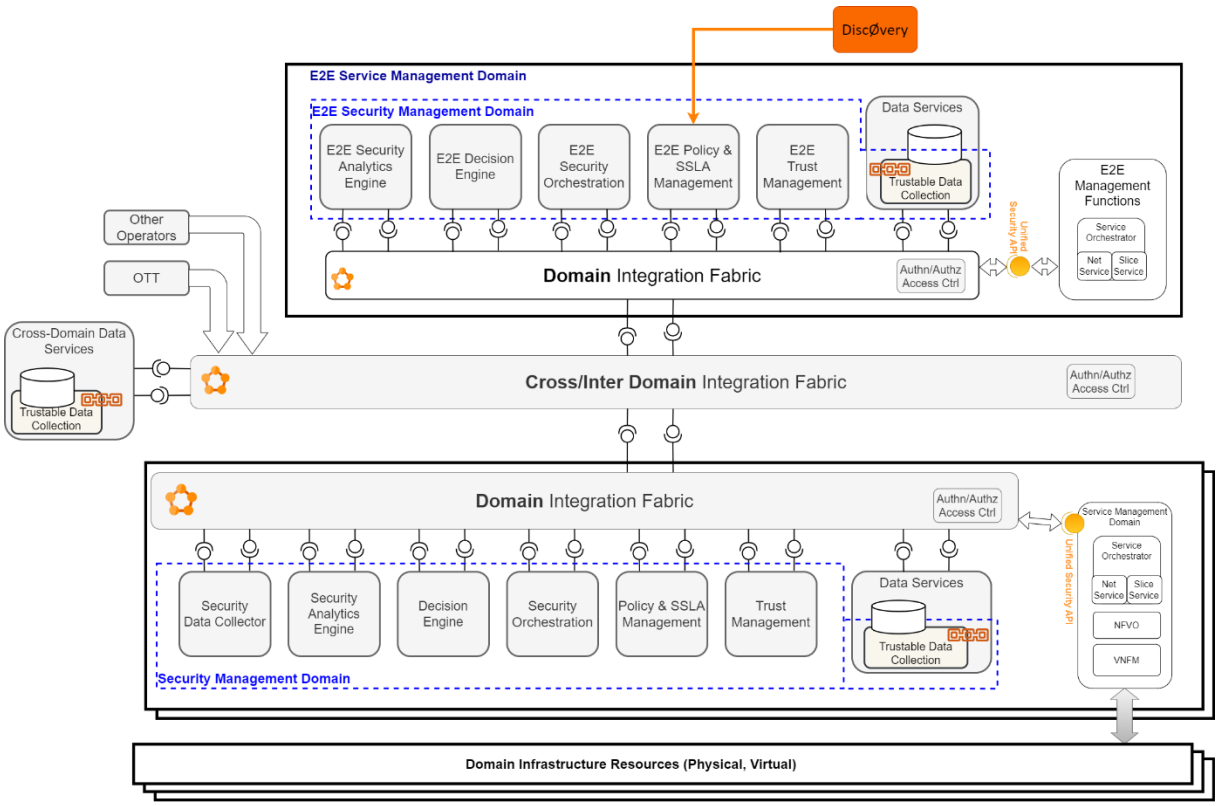


Figure 38. DiscØvery in the HLA

5.2.11.3 UML sequence diagram

Figure 39 shows the UML of DiscØvery.

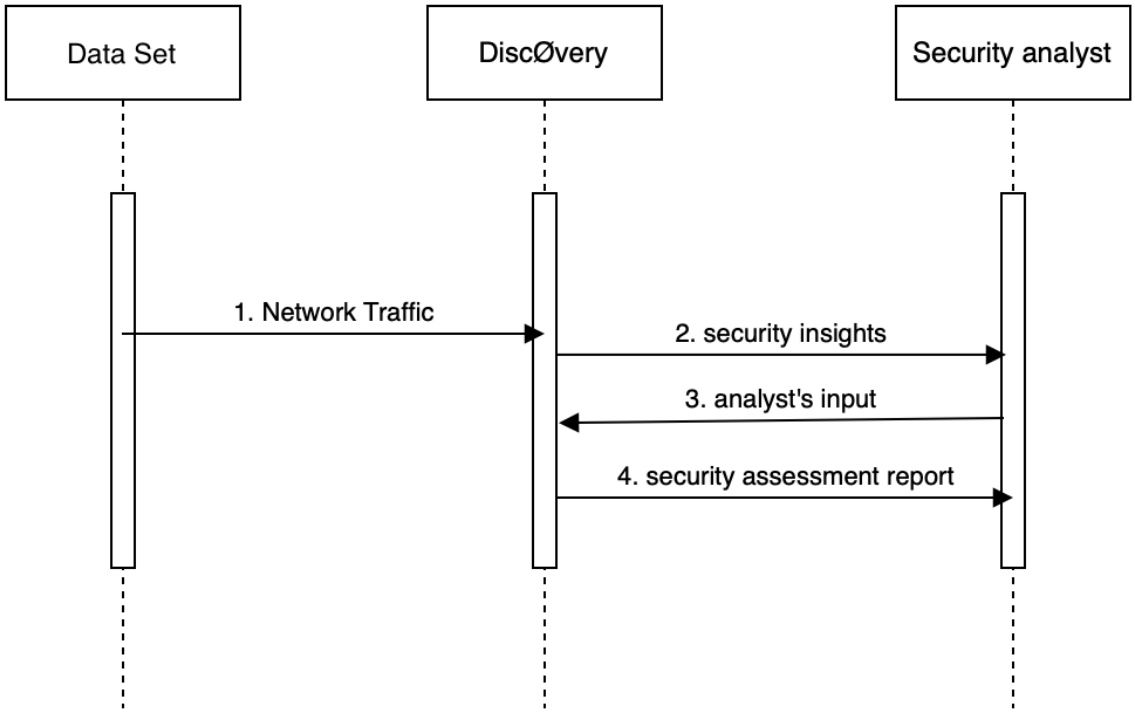


Figure 39.UML Diagram of DiscØvery

5.2.11.4 Mapping with Liability Functional Blocks

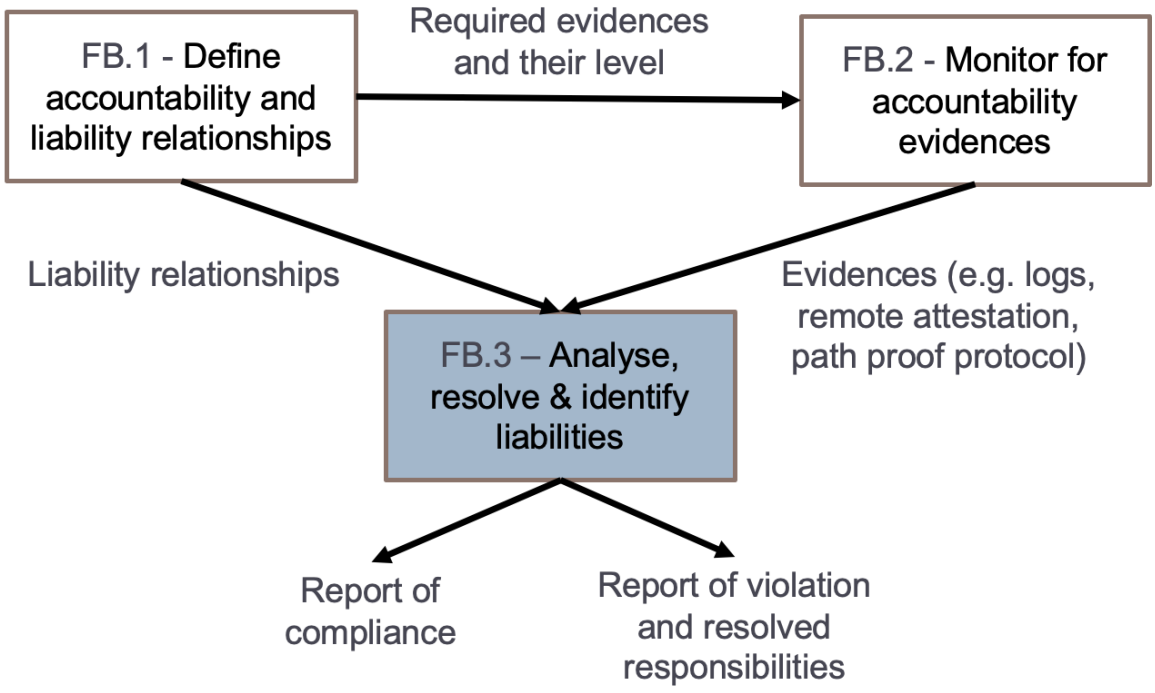


Figure 40. Liability functional block mapping of DiscØvery

5.2.11.5 Mapping with metrics

5.2.11.5.1 MS9 metrics

Generic KPIs	Mapping
Mean Time To Detect	Not relevant
Mean Time to Contain	Not relevant
Mean Time to Resolve	Not relevant
Transaction speed	Not relevant
Packet Loss Ratio	Not relevant
Number of False positives	Not relevant
Number of False negatives	Not relevant
Initial time	Not relevant
Migration time	Not relevant
Service response time	Not relevant
Service downtime	Not relevant
SSLA enforcement	Not relevant

Table 26. MS9 metrics

Test-Case-Specific KPIs	Information
Blocked adversarial examples rate	Not relevant
Ratio of allowed malicious scale-up	Not relevant
Automated vulnerability assessment	A vulnerability assessment based on vulnerability databases is generated for the network.
Automated model generation	A network model is automatically generated based on network capture files.
Threat assessment	A threat assessment based on the high-level threats that can impact the network.
Cyber-security insights assessment	A list of insights and guidelines on how to improve the security posture of the network.
Latency	Not relevant
Mean Time to implement the MTD action	Not relevant
MTD action cost	Not relevant
Protection gain of an MTD policy	Not relevant
Mean decision time for MTD action	Not relevant
QoS gain/loss of the protected resources	Not relevant

Table 27. Mapping of MS9 Generic KPIs

5.2.11.5.2 MS10 metrics

MS10 metrics are not relevant for DiscØvery.

5.2.11.5.3 Accountability / liability metrics adapted from the state of the art to Inspire5G+

DiscØvery can be configured to provide accountability metrics on the security mechanisms of a networks based on the identified policies. Additionally, as part of its cyber-insights functionality it can provide alternative policies to improve the existing accountability of the network.

6 Case Study of Liability Management on Demos

6.1 Case study of liability management in demo1

This demonstration does not demonstrate liability.

6.2 Case study of liability management in demo2

In the article [41], we described the INSPIRE5G-Plus demo2 demonstrator. With a use case focused on function isolation based on criticality, we illustrated how a 5G E2E Service Provider can deliver Security SLAs to their customers (Service Owners) by leveraging a set of security enablers developed in the INSPIRE-5Gplus project.

The elaborated enablers are in particular a novel sTakeholder Responsibility, Accountability and Liability deScriptor (TRAILS), a Liability-Aware Service Management Referencing Service (LASM-RS), an anomaly detection tool (IoT-MMT), a similarity-based Root Cause Analysis tool (IoT-RCA), two Remote Attestation mechanisms (Systemic and Deep Attestation), and two Security-by-Orchestration enablers (one for the 5G Core and one for the MEC). With them, E2E Service Providers can manage their accountability, liability and trust placed in subcomponents of a service (subcontractors).

We also showed how the functional objectives of a liability management system detailed in section 2 are achieved by this combination of enablers. Figure 41 shows how each enabler involved in demo2 is mapped with the liability management system functional blocks.

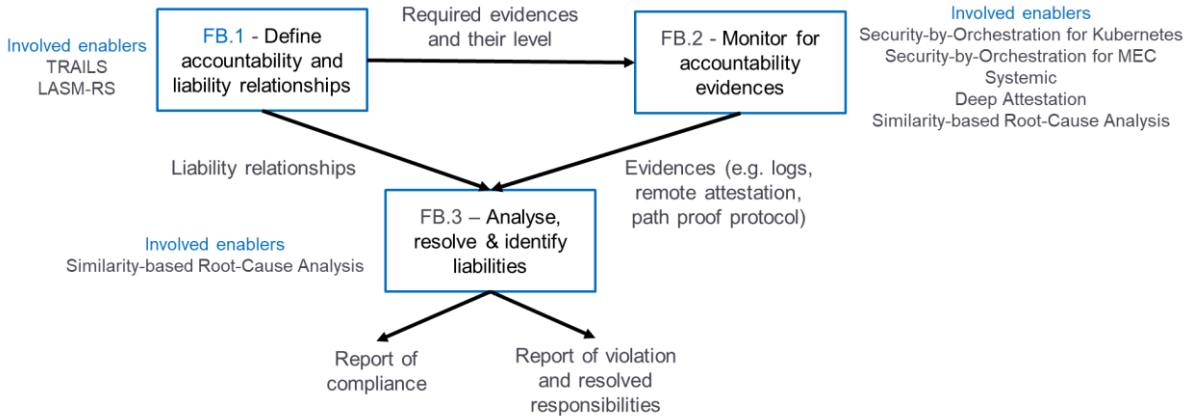


Figure 41. Demo 2 mapping with liability management functional blocks

6.3 Case study of liability management in demo3

This demonstration does not demonstrate liability.

7 Second Workshop on Accountability, Liability and Trust for 5G and Beyond

The Second Workshop on Accountability, Liability and Trust for 5G and Beyond was collocated with the conference 6GNet in Paris on the 8th of July 2022. The corresponding webpage (https://6g-conference.dnac.org/walt5gplus-2022-workshop/) is illustrated in Figure 42.

Figure 42. Second Workshop on Accountability, Liability and Trust for 5G and Beyond webpage

The program of the workshop is described in Figure 42. The panel discussions revolved around the following questions:

- What is the major challenge / lock / concern for a multi parties (and dynamical) liability management for 2030? And why?
- What is the nice to have thing for multi-party liabilities? (*wish list – dream, not necessary connected to reality*)
- How you see impacts of the potential hybrid approaches mixing 'EU Certifications schemes and Assurances' for some parties with 'contractual SLAs' for the others? *(which models to manage them for an end to end point of view?)*
- In term of future of Liability, may we need real test scenario, like crisis exercises? How to perform it?

The panellists acknowledged the needs stemming from the growing interconnection of systems and

the difficulty to manage trust and liability among actors which are not necessarily linked by a contractual relationship (as showcased by the paper “eSIM Adoption: Essential challenges on Responsibilities Repartition”).

Then, the panellists discussed the complexity to establish an end-to-end chain of Trust over heterogeneous Domains linked together. They noted that trust is often built on evidence that is provided by the domain owners themselves. For example, under Common Criteria evaluation Scheme, the only metrics that measures the trust and that is recognized by the various signatories of the SOG-IS agreement is the Assurance level which measures the capacity level required of attackers to discover and reproduce the attacks uncovered during the tests.

The panellists agreed that attestation frameworks and manifest enablers are key elements in liability management. Indeed, attestation frameworks, such as the ones developed in INSPIR5G+ WP4, allow to collect evidence and measure them over specific node, based on a contract to be established between the parties before operating a service under a SLA. At the moment of SLA definition the parties agreed on the way to measure the reality of a property and based of the common recognition on the way to measure it we demonstrate we operate the measure as claimed on the right component and signed the collected result. The 2 parties are now in capacity to control that the SLA is really operational. On the side on Manifest enablers, they materialize a “convention of proof” which based on the commitments, the evidence to be collected as negotiated by the parties before operating a service under an SLA. At the moment of SLA definition the parties agreed on the way to measure the reality of a property and based of the common recognition on the way to measure it we demonstrate we operate the measure as claimed on the right component and signed the collected result. The 2 parties are now in capacity to control that the SLA is really operational.

The panellists also discussed an emerging hybrid approach which consists in combining some Domains evaluation under existing scheme (e.g., CC Assurance level delivered by Common Criteria evaluation, or EUCS certification scheme) with other Domains only constrained by SLA defining clearly the committed level of security services they offered. But even with this approach, the combinatory generated coupled with the complexity of these system of systems to be evaluated are out of reach. ENISA reduced the global problem to be resolved to a subset of around 10 business line, hyper specialized and focused on one service, for instance: the “Access control procedure to a 5G network” or “the provisioning line of the Telecom Context in one eUICC” operated over multi-party area.

1st International Conference on 6G Networking
July 06-08, 2022
Paris, France (Hybrid Conference)

WALT5G+ Workshop - Friday, July 08

09:00 - 10:00 Keynote #1: Cybersecurity: A collective responsibility and power
Claire Loiseaux (Internet of Trust, France)

10:00 - 11:00 Session 1

Framework for Trustworthy AI/ML in B5G/6G (R)
Sokratis Barmpounakis (WINGS ICT Solutions, Greece), Panagiotis Demestichas (University of Piraeus, Greece)

Trust Enhanced Security for Routing in SDN (R)
Nurefsan Sertbas Bulbul (Universität Hamburg, Germany), Orhan Ermis (Luxembourg Institute of Science and Technology, Luxembourg & LIST, Luxembourg), Serif Bahtiyar (Istanbul Technical University, Turkey), Mehmet Ufuk Caglayan (Yasar University, Turkey), Fatih Alagoz (Bogazici University, Turkey)

11:00 - 11:30 Coffee Break

11:30 - 12:30 Session 2

Level of Trust and Privacy Management in 6G Intent-based Networks for Vertical Scenarios (R)
Jesús A. Alonso-López, Luis Alberto Martínez Hernández, Sandra Pérez Arteaga, Ana Lucila Sandoval Orozco, Luis Javier García Villalba (Universidad Complutense of Madrid, Spain), Antonio Pastor (Telefonica I+D & Universidad Politécnica de Madrid, Spain), Diego Lopez (Telefonica I+D, Spain)

Modeling the Accountability and Liability Aspects of a 5G Multi-Domain On-Demand Security Services: An Unexpected Journey
Chrystel Gaber (Orange Labs, France), Anser Yacine (Conservatoire National Des Arts Et Métiers (CNAM) Paris & Orange Labs, France)

Defining the Threat Manufacturer Usage Description Model for Sharing Mitigation Actions (R)
Sara Nieves Matheu García and Antonio Fernando Skarmeta Gomez (University of Murcia, Spain)

12:30 - 13:30 Launch Break

13:30 - 14:30 Keynote #2: Towards a Resilient and Trusted 5G & Beyond: Current Challenges and Future Directions
Roberto Cascella (ECSO, Belgium)

14:30 - 15:00 Coffee Break

15:00 - 15:40 Session 3
The Impact of Manufacturer Usage Description (MUD) on IoT Security
Zeno Heeb, Onur Kalinagac, Wissem Soussi and Gürkan Gür (Zurich University of Applied Sciences (ZHAW, Switzerland)

eSIM Adoption: Essential Challenges on Responsibilities Repartition
Chrystel Gaber and Pierrick Kaluza (Orange, France)

15:40 - 16:40 Panel: Liability and Trust in Future Networks for 2030
Moderator: Gürkan Gür (ZHAW, Switzerland)

Panel Members :
- Gürkan Gür (ZHAW, Switzerland)
- Chrystel Gaber (Orange, France)
- Claire Loiseaux (Internet of Trust, France)
- Roberto Cascella (ECSO, Belgium)

16:40 - 17:00 Wrap Up

Figure 43. 1st International Conference on 6G Networking

8 Conclusions

Liability, accountability and responsibility are interlinked concepts which are at the centre of business and commercial relationships. Together, they express what task is expected to be performed (responsibility), the results expected and their evidence (accountability) and the consequences for not achieving the agreed results (liability).

Based on an overview of the existing legal and standards framework, this deliverable highlights the associated needs. It demonstrates that a fixed level of security throughout the entire 5G infrastructure is neither feasible for 5G E2E Service Providers nor satisfactory for Vertical Use Cases. Rather, the need is for on-demand security services and on-demand accountability.

The state of the art on liability modelling and handling shows a variety of initiatives around the topic of liability and liability management while none of them targets the same area as the one considered in this deliverable. Based on general definitions found in the state of the art, this deliverable defines a set of metrics related to transparency, responsibility, attributability and liability that can be used to define a service with on-demand accountability i.e., a 'convention of proof'.

This deliverable also defines a framework for a liability management system. The expectations for such a system are formalized with three functional objectives related to the identification of liability and accountability relationships, the collection of evidence and the analysis related to liability and compliance. The enablers developed in INSPIRE-5GPlus illustrate how each of these functions can be implemented and mapped with the High-Level Architecture defined in the project. Finally, the demonstrators of the project provide an example of how these enablers can be combined to achieve the higher goal of liability management.

Liability management for 5G End to End Management Services is still in infancy stage and this deliverable is the first brick to build such systems. One of the major challenges that lies ahead concerns the integration and use of AI in 5G Service Management systems. Currently, the scientific community concentrates on the definition of the trustworthiness of AI and multiple models are proposed. Once these approaches are consolidated or that a model emerges, it would be interesting to define what on-demand accountability means for such AI-based decision systems and use it to extend the on-demand accountability approach proposed in this deliverable.

References

[1] Möllering, G. (2005). The trust/control duality: An integrative perspective on positive expectations of others. International sociology, 20(3), 283-305.

[2] Contractworks software, https://www.contractworks.com/resources/topic/case-study, last visited in June 2022

[3] Cobblestone software, https://www.cobblestonesoftware.com/ , last visited in June 2022

[4] ContractPodAI product, https://contractpodai.com/news/contract-management-roi/, last visited in June 2022

[5] Hyperlex Contract management solution, https://hyperlex.ai/solution/, last visited in June 2022

[6] Cobbelstone Software demonstration, Cobblestone, https://www.youtube.com/watch?v=daf1Dk_yBvo, last visited in June 2022

[7] Design Patterns: Elements of Reusable Object-Oriented Software, Erich Gamma, and Rechard Helm and Ralph Johnson and Jon Vlissides, 1994, publisher: Addison-Wesley

[8] Chain of Responsibility, https://refactoring.guru/design-patterns/chain-of-responsibility , last visited in June 2022

[9] Myunghwan Kim, Roshan Sumbaly, Sam Shah, "Root cause detection in a service-oriented architecture", SIGMETRICS Perform. Eval. Rev. 41, 1, 93–104, 2013

[10] Dewei Liu, Chuan He, Xin Peng, Fan Lin, Chenxi Zhang, Shengfang Gong, Ziang Li, Jiayu Ou, Zheshun Wu, "MicroHECL: High-Efficient Root Cause Localization in Large-Scale Microservice Systems", CoRR 2021

[11] L. Wu, J. Tordsson, E. Elmroth and O. Kao, "MicroRCA: Root Cause Localization of Performance Issues in Microservices," NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, 2020

[12] A. Samir and C. Pahl, "DLA: Detecting and Localizing Anomalies in Containerized Microservice Architectures Using Markov Models", 7th International Conference on Future Internet of Things and Cloud (FiCloud), 2019

[13] European Commission, Directorate-General for Justice and Consumers, *Liability for artificial intelligence and other emerging digital technologies*, Publications Office, 2019, https://data.europa.eu/doi/10.2838/573689

[14] European Commission, Civil liability – adapting liability rules to the digital age and artificial intelligence, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en , last visited in June 2022

[15] C. Bonhomme, C. Feltus and D. Khadraoui, "A multi-agent based decision mechanism for incident reaction in telecommunication network," ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010, 2010, pp. 1-2, doi: 10.1109/AICCSA.2010.5587036

[16] G. Guemkam, C. Feltus, P. Schmitt, C. Bonhomme, D. Khadraoui and Z. Guessoum, "Reputation Based Dynamic Responsibility to Agent Assignment for Critical Infrastructure," 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, 2011, pp. 272-275, doi: 10.1109/WI-IAT.2011.194.

[17] G. Hatzivasilis, P. Chatziadam, N. Petroulakis, S. Ioannidis, M. Mangini, and C. Kloukinas, A.Yautsiukhin, M.Antoniou, D.Katehakis, G.Dimitrios, M.Panayiotou, Cyber Insurance of Information Systems: Security and Privacy Cyber Insurance Contracts for ICT and Healthcare, 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)

[18] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[19] ISO 14971:2019, Medical devices — Application of risk management to medical devices, https://www.iso.org/standard/72704.html , last visited in June 2022

[20] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC Text with EEA relevance

[21] R. Morabito, V. Cozzolino, A. Y. Ding, N. Beijar and J. Ott, "Consolidate IoT Edge Computing with Lightweight Virtualization," in *IEEE Network*, vol. 32, no. 1, pp. 102-111, Jan.-Feb. 2018, doi: 10.1109/MNET.2018.1700175.

[22] D. Hetzer, M. Muehleisen, A. Kousaridas and J. Alonso-Zarate, "5G Connected and Automated Driving: Use Cases and Technologies in Cross-border Environments," *2019 European Conference on Networks and Communications (EuCNC)*, 2019, pp. 78-82, doi: 10.1109/EuCNC.2019.8801993.

[23] J.S. Bedo, E. Calvanese Strinati, S. Castellvi, T. Sherif, V. Frascolla, W. Haerick, I. Korthals, O. Lazaro, E. Sutedjo, L. Usatorre, M. Wollschlaeger, White paper 5G and the Factories of the Future, 2015, 5GPPP whitepaper

[24] ENISA, Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, 2017

[25] Y. Khettab and M. Bagaa and D. L. C. Dutra and T.Taleb and N.Toumi, Virtual security as a service for 5G verticals, 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018

[26] ENISA, Good Practices for Security of Internet of Things in the context of Smart Manufacturing, 2018

[27] ENISA, Mapping of OES Security Requirements to Specific Sectors, 2018

[28] ENISA, Security and Resilience in eHealth - Security Challenges and Risks,2015

[29] V. Oleshchuk and R. Fensli, Remote Patient Monitoring Within a Future 5G Infrastructure, 2010

[30] INSPIRE-5GPlus, D4.1: Trust mechanisms for 5G environments

[31] C. Gaber and P. Kaluza, eSIM Adoption : Essential Challenges On Responsibilities Repartition, Workshop on Accountability, Liability and Trust, 2022

[32] S. Chan, What you need to know about China's AI ethics rules,Techbeacon, 2022, https://techbeacon.com/enterprise-it/what-you-need-know-about-chinas-ai-ethics-rules, last visited June 2022

[33] S.1776 – Artificial Intelligence for the Military Act of 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1776/text?q=%7B%22search%22%3A%5B%22s1776%22%5D%7D&r=1&s=1 , last visited in June 2022

[34] S.1705 – AICT Act of 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1776/text?q=%7B%22search%22%3A%5B%22s1776%22%5D%7D&r=1&s=1 , last visited June 2022

[35] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 , last visit in June2022

[36] LNE, Development of standards and labels, https://www.lne.fr/fr/expertises-innovation/creation-referentiels-labels-certification , last visit in June2022

[37] Labelia, le label IA responsable et de confiance, https://www.labelia.org/fr/labelia), last visited in June 2022

[38] GEEIS AI https://arborus.org/label/ , last visited in June 2022

[39] ISO/IEC JTC 1 Information technology

[40] INSPIRE-5GPlus, D4.3: Liability mechanisms for 5G environments, 2021

[41] C. Gaber, G. Arfaoui, Y. Carlinet, N. Perrot, L. Valleyre, M. Lacoste, J.P. Wary, Y. Anser, R.Artych, A. Podlasek, E.Montesdeoca, V.Hoa La, V.Lefebvre, G. Gür, The Owner, the Provider and the Subcontractors: How to handle Accountability and Liability for 5G End to End Service, 6GNet, 2022

[42] INSPIRE-5GPlus, D4.2: Trust management in multi-tenant/multi-party/multi-domain 5G environment, 2022

[43] INSPIRE-5GPlus, MS8 report

[44] C. Lee, K. M. Kavi, R. A. Paul, and M. Gomathisankaran, “Ontology of Secure Service Level Agreement,” in 2015 IEEE 16th International Symposium on High Assurance Systems Engineering, 2015, pp. 166–172

Appendix A Additional info

A.1 MS9 KPI

Generic KPIs
Mean Time To Detect
Mean Time to Contain
Mean Time to Resolve
Transaction speed
Packet Loss Ratio
Number of False positives
Number of False negatives
Initial time
Migration time
Service response time
Service downtime
SSLA enforcement

Table 28. Summary of MS9 Generic KPIs

Test-Case-Specific KPIs
Blocked adversarial examples rate
Ratio of allowed malicious scale-up
Automated vulnerability assessment
Automated model generation
Threat assessment
Cyber-security insights assessment
Latency
Mean Time to implement the MTD action
MTD action cost
Protection gain of an MTD policy
Mean decision time for MTD action
QoS gain/loss of the protected resources

Table 29. Summary of MS9 Test-case Specific KPIs

A.2 MS10 KPI

This section recalls the KPI defined in MS10 that were added MS9 KPI

- Mean Time To Detect that a function has been tampered with or is in incorrect location
- Mean Packet Loss Ratio during the switch between normal to critical mode
- Mean Ratio of Time Functions are Not isolated In Critical mode
- Mean Observation Report Request Response Time corresponds to the mean time required to provide an observation report after it was requested.

MS10 additional KPI
Mean Time To Detect that a function has been tampered with or is in incorrect location
Mean Packet Loss Ratio during the switch between normal to critical mode
Mean Ratio of Time Functions are Not isolated In Critical mode
Mean Observation Report Request Response Time corresponds to the mean time required to provide an observation report after it was requested

Table 30. Summary of MS9 Test-case Specific KPIs