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

D2.2: Initial Report on Security Use Cases, Enablers and Mechanisms for Liability-aware Trustable Smart 5G Security

Version: v0.14

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	30/04/2021
Submission date	25/05/2021
Lead editor	Jordi Ortiz (University of Murcia)
Authors	Vincent Lefebvre (TAGES), Alejandro Molina, Ana Hermosilla, Rodrigo Asensio, Antonio Skarmeta (UMU); Chafika Benzaid, Othmane Hireche, Tarik Taleb (AALTO); Orestis Mavropoulos (CLS), Gürkan Gür, Wissem Soussi (ZHAW), Antonio Pastor (TID), Huu Nghia Nguyen, Edgardo Montes de Oca (MI), Dhouha Ayed, Geoffroy Chollon, Cyril Dangerville (TSG), Rafal Artych (OPL), Pol Alemany, Charalampos Kalalas, Ricard Vilalta, Ricardo Martínez, Laia Nadal, Javier Vílchez (CTTC), Pawani Porambage, Tharaka Hewa, Diana Pamela Moya (UOULU), Marc Lacoste (ORA)
Reviewers	Raúl Muñoz (CTTC), Maria Christopoulou (Demokritos)
Work package, Task	WP2, T2.2
Keywords	Security Enablement, 5G Security Use Cases, ZSM HLA

Abstract

This Deliverable introduces the enablements that support current and future security assets and architectures in present 5G and beyond. A description of these enablements and the current state of the art is revisited while identifying inherent risks and challenges from their usage, while envisaging their possible usages. Based on these technologies and the enablements introduced, a set of initial Use Cases at platform and vertical level contextualize and demonstrate the usage of the security enablements as well as the trust/liability mechanisms. The set of requirements that need to be addressed and their relationship with the Use Cases is listed and addressed by proposing the High-Level Architecture (HLA) being the backbone of the project outcomes. Finally, an analysis of the COVID-19 on the 5G Security landscape is presented.

Document revision history

Version	Date	Description of change	List of contributor(s)
v0.1	23/01/20	Table of Content	Jordi Ortiz
v0.2	29/06/20	Extended table of content with contributors list. Initial content added	Jordi Ortiz, Jorge Bernal, Ramón Sánchez, Ana Hermosilla
v0.3	12/10/20	First round of contributions to Section 3	All partners
v0.4	11/01/21	Updated Table of Contents	Jordi Ortiz
v0.5	11/02/21	Sections 2 and 3	All partners
v0.6	01/04/21	Sections 5, 6 and Annex A	All partners
v0.7	04/04/21	Pandemic and Close Loop	Chafika Benzaid, Jordi Ortiz
v0.8	16/04/21	Section 3 and Annex B	Gürkan Gür, Edgardo Montesdeoca, Vincent Lefebvre
v0.9	20/04/21	First version to review and Section 3 enhancements	Cyril Dangerville, Marc Lacoste, All partners
v0.10	01/05/21	Reviewed integrated version	Jordi Ortiz
v0.11	11/05/21	First Review version	Jordi Ortiz
v0.12	13/05/21	Second Review version	All partners
v0.13	16/05/21	Final version	Antonio Skarmeta, Jordi Ortiz
v0.14	17/05/21	Final editing	Anja Köhler

List of contributing partners, per section

Section number	Short name of partner organisations contributing
Section 1	UMU
Section 2	AALTO, TAGES, MI, ZHAW, CTTC, NCSRD, TSG, UOULU, ORA, CLS, UMU
Section 3	TID, AALTO, TAGES, MI, ZHAW, CTTC, NCSRD, TSG, UOULU, ORA, CLS, UMU
Section 4	TID, AALTO, TAGES, MI, ZHAW, CTTC, NCSRD, TSG, UOULU, ORA, CLS, UMU
Section 5	UMU, AALTO, ZHAW
Section 6	UMU, AALTO
Appendix A	CLS

Disclaimer

Acknowledgment

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

This deliverable further extends and updates the analysis of potential Security Enablements performed already in the context of INSPIRE-5Gplus focusing on the risks and challenges to be faced. In addition, a prediction of the future applications of such enablements to enhance the liability and trustworthiness of 5G architecture is foreseen. In that line, enablements related to network automation & zero touch management are further researched; trusted execution environments for different hardware vendors are further analysed and their future usage is proposed; DLT, Dynamic Liability and Root Cause Analysis are described also key enablements to operate 5G networks; AI techniques are not only envisioned to operate autonomously but also to defend autonomously from autonomous attacks; Finally SSLAs and Multi-Domain policies are envisioned as the contractual and user/business inputs that need to drive the automation.

An initial set of security use cases is introduced, their relationship with the identified enablements and more importantly, how this initial list is going to be addressed in INSPIRE-5Gplus' proposed test cases. These Use Cases have been identified by their coverage of security requirements from previous 5G-PPP projects, the enablers envisaged within WP3 and WP4, their usability and complementarity.

Considering the enablements and the use cases, INSPIRE-5Gplus' High-Level Architecture is presented alongside the requirements that lead to its definition, the functional blocks and services provided and the closed-loop. In addition, non-functional requirements were extracted from the business and organizational requirements questionnaire that can be inspected in detail in the Appendix.

Finally, an analysis of the COVID-19 pandemic on 5G Security threat landscape is also performed identifying how the usage of the network has changed, probably to remain evolving. Also, the perception of network services from the users has changed, realizing on their dependence on the offered services for their daily life. The surface to be protected has increased and operators need to act accordingly.

The content of this deliverable includes:

- The definition of Enablement.
- The analysis and update of enablements state of the art.
- Identifies the Risks and Challenges of each enablement.
- Predicts the future applications related to security of each enablement.
- Defines an initial list of Use Cases and their relationship with the enablements.
- Introduces the High-Level Architecture proposed by INSPIRE-5Gplus in detail.
- Produces an analysis of the pandemic on the security landscape.
- Lists the results of the business and organizational requirements questionnaire.

The work that has been carried out in the scope of Work Package 2 during the first 18 months of the INSPIRE-5Gplus project, covering the identified enabling technologies and the definition of the High-Level Architecture leveraging on such technologies with a set of Illustrative Use Cases to demonstrate the potential of the proposal as a collaborative work of the partners involved, serving as the foundation to the deeper analysis of Use Cases already on-going and the development of INSPIRE-5Gplus enablers.

Table of Contents

List of Figures

List of Tables

Abbreviations

5GC	5G Core
AMF	Access control and Mobility Management Function
AUSF	Authentication Server Function
CU	Central Unit
DU	Distribute Unit
DVB	Digital Video Broadcast
E2E	End-To-End
EC	European Commission
eCPRI	evolved Common Public Radio Interface
eMBB	Enhanced Mobile Broadband
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FOSS	Free and Open Source Software
GAN	Generative Adversarial Network
GDPR	General Data Privacy Regulation
gNB	Next Generation Node B
HOA	Higher Order Ambisonics
JSON	JavaScript Object Notation
mMTC	massive Machine Type Communications
KVM	kernel-Virtual Machines
MANO	Management and Network Orchestration
MEC	Multi-Access Edge Cloud
mMTC	massive Machine Type Communications
NF	Network Function
NFV	Network Function Virtualisation
NR	New Radio
NRF	Network Function Repository Function
NS	Network Service
NSA	Non-stand Alone
NSSF	Network Slice Selection function
OS	Operating System
PCF	Policy Control Function
PNF	Physical Network Function
REST	Representational State Transfer
RRU	Remote Radio Unit

SA	Stand Alone
SBA	Service-Based Architecture
SDN	Software Defined Networking
TCB	Trusted Computing Basis
UDM	Unified Data Management
UPF	User Plane Function
URLLC	Ultra-Reliable and Low Latency Communications
ZSM	Zero-touch network and Service Management

1 Introduction

1.1 Scope

As the second public deliverable of the INSPIRE-5Gplus project's Work Package 2 (WP) introducing the first subset of Use Cases, Enablers and Mechanisms for liability-aware trustable smart 5G security. This deliverable identifies a set of architecture level requirements to provide liability-aware trustable and smart 5G security based on a set of emerging enabling technologies. The deliverable also provides an initial list of Use Cases and their relationship with the emerging enabling technologies to finally introduce the INSPIRE-5Gplus' proposed High-Level Architecture. The present deliverable addresses the milestone "Identification of relevant enablers to provide liability-aware trustable smart 5G security and definition of security use cases".

1.2 Target audience

The target audience of this deliverable are stakeholders related to security of 5G technologies and infrastructure. The deliverable describes technical terms and technologies that are used to increase the security posture of 5G systems and use cases.

1.3 Terminology

- **Security Asset**

A security asset is any component that supports security related activities (protection, detection and/or mitigation). It can represent hardware, software or virtualized functions.

- **Security Enabler**

INSPIRE-5Gplus Security Enablers are the major building blocks to achieve a fully automated End-to-End security management in multi-domain 5G environments. They are all the security features, products or services developed within the project. These enablers can leverage on one or more security assets, their configuration and logic of operation to empower the Security as a Service paradigm.

- **Security Enablement**

Security Enablements are defined as new initiatives and technologies/techniques possessing the potential to significantly contribute to 5G security evolution. An enablement is therefore the technology and abstraction on which Security Enablers are based. The enablements, unlike enablers, are not limited by actual technology or the scope of the project. They are thought to be the building blocks on which present and future enablers can be categorized. One security Enabler can rely on multiple Security Enablements.

- **Security Management & Orchestration Functions**

The security management and orchestration functions are the set of functional modules (e.g. security decision engine, security orchestrator, trust manager) that operate in an intelligent closed-loop way to enable SD-SEC orchestration and management that enforces and controls security policies of network resources and services in real-time. These functions leverage several security enablers to implement their services.

1.4 Structure

The main structure of this deliverable is summarized as follows:

- Section 2 contains the emerging enabling technologies based on which a liability-aware trustable and smart 5G security solution is based;
- Section 3 contains the initial list of identified Use Cases;
- Section 4 introduces the proposed High-Level Architecture relying on the architectural level requirements and addresses the mapping of the emerging enabling technologies into it;
- Section 5 describes the effect of the pandemic on the security landscape.
- Section 6 concludes this deliverable;

2 Emerging Enablements

This section revisits the enabling technologies identified in D2.1 [2], updates the existing State of the Art and identifies the risks and challenges of these enablements. More importantly how these enablements, while facing these restrictions, still can be used to enhance the different characteristics (zero-touch management, liability, trust, etc.) that an E2E 5G security solution is thought to provide. These enablements do not only introduce inherent risks but also impose requirements taken into account to propose INSPIRE-5Gplus' High-Level Architecture. These requirements are described as part of Section 4.2.2, due to their involvement into the initial set of Use Cases presented in Section 3.

2.1 Automation & Zero touch management

Management automation is key in dealing with the envisioned complexity of 5G systems while meeting their stringent performance requirements [1]. Indeed, the shift to fully automated End-to-End (E2E) management will boost the flexibility and efficiency of service delivery and reduce the Operating Expenses (OPEX) through self-managing capabilities (e.g., self-configuration, self-optimization, self-healing, and self-protection). ETSI's Zero Touch network and Service Management Industry Specification Group (ZSM ISG) is a prominent initiative to meet the goal of fully automated management, that we identified in D2.1[2]. The primary goal of the ETSI ZSM ISG is to specify an end-to-end network and service management reference architecture [3] enabling agile, efficient, and qualitative management and automation of emerging and future networks and services. The ZSM framework's reference architecture is designed to empower full automated network and service management in multi-domain environments that include operations across legal operational boundaries [3].

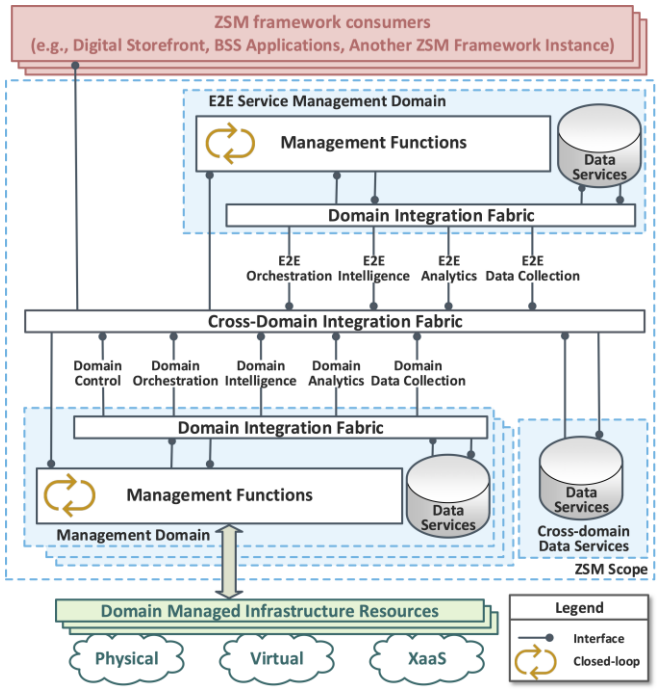


Figure 1 - The ZSM Reference Architecture.

As illustrated in Figure 1, the ZSM architecture [1] comprises multiple management domains (MDs) including E2E service MD, intra- and cross-domain integration fabrics, and cross-domain data services. Each MD is responsible for intelligent automation of management and orchestration of resources and services within its scope. The E2E service MD is a special MD that manages E2E, customer-facing services across multiple administrative domains. It is worth mentioning that the decoupling of MDs from the service MD reduces the overall system's complexity and allows

independent evolution of domains and E2E management operations. Each MD, including the E2E service MD, encompasses several management functions grouped into logical groups (e.g., domain collection services, domain analytics services, domain intelligence services, domain control services, and domain orchestration services) and supplies a set of management services via service interfaces. The services are provided and consumed through either the intra-domain integration fabric (for services local to a domain) or the cross-domain integration fabric (for services that can be exposed cross-domain). The Cross-domain Data Services facilitate access to data and its cross-domain exposure. The data can be used by intelligence services to enable AI-based closed-loop automation at domain-level and cross-domain [1].

Being aware of the importance of management automation in 5G, the topic has gained much attention from the research community. Some of the existing contributions in the literature have targeted the empowerment of self-healing (e.g., [14], [15]), self-adaptative (e.g., [17]), and self-protection (e.g., [18], [19]) capabilities to address anomalies and attacks in 5G networks. The AI-based management automation has also been in the heart of several 5GPPP's Phase 1 (e.g., Cognet[2], CHARISMA[3], SELFNET[4]) and Phase 2 (SliceNet[5]) projects. However, most of the existing solutions rely on basic ML techniques and/or target single domain. Two ongoing Phase 3 ICT-20 projects, namely MonB5G[6] [19] and 5GZORRO[7] [20], are leveraging the AI-assisted zero-touch management paradigm to enable full automated network, service, and security management across domains. Different from INSPIRE-5Gplus, the two projects are not aiming at security management and considering security as only one of the FCAPS (Fault, Configuration, Accounting, Performance and Security) operations to be enabled in their platforms. Recall that INSPIRE-5Gplus aims to provide a zero-touch E2E security management framework that follows the key design principles of the ETSI ZSM reference architecture.

Despite the promised flexibility, efficiency and cost-effectiveness in security management, full automation poses new security risks stemming from its ability to replicate a small, isolated error broadly and rapidly, which can jeopardize the security of the entire ecosystem. In what follows, we discuss the potential security risks that may hinder a ZSM system and advocate a set of measures to be put in place to safeguard ZSM system security.

2.1.1 Risks and Challenges

In INSPIRE-5Gplus, we comprehensively investigated the potential security threats that may hinder a ZSM system [1]. Indeed, the introduced attack surface is broad as a ZSM system relies on several enabling technologies and concepts (e.g., virtualization, programmability, automation, AI/ML); each of them bringing its own security threats, which need to be carefully addressed. In the conducted study, we classified the potential security threats into 5 categories, namely: (1) Open API's security threats, (2) Intent-based security threats, (3) security threats driven by closed-loop networked automation, (4) AI/ML-based attacks, and (5) attacks due to adoption of programmable network technologies (i.e., NFV and SDN). Table 1 below summarizes the main security threats we identified. To demonstrate how these attacks can be leveraged to hinder the security of the managed system, we described various illustrative examples, including: how an Intent tampering attack results in setting an undesirable security level to a slice, how attack driven by closed-loop automation can lead to a Man-In-The-Middle attack, and how an adversarial attack against an ML model allows to evade

[2] http://www.cognet.5g-ppp.eu
[3] http://www.charisma5g.eu
[4] https://selfnet-5g.eu
[5] https://slicenet.eu
[6] https://www.monb5g.eu
[7] https://www.5gzorro.eu

detection of malicious DoS traffic. More details on the identified ZSM's threat surface and the illustrative examples can be found in [1]. Note that the threats related to the use of AI/ML are further elaborated in Section 2.3 of this deliverable. Similarly, threats related to TEE are further elaborated in Section 2.2.

Enablement	Security Threats	Mitigation Measures
Open API	Parameter attacks	Input validation
	Identity attacks Tampering attacks MITM attacks	Secure communication
	(D)DoS	Throttling/rate limiting the usage of APIs
Intent-based Interfaces	Information exposure Intent tampering	Authentication & authorization controls Secure communication
	Malformed Intent	Intent format validation
	Conflicting Intents	Conflict detection/resolution
AI/ML	Adversarial attacks	Input validation Adversarial training Defensive distillation Defence GANs Concept drift
	Model extraction attacks Model Inversion attacks	Control information provided by ML APIs Add noise to ML prediction Add noise to execution time of the ML model
SDN/NFV	Spoofing Privilege escalation Information disclosure Tampering	Authentication & authorization controls Secure communication TPM, vTPM
	DoS	Malicious traffic monitoring Limiting the number of flow requests Resource monitoring and usage limitation Resource isolation Distributed SDN controller architecture
	Introspection attacks	TEE
	Software vulnerabilities	Secure software patching procedures

Enablement	Security Threats	Mitigation Measures
		System hardening techniques

Table 1 - ZSM security threats and mitigation measures [1].

2.1.2 Future Applications

In 5G and beyond networks, the adoption of zero-touch security management is a key to empower intelligent and autonomic security management capabilities (e.g., self-protection, self-defence, self-healing), and enable flexible and dynamic provisioning, deployment, and management of security services. This will allow improved robustness and lower operational costs. But as we already pointed out in D2.1[2], the ZSM serves as a blueprint for implementing E2E closed-loop automated network management. This means practical instantiation and implementation needs to be developed to demonstrate the viability of ZSM in delivering fully automated and smart security management cross domains. To this end, the services composing the domain-level and E2E level security management closed-loops need to be specified and implemented. This includes for instance services for collecting security-relevant data, analysing the collected data to extract insights on potential security threats, deciding the appropriate mitigation plan to address the detected/predicted security threats, and enforcing the necessary security policies to fulfil the expected Security Service Level Agreement (SSLA).

Furthermore, appropriate measures to address the security risks stemming from the adoption of ZSM are paramount to fully reap its benefits in empowering fully automated security management in 5G and beyond networks. Driven by the identified threat surface of ZSM, we advocated a set of potential mitigation measures and best practices that should be adopted to make a ZSM system resilient to the aforementioned security threats. Table 1 summarizes the mitigation measures we are advocating to tackle the identified security threats. In INSPIRE-5Gplus, we pay a particular attention to the use of TEE for addressing some attacks related to softwarization/virtualization technologies and to the defences for withstanding against threats targeting AI/ML techniques. The use of TEE and defences against adversarial attacks are further elaborated, respectively, in Section 2.2 and Section 2.3 of this deliverable.

2.2 Trusted Execution Environments

Hardware based Trusted Execution Environments (TEE) embed processor design directly therefore offered on commodity processors as a security enablement for arbitrary payloads. Their core function is to elaborate silicon-powered encryption-decryption of the payload memory pages for payload isolation against other payload or kernel code. Introspection attacks conducted by privileged users are halted too as the decrypted pages cannot be accessed outside the TEE itself

The security functions offered by TEEs vary by vendors (e.g., Intel, ARM, AMD, Risc-V) as identified in D2.1[2] and its Appendix B which produced an in-depth survey of existing TEEs and alleviating frameworks. These functions are by order of prevalence runtime process memory isolation, data at rest secure storage and remote attestation.

In contrast to TPM (i.e., Trusted Platform Module), TEE though being specified in their principle by Global Platform industry and users working group, do vary significantly in their implementations, which are themselves are different. TPM are stand-alone chipsets (although some integrated design also exist) exposing precise specified and pre-defined cryptographic and safe data storage functions. Both assets (i.e., TPM and TEE) serve different security goals and are complementary: While TPMs remain instrumental in establishing platform trust through a TPM-measured boot, TEE bring trust to the application as well as payload isolation. At Inspire-5Gplus, we believe both technologies are complementary, and their association brings an absolute security cover. Typically, all side channel attacks on TEE (when they do not rely on physical instrumentation) can be prevented if both kernel

code verification and process whitelisting are separately brought, typically by leveraging a TPM. Conversely, TEE will bring what a TPM cannot offer: payload isolation, data sealing and platform type remote attestation.

Apart the discrepancies in offered security functions, a key differentiation element is the size and type of the Trusted Computing Basis (TCB) (i.e., TEE content). Intel's SGX and AMD's SEV shelter totally different TCBs. Intel's SGX SDK advocates for the most restricted TCB (i.e., security-sensitive part of an application while AMD's SEV embarks complete virtual machine content (including the guest operating system, libraries, ...). If the latter reduces drastically the developer burden for the implementation (i.e., effortless transparent implementation), it also leads to a much higher number of vulnerabilities to exploit the attacker may know a priori (i.e., in O.S or open-source libraries). With AMD's SEV, the effortless implementation should be balanced with a higher attention on vulnerability search. Conversely, Intel's policy is well-funded as any TEE embedded vulnerability exploit operates covertly. Oblivious rogue processing is a scaring scenario to prevent. As an important reminder, TEE do not prevent vulnerable code to execute. As a consequence of Intel's design, SGX comes with a restricted memory space (to 128 Mb) while SEV TCB size is not capped. In practice, this diverging TCB definition leads to two very different solutions not associated and generally not directly compared by academic researchers. Our survey also shows the two original and different main weaknesses on both sides (i.e., SGX's code confidentiality and SEV page integrity), which since then have been corrected (i.e., Intel V2.0 PCL mode [22] and AMD's SEV-SNP [23] new version respectively).

Finally, in order to invest on TEE technology, one cannot ignore the intense and unabated battle lead by agile academic researchers since SGX and SEV market releases. Undoubtedly, Intel SGX security guaranties have been challenged with (much) higher pressure as SGX's security promises are either viewed as more far-reaching or because Intel is in a dominant (though challenged) market position. Intel's iPSIRT team has been under intense and constant pressure since 2017 through several waves of distinct side channel attacks, provoking and speeding up several runs of rapidly offered microcode updates. One more element took part in this harsh challenging campaign: TEE's unprecedented security threat, which opposes TEE to an unlimited attacker (i.e., full privileged user, malicious kernel). TEE security threat is most challenging and academics researchers somehow demonstrated that it was not easy to hold (if not being untenable on the long run). As one more memory isolation technique (as offered by hypervisors and kernel-user separation from operating systems), TEEs had faced instantly pre-conceived isolation break challenges initiated against other techniques. The same tactics were taken, leveraging previously defined methods (content-based page fault generation, cache-timing attacks, speculative execution). Spectre and Meltdown initial attacks (breaking memory isolation on commodity operating system) have been rapidly derived in their SGX-pronged variant as early as six months later. Skilled academic teams from EC and US have (collegially and through responsible releases with Intel's iPSIRT team) have jostled SGX but without breaking it thanks to Intel pro-activity in emitting timely the corresponding patches. In fact, SGX has been hardened during these hard times while no real-world attack has ever emerged. At the end of the day however, a collateral victim can be viewed as being performance. SGX SCA exploit weaknesses always to be associated to the processor architect-designer search for higher performance. As a consequence, removing such vulnerabilities (which turns to be Intel's microcode mitigation) impacts forcibly the performance in a negative way.

2.2.1 Risks and Challenges

The essential risks identified in the utilization of TEE are identified security risks and the performance impact. Three main **security risks** can be identified as the intrinsic vulnerabilities of the TEE technologies, the vulnerability of the trusted application (i.e., Trusted Computing Base) and the risks associated with a wrong definition of the TCB.

- ***Intrinsic vulnerabilities of TEE technology risks***

We surveyed the main side channel attacks and exploitation of architectural weakness over the three

main processor families (Intel, AMD, ARM). Our findings are given below.

1. Intel ’s SGX Side Channel Attacks:

Since SGX inception (first SGX V1 enabled processors on the market at the end of 2014), the following four waves of SCAs had successively surfaced:

Page-fault attack, [24][25][26] (first wave) aka controlled-channel attack exploits DRAM access patterns to infer a secret used by the victim at a precise (i.e., controlled) step of its execution. Page faults (and their memory address) can be deterministically or statistically associated to the page content. Page faults are generated by the rogue O.S intentionally and the sequence of page faults during execution is correlated to the targeted secret.

Direct cache-timing attacks [27][28][29][30],(second wave) are focused on the cache, shared by SGX victim code and a sibling rogue spy process. Compared to page fault-SCAs which confer a spatial granularity are 4 Kbytes (ie, the size of a swapped page), cache timing attacks enhance drastically the resolution to 64 bytes (i.e., the size of a cache line, the elementary cache store). Two prominent extraction methods are Flush and Reload and Prime and Probe. Both consist at forcing the victim to load a secret in the cache (through cache content eviction prior to the load) and infer, through timing measure, the loaded content value according to the location of the loaded cache line.

Speculative execution attacks, [33][34][35][36] (third wave) emerged in early 2018 with immense mediatic attention caused **Spectre** [32] and **Meltdown** [31] twinned and concurrent publications and whose scope spans over all major processor architectures (e.g., AMD, ARM and Intel) and all types of memory isolation techniques (e.g., kernel-user space, hypervisors, TEE). Speculative execution is a CPU design optimization technique aimed at gaining CPU performance. The processor speculatively (i.e., takes a deliberate decision to) executes instructions and memory fetches in advance, before it timely validates and integrates this execution path results or conversely it removes all states. By doing so, all memory guards are abated in the sake of performance during this transient phase. Spectre and Meltdown exploits two different types of speculative executions as branch prediction (i.e., control flow-based advanced branch execution) and out-of-order execution (i.e., aggressive sequencing of processor micro-operations inside one instruction). Specifically targeting SGX, two major publications emerged six months later demonstrating the practicality of one Spectre-like and one Meltdown-like attack aka SGXPectre and Foreshadow.

Micro Architectural Data Sampling attacks [37][38][39][40][41][42][43], (fourth wave) refers to speculative execution processed at the lowest level using process-agnostic untainted buffers surrounding the ALU. Buffers content (valid or stale) is systematically speculatively used by-default by the ALU while they are not tagged and are therefore address-space independent. MDS diverts from wave 3 as going through a deep reverse engineering on the Intel architecture exclusively to infer how buffers interfere between them, the ALU and L1/L2 caches, leading to buffer leaks (directly or indirectly by the L1 cache).

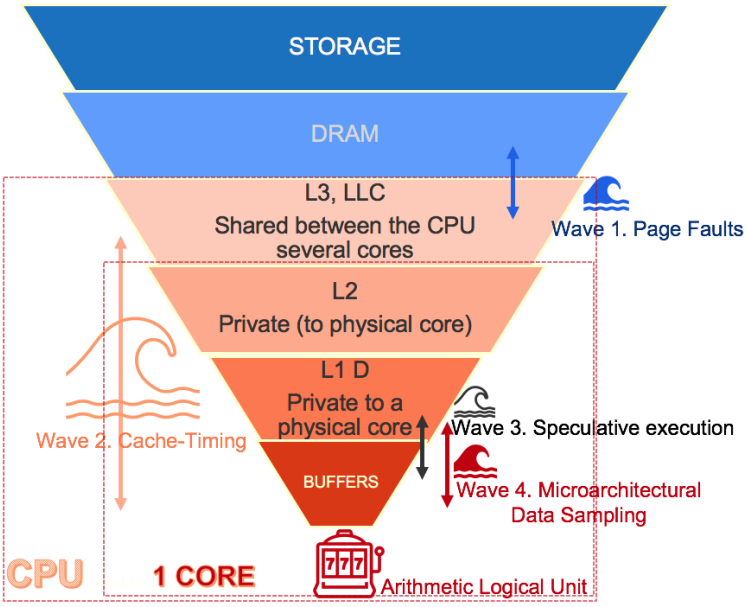


Figure 2 - Waves of Side Channel Attacks and relative position against memory elements.

Figure 2 represents four waves of Side Channel Attacks and relative position against memory elements. The figure shows the memory action domains of the SCA waves as well as the progressive descent closer to the ALU.

Mitigations offered by Intel against SGX-targeted SCAs:

- Wave 1 and 2 are not mitigated by Intel's microcode updates as they are viewed as software vulnerabilities. Performance costly software mitigations are offered by various solutions [44][45][46][47][48][49][50][51][52][53][54][55][56][57][30][58][59]. Better, one shall consider the use of Intel facilities (not specifically addressing SCAs and offered separately) such as the use of AES-NI instruction [69] set or cache allocation technology (CAT). [70]
- Wave 3 and 4 are conversely almost always mitigated by Intel's microcode as being considered by as falling within SGX's security threat. Some of the offered mitigations ask for developer accurate and measure leverage to prevent a severe overhead.
- All SCAs impose either a malicious kernel or a malicious sibling process spying the victim code. As a consequence, none of the SCAs can be successfully mounted in an environment where the kernel is verified and a process whitelisting produced. ETSI NFV Sec specified environment is the defence needed to halt all and any SCAs of today and tomorrow. More, all SCAs are targeted and coined to extract a secret handled by a pre-known software. None of the SCAs work for specific and unknown code if this code cannot be extracted in clear text before outside the TEE. Intel V2.0 PCL mode shall be used as it brings software confidentiality before entering the TEE.

2. AMD's SEV Side Channel and structural Attacks:

Before June 2020's release of SEV-SNP upgrade, three types attacks were exploiting SEV VM page integrity lack: Chosen plaintext attacks [63], Page table manipulation [60][61] and an hybrid cache-timing and Fault injection attacks [62]. The two latter modes are similar to techniques leveraged in wave 1 and 2 (against SGX). SEV has another failure with its unprotected **I/O** as recently exploited by [63] Exploiting Unprotected I/O exploits page faults (with a higher granularity than SGX).

A last known exploited path is **SEV unencrypted control block** (Hetzlet and Buhren: exploiting unencrypted VMCB**)**, a data structure in memory shared by the hypervisor and the guest VM, which stores the values of guest's general-purpose registers and control bits for handling virtual interrupts at the time of VMexit. The technique exploits unencrypted VMCB using code gadgets in

the guest memory based on return-oriented programming to arbitrarily read and write encrypted memory in the guest VM. The security issue caused by unencrypted VMCB, however, has been mitigated by SEV-ES variant.

When considering **Speculative attacks** (wave 3) targeted on TEE-capable or not processors, AMD shows a significant advantage against SGX. In general, enlisted CVEs against SEV are more than one range of order less numbered than SGX's. The NG Spectre and Meltdown attacks are significantly less affecting SEV than SGX and new generations of AMD processor (Epyc and Ryzen) are immune against Meltdown (Spectre v3). As a reminder, as SGX's MDS (wave 4) is targeted to Intel's own micro architecture, it comes with no surprise that SEV is immune to MDS. AMD also offers microcode updates to mitigate several attacks on legacy processors, as well as a guideline whitepaper for developers (*Software Techniques for managing Speculation on AMD processors*).

3. ARM's Trustzone Side channel and structural attacks

ARMageddon [64] demonstrated that all types of cache timing attacks (similar to wave 2) are possible (Flush and Probe, Prime and Probe, Flush and Flush, Evict and Reload) in cross-core scenario in non-rooted platforms. The attacks are all related to the T-Table lookup phase of AES.

Lapid et al [65] has also proven to extract AES 256 key (in its harder to extract GCM mode) from Samsung trustlet.

Trustzone Secure Monitor Calls has been discovered with vulnerabilities by Gal Beniamini [66], making it possible to erase trusted O.S memory by issuing an overflow in the trusted application leading to get a reach to the SMC. This attack can be viewed as related to a TCB-inside vulnerability though it also exploits the SMC handler (an architectural component).

Speculative attacks: Straight-Line Speculation (SLS) is a control flow based speculation class of attacks (similar to wave 3) exclusively valid for ARM V8-A (cortex A) and for which ARM deliver a white paper to developper (June 2020) [67], as well as automated mitigations through patchs to compilers (GCC and LLVM). It is referenced as CVE 2020-13844 and was discovered as part of Google's safe side challenge program.

Challenges associated to TEE intrinsic vulnerabilities

The global security landscape is fragmented, constantly evolving and maintaining the TEE security guaranties demands an investment specific to each CPU family. TEEs, when scratching below the surface (and the marketing selling material) are light overlays on pre-existing architectures, sharing many CPU resources with the non-protected world. As such, even though they have shown a strong resilience thanks to software (microcode) updates, it is hazardous to over rely on one TEE technology on the long run. Having said that software will always be more secure inside a TEE than outside.

Each type of TEE brings its own security issues and mitigation strategies and workflow (e.g., TCB recovery service from Intel) which calls for a specific expertise effort for each of them. In practice, security experts are not covering the whole fragmented CPU vulnerability area. The ARM expertise essentially required for smartphone application security (with possible extension to IoT) is a distinct expertise area from X-86 TEE field. For the latter, a question remains as SGX experts are probably less acquainted with SEV security issues. As stated above, there are simple and long-term strategies to drastically reduce such complexity (i.e., authenticating the kernel, white-listing all process mounted on a platform, ensuring code confidentiality all way through before the code is located inside the TEE ready for execution). However, these sanitization measures on the targeted platform may not be practical. Typically, on a MEC motherboard, a TPM may not be present. Henceforth, two security challenges can be defined as:

- Reducing the dependency to one TEE type in the sake of a universal TEE enablement which does not reduce the overall security level and generate high overhead.
- Defining a model to reach platform trustiness with minimal hardware and software requirements

Risks associated to TCB content's definition and vulnerabilities

When using TEE, it is of primordial importance to make sure than the code (or when a VM in the case of SEV) does not contain vulnerabilities. There are no TEE-specific tools for vulnerability search but simply a more stringent need to use such standard tools and associated update management methodologies. Reducing the TCB size is always relevant but it reaches rapidly its limits with VM content (AMD's SEV case) as the guest O.S cannot be reduced beyond the core minimal as well as the application cannot be safely split into several VMs. TCB size reduction is the prime and fundamental question for Intel's SGX user. Security architects should get a clear understanding on the code structure to define the "security-sensitive", to cut it out from the rest and consider how the transfers between both parts can leak secrets and impact negatively the security. It is not an easy question. A challenge for us is how to cancel this complex question, by offering a solution that takes it on the behalf of the users.

With regards to the **performance impact**, here-below, we restrict our analysis on X-86 TEE, starting with SGX performance survey followed by a comparison with SEV.

Targeted for the telecom industry, [80] elaborates a horizontal (slice) Chain of Trust bridging enclaves (typically spread over a slice) can be constructed based on Intel system enclaves. SGX for SDN and NFV implementations have been experimented extensively [75][76][77][78][79]. Based on OpenSGX emulation tool, the implementation delivers a first idea of the latency in establishing the CoT according to the size of the chain (i.e., number of checked nodes).The lessons learnt regarding SGX performance from these works are given below:

- SGX Enclave max memory area (EPC) limitation at 128 Mb constrains the type of network processed data (i.e., metadata instead of control plane or data frames).
- Two events contribute heavily to SGX overhead: SGX paging (decryption and encryption when a page is loaded and stored from the EPC to the processor cache) and SGX context switches. Researches have been produced on both sides to reduce the overhead [73][74]**.**
- To reach near-native throughputs, performance optimization is a must (e.g., define the best trade-off for the TCB (code and processed data) content leading to the reduction of paging and context switches). The performance impact varies in a large extent from a few percent to 100%. Optimization is unescapable.
- Frameworks such as OpenSGX, whatever their merits in simplification, may lead to unacceptable throughput drop.

While comparing SGX with SEV, [72] produces a direct benchmarking for both SGX and SEV and for a significant and representative set of publish/subscribe cloud applications. It is worth noting that the SGX implementation is based on Graphene framework (a source of performance drop). The authors' conclusion that SEV induces significantly less overhead than its SGX competitor (e.g., "Many of our memory-intensive benchmarks run at near-native speed with SEV") actually comes with no surprise. As SEV shelters a full VM stack, while paging costs shall be equivalent between both techniques, SEV certainly induces less context switches than SGX.

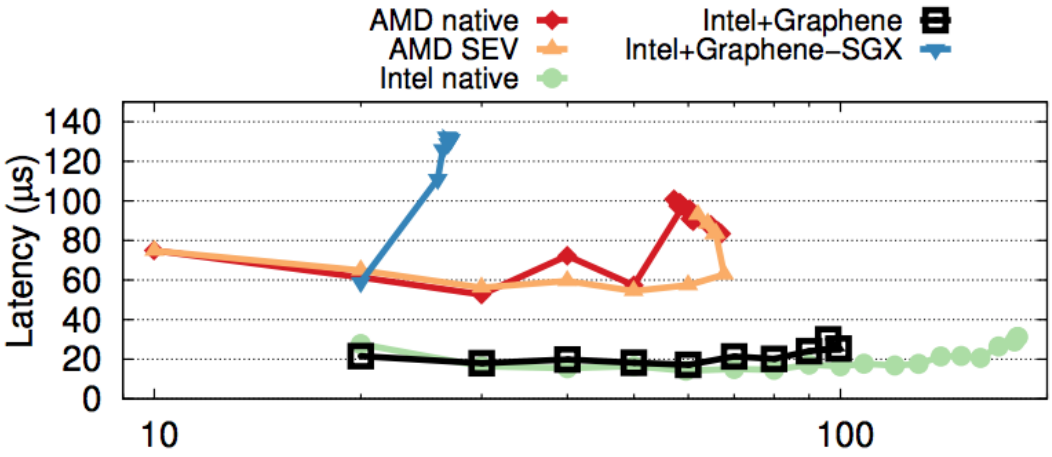


Figure 3 - Comparison of latency for various systems

Figure 3 shows lower latency at Intel native but a significant slowdown (higher latency) when using SGX, while SEV latencies are closer to the AMD native curve.

Performance of SEV does not need more optimization than SEV needs any sorts of implementation efforts for the users. Conversely, SGX does require optimization for being used on core network functions to reach near native throughputs. This optimization can impact the security scheme defined by the security architect (as stated above). Performance optimization does not fit well (at least at first view) with TEE frameworks as surveyed in document D2.1[2] whether they are aimed at simplifying SGX implementation or at offering common APIs to access both SGX and SEV technologies. A challenge is to remove the optimization task from the users to reach near-native performance. Another challenge is to design TEE use scheme with regulates the security level according to measured real performance impact. As a side note, this solution shall be carefully designed to avoid any tampering of the regulation leading to low security by an attacker.

2.2.2 Future Applications

In view of TEE risks and challenges analysis, we view two possible usages in the telecom industry, protecting a VNF and protecting a VSF.

SEV has undoubtedly some advantages with regards to the workflow and the performance impact (at least when compared to non-optimized SGX implementation). Its downsides are first its ample TCB with apriori-known vulnerabilies. Although the attacker does not view the VM content in cleartext at any time, the TCB is still a vast attack surface where probed vulnerabilities can be exploited. The second drawback is its tight association with virtual machine deployment model which may likely loose ground against containers. Therefore, we rather consider SGX as the TEE model to implement. Although SGX is more demanding in terms of knowledge acquisition, security expertise and performance optimization, it can be leveraged by any payload deployment model. Of course, this investment is worth assuming that the actual host server is equipped with an Intel processor, deemed as a relatively low-risk assumption.

For **virtualized network functions (VNF)** delivering security guaranties through cryptographic primitives (typically to establish end-to-end secure channels as described in our project TC4), the security baseline for its deployment is ETSI NFV-SEC standard. As a reminder, ETSI software security (derived from ETSI NFV-SEC specifications and group research) can be simply defined as: VNF and VSF shall run exclusively on trusted platforms. More, the platform cannot execute untrusted code. As all SCAs are either spawned from a malicious kernel or a sibling process, therefore using trusted kernel and process-whitelisted platforms **halt all SCAs**. There is no formal requirement to leverage SGX for a NFV in ETSI specifications. However, there is no contradiction either and SGX can bring many advantages with its remote attestation and secret provisioning, typically to establish end-to-end

secure channels. In ETSI-specified execution environments, SGX guaranties are fully met as no side channel are workable and they bring **data and code confidentiality, enough to halt all introspection attacks** that could be mounted at any location running NFVs (and which is not covered by ETSI specifications). For cryptographic code in the ETSI environment, the strict requirement to use of hardened primitives leveraging Intel AES-NI hardwired instructions (for memory access pattern obliviousness) may be questioned and challenged as no SCAs can be theoretically launched. However, it is certainly better to adopt the most secure primitives, whatever execution environment and especially if they also bring performance gains.

For **virtual security functions (VSF)** embedding specific security algorithms (to identify attack vectors, refrain DDoS, modify the network structure, …), the situation is quite different. First, such functions are deployed in **a limited number of platforms** where SGX can be more easily leveraged on the workflow point of view. Secondly, contrarily to VNFs, VSFs are far less dependent on open sources and therefore deviate from the legacy profile standardized VNFs may expose to attackers. VSFs have specific semantics and functionalities and are not pre-known to attackers. If the SGX PCL mode is leveraged, the code cannot be analysed (i.e., encrypted outside SGX) and **no more SCAs** can be spawned here too. In fact, the latter assertion relies on the security of the SGX Intel enclaves and the remote attestation mechanism. **For this reason, all Intel mitigations including removal of the hyperthreading mode shall be implemented on the controlled platform.** An attack on the Intel enclaves could (theoretically) reveal the PCL mode AES key to obtain a decrypted and possibly a tampered VSF. Once the VSF runs inside the (safe) enclave, all its decision-taking process is kept confidential and integrated. When a VSF is deployed, Intel remote attestation using the last update of the SDK brings additional security guaranties related to the platform trustiness and the ability to establish a secure channel tied from the vendor and the deployed remote VSF. This secure link enables to modify remotely and covertly the network protection profile according to evolving threat conditions.

We would only recommend that all offered mitigations shall be active and for that the baseline is to follow the basic steps of:

- Leverage TCB recovery-remote attestation mechanism and follow Intel detailed instructions
- Switch off hyperthreading when that is viewed as necessary and possible. Typically, this decision is much easier to take for isolated platform-process VSF than for core NFV which basically are de facto protected against all SCA by applying ETSI specifications. In the latter, removing Hyperthreading can be viewed as a costly decision with an uncertain real benefit.

On both sides (VNF and VSF), these baseline security measures **bring long term immunity** and best defences to future upcoming SCAs.

2.3 Artificial Intelligence

5G and beyond networks will be characterized by diverse technologies (e.g., SDN, NFV) and services, massive number of connected devices, and high traffic volume, resulting in dynamic and complex cyber-threat landscape. Thus, a scalable and timely detection and mitigation of security threats is essential. AI/ML techniques are deemed to play a key role in achieving this goal, thanks to their capability in enabling intelligent, adaptive and autonomous security management[90]. In what follows, we present recent advances in using AI/ML techniques for tackling security issues in next-generation mobile networks, and describe previous projects focusing on 5GPPP. Then, in the next subsection we identify some of the challenges and risks involved. Finally, in the last subsection we provide some insights on how these can be addressed.

Authentication and Authorization

Authentication and authorization services play a key role in enhancing 5G and beyond security by thwarting impersonation attacks and controlling access privileges. To cater to the stringent performance requirements of mMTC and URLCC applications, the emerging authentication and

authorization schemes are increasingly relying on multiple non-cryptographic attributes, associated to users, resources and environment (e.g., time and location). AI/ML techniques are poised as an attractive option to automatically combine these diverse and time-varying attributes to enable authentication and dynamically enforce fine-grained access policies [90]. Moreira et al. [91] built a K-Nearest Neighbors (KNN)-based model to determine the authenticity of mobile terminals in network slices based physical layer information (i.e., Received Signal Strength). The work in [92] proposes a Gaussian Mixture Model (GMM)-based physical layer authentication scheme which leverages the channel state information to detect identity spoofing attacks. In the same vein, the authors in[93] used channel state information to devise a Convolutional Neural Network (CNN)-based multi-user authentication scheme for enhancing edge computing security. Hoang et al. [94] exploited the wireless signal features to build SVM-based models for detecting active eavesdropping attacks. Fang et al. [95] introduced ML-based intelligent authentication approaches by opportunistically leveraging physical layer attributes (e.g., carrier frequency offset, channel impulse response, and receiving signal strength indication) to achieve continuous and situation-aware authentication in 5G and beyond networks. The work in [96] proposes a holistic authentication and authorization approach leveraging online ML and trust management for achieving adaptive access control in a large-scale and dynamic IoT environment. The proposed access control scheme exploits the time-varying features of the transmitter, hardware-related attributes and user behaviours, to refine and update access policies on run-time.

Network Anomaly/Intrusion Detection and Prediction

A timely detection and prediction of anomalous behaviours caused by malicious or accidental actions is vital to meet the stringent reliability and availability requirements of 5G and beyond networks[90]. ETSI ENI (Experiential Network Intelligence) ISG (Industry Specification Group)[97] has identified AI/ML usage as a requirement to recognize abnormal traffic patterns that can lead to service unavailability or security threats in next-generation networks. The use of shallow and deep learning approaches for detecting and forecasting network intrusions has attracted considerable attention[98]. Krayani et al. [98][99] designed a Dynamic Bayesian Network (DBN) model to detect jamming attack in Orthogonal Frequency Division Multiplexing (OFDM)-based cognitive radio networks.

Herrara et al. [100] reviewed the application of ML techniques for SDN security. The authors classified the solutions into two classes: (i) solutions building ML models to identify general anomalies or specific network attacks and (ii) solutions developing IDS frameworks encompassing the whole cycle of detecting and mitigating attacks in SDN.[101]and[102]investigate the potential of Deep Neural Networks (DNN) for detecting intrusion in SDN. The work in [103] proposes a ML-based collaborative DDoS mitigation mechanism in a multi-SDN controller environment. The DDoS attack is detected using a Naïve Bayes classifier fed with network flow features. Narayanadoss et al.[104] used Deep Learning (DL) techniques, particularly ANN, CNN and LSTM, to thwart crossfire attacks; a variant of botnet-based DDoS attack. Siracusano et al. [105] applied ML techniques, namely Decision Tree (DT), KNN and DNN, to detect low-rate DDoS using the features of malicious TCP flows.

The authors in[106] evaluated the efficiency of Apache Spot ML framework in detecting attacks in an SDN/NFV-enabled environment. Three attacks have been considered, namely: (i) data exfiltration attack via DNS (ii) UDP flooding DDoS attack, and (iii) application-layer DDoS attack. Isolation Forest model [107] is used in [108] to identify data exfiltration attack via DNS.

Among the research work and challenges identified by Arjoune and Faruque [109], deep learning techniques can be used to detect and prevent jamming attacks against 5G-based unmanned aerial vehicles (UAVs) and mmWave Massive MIMO. As an example of recently published work, Gupta et al. [110] survey the techniques for protecting drone communications. They consider that the use of cryptographic techniques requires high amounts of computation, and propose a blockchain-based 5G drone communication architecture combined with AI techniques.

The COGNETproject (http://www.cognet.5g-ppp.eu) selected a set of most relevant challenges for 5G intelligent network management and how to solve them based on the application of ML techniques.

It focuses on three areas: Network resource management, service demand prediction and network resilience performance. As part of the latter area, network security and resilience are addressed with different ML techniques. The project uses supervised (e.g., xgboost) and unsupervised (e.g., clustering) learning techniques to detect different types of network attacks such as DoS Sync flood or malware activity. Also, performance degradation detection is identified based on anomaly detection over CPU and network usage by some VNF.

The 5GVINNI project (https://www.5g-vinni.eu/) has a strong involvement in the use of AI/ML techniques to achieve their goal of zero-touch orchestration, operations and management (but not targeting security) for different verticals.

Several other projects rely on artificial intelligence for improving the autonomic management, such as: AI@EDGE (https://aiatedge.eu/) that is building an AI and Edge computing platform for network automation in B5G networks; 5G-CLARITY (https://www.5gclarity.com/) that focuses on private networks (e.g. for manufacturing) based on SDN/NFV managed using AI techniques and intent-based policies; and, ARIADNE (https://www.ict-ariadne.eu/) that is employing AI/ML techniques to manage high-frequency communications and dynamic assignment and reconfiguration of the meta-surfaces to obtain reliable High Bandwidth connections in B5G.

2.3.1 Risks and Challenges

Several issues that are specifically critical when using AI techniques for 5G intrusion detection need to be further explored, such as the robustness of machine learning to adversarial attacks [111]. Many of the research work use public CTU datasets (https://mcfp.felk.cvut.cz/publicDatasets/) that contain real-traffic for training supervised or semi-supervised machine learning algorithms that can be useful for proof-of-concepts but are very often not enough for defining normal behaviour to detect anomalies in operational settings. This limits the effectiveness of the solutions proposed and actually makes them vulnerable by providing information to potential attackers on how to avoid detection.

Sagduyu et al. [111] investigate adversarial attacks on 5G spectrum sharing and network slicing. In the first case, attackers can reduce the throughput of the 5G communications leaving only a small footprint. In the second case, the adversary trains a GAN over the air to generate spoofing signals and transmits them to infiltrate the 5G signal authentication at the gNodeB. A defence technique is proposed that consists of generating controlled errors with limited performance impact to deliberately fool the adversary into training inaccurate models.

Suomalainenet al. [112] explore this topic further. They consider that the use of un-scrutinized data for training can have serious consequences the produced actionable intelligence, and that scrutinizing the data opens privacy challenges. ML are used in many different disciplines with excellent results in small closed environments, but in 5G they can inadvertently open the network to serious security challenges such as unfair use of resources, denial of service, as well as leakage of sensitive information. Among the solutions proposed they advocate improved security awareness of the end-to-end situation using multi-domain data (e.g., based on SIEM, honeypots, CTI and intelligence sharing).

Another major issue that makes intrusion detection difficult to use are the number of false positives that are generated. This is especially true in very dynamic systems like SDN/NFV-based 5G/IoT networks. Automated management of security can help but human intervention is nevertheless very often required. Most of approaches for false alarm reduction are based on data mining or machine learning techniques.

The key role that AI plays in enabling fully autonomous security management capabilities [117] makes AI an attractive target for attackers. In fact, AI systems, particularly ML systems, can be influenced to learn wrong models, make erroneous decisions/predictions, or leak confidential information. The attacks against ML systems are considered *causative* if they target the training phase or *exploratory* if they aim at the inference phase. They can be conducted in a *white-box*, *grey-box* or *black-box* setting, depending on whether the attacker has, respectively, full, partial or no

knowledge about the training data, the learning algorithm and its hyper-parameters. The adversary may perform *indiscriminate attacks* to cause the misclassification of any sample or *targeted attacks* to lead to misclassification of a specific sample. By attacking a ML system, the adversary may decide to break its *integrity* by evading detection without affecting normal behaviour of the system; its *availability* by deteriorating the system usability; or its *privacy* by gaining sensitive information about the training data, the ML system or its users. In INSPIRE-5Gplus, we conducted a thorough investigation of the security risks that may come along with the envisioned AI's benefits if their vulnerabilities are leveraged by malicious actors. In view of increasing the resilience to AI threats, we advocated several defence measures while advising on which components of the ML5G unified architecture they could be enforced. In what follows, we summarize the main outcomes of conducted study [90].

Potential Attacks against ML Systems

- Poisoning Attacks

In poisoning attacks, also referred to as causative attacks, an attacker aims at influencing the learning outcome to his advantage by tampering with data or the learning algorithm at training phase. The appeal of this attack stems from the constant retraining requirement of a learning model to account for the new data distribution, giving the attackers the opportunity to poison the trained model. The poisoning attack can be mounted using different strategies: data injection, data manipulation, and logic corruption.

- Data Injection Attacks

This strategy is used when the attacker has no access to the training data. It aims at altering the data distribution by feeding carefully crafted malicious samples into the training dataset while keeping original samples unchanged.

- Data Manipulation Attacks

The attacker is assumed to have a full access to the training data, allowing them to directly contaminate the original data used for training the learning model. The contamination can be performed by either flipping labels (e.g., benign to malicious and vice-versa) or introducing small perturbations on input features.

- Logic Corruption

The attacker focuses on interfering with the learning algorithm or its learning logic. This strategy can be used against models that leverage distributed learning (e.g., federated learning), which relies on several agents for training. Thus, a malicious agent may manipulate the local model parameters to compromise the global model.

- Evasion Attacks

An evasion attack targets the inference stage. Unlike poisoning attacks, these attacks require no influence over the training process. The attacker seeks to escape the learned model at test time by introducing small perturbations to the input instances. Such perturbations are called adversarial examples.

- Model's API-Based Attacks

The emergence of the ML-as-a-Service (MLaaS) paradigm makes ML models susceptible to new attacks, namely: model inversion attack, model extraction attack, and membership inference attack. The model inversion attack aims to recover the training data by leveraging the outputs of the targeted ML model. Meanwhile, the model extraction attack focuses on revealing the model's architecture and parameters to reproduce a (near)-equivalent ML model, by observing the model's predictions and/ or execution time. The purpose of a membership inference attack is to determine whether a sample has been used to train the target ML model, by exploiting the model's output.

Finally, the widespread use of encryption makes detection techniques, such as DPI, practically

useless. Encryption limits the meta-data that can be extracted from the network traffic and even makes it easier for attack techniques to evade detection, e.g., bots communicating with Command-and-Control servers and exfiltrating sensitive data. Behaviour-based analytics and Cyber Threat Intelligence can help identify respectively suspicious network behaviour and network traffic involving non trustworthy devices, IPs and hosts.

2.3.2 Future Applications

Here we provide some insights of how the risks and challenges from the previous subsection can be faced: hybrid techniques to improve the accuracy of the cyber-threat detection; defence mechanisms against adversarial ML and evasions; and techniques such as Moving Target Defence to improve the system's resiliency.

Hybrid machine learning

One of the main challenges related to machine learning techniques for intrusion detection is that no single classification technique is capable of detecting all classes of attacks with acceptable false positive rates, accuracy and performance. Many different works, both done by academic and industrial research have shown that a single machine learning technique is not enough to obtain efficient and accurate results. They might detect specific attacks (e.g., detecting unusual trends that can correspond to DDoS attacks) or perform specific tasks that are needed (e.g., classifying encrypted traffic) but do not provide a complete and effective intrusion detection system. Notably, zero-day attacks are not well detected by supervised machine learning since they are trained using datasets that do not contain these attacks. Detecting deviations from normal behaviour works but will generate too many false positives if the system that needs to be protective is dynamic, as in the case here, with the behaviour that often changes. Even if an unsupervised technique is used, it will also tend to detect many false positives or true negatives. Furthermore, practically all machine learning techniques take time and require much computation resources.

To address these issues, we need to consider (as discussed in 2009 by [113] and recommended for instance by [114][115][116]) combining different machine learning techniques, such as hybrid or ensemble techniques that act as classifiers, which are used to classify or recognize whether the network traffic and business activity is normal or corresponds to an attack.

A hybrid classifier should combine or cascade several machine learning techniques so that the system performance and the accuracy of the detections is improved. A first classifier can take the raw data and prepare it for the next classifier that will improve its efficiency. This first classifier can, for instance, pre-process the input training samples, or the data to be analysed, to eliminate redundant or superfluous data (e.g., using techniques such as exploratory data analysis, principal component analysis and feature selection). This first classifier can also divide the data into sessions that can be considered free of attacks (e.g., corresponding to behaviour that is common and with no anomalies) and those that need to be further explored (e.g., corresponding to behaviour that is not considered common or that contains some anomaly). The following classifiers can implement different supervised and unsupervised techniques for optimising the decision making and the predictive modelling.

Ensemble classifiers would allow improving the classification performance of one classifier by combining several different simplified learning algorithms or learners so that the process can be optimised or even parallelised. The final result can be based on what the majority of the classifiers provide as result or by applying other machine learning techniques such as boosting (e.g. reducing bias and variance) or bagging (e.g. bootstrap aggregating).

Defence mechanisms to tackle attacks against ML

Attacks on ML can be leveraged to undermine the security of 5G and Beyond networks. For instance, the poisoning of spectrum data can be used to cause channel jamming in cognitive radio networks; adversarial identity spoofing can be performed against an ML-based authentication model; and, ML-

based network anomaly detection module can be evaded [90].

In what follows we describe some potential defence mechanisms that could be adopted to foster confidence in AI systems, and highlighting their limitations and adoption challenges:

1. Adversarial Machine Learning

Adversarial Machine Learning (AML)[118] aims at improving the robustness of ML techniques to adversarial attacks by assessing their vulnerabilities and devising appropriate defence measures, as for example:

- Defences against Poisoning Attacks

Several countermeasures have been proposed against poisoning attacks, which can be broadly categorized into *input validation* and *robust learning*. ***Input validation*** seeks to sanitize the (re)training data from malicious and abnormal samples before feeding it into the ML model. Outlier detection is a common defensive technique used to identify and remove suspicious samples from the training dataset. However, this technique can be bypassed by crafting poisoned samples that can mislead the learning process while remaining within the genuine data distribution. The Reject On Negative Impact (RONI) approach sanitizes data by removing samples that have a detrimental impact on the learning performance. The micromodels strategy performs data cleaning by first generating multiple micro-models trained on a disjoint subset of input samples. The micro-models are then combined in a majority voting scheme to eliminate the anomalous training data subsets. Clustering-based techniques have been used to mitigate the label flipping attack. These techniques consist in dividing the training data into clusters, where the samples within the same cluster are relabelled using the most common label in this cluster. Unlike input validation, ***robust learning*** aims at developing learning algorithms that are robust to training data contamination by leveraging robust statistics techniques [119].

- Defences against Evasion Attacks

A variety of defensive strategies have emerged for defeating evasion attacks, including adversarial training, defensive distillation, ensemble methods, defence Generative Adversarial Networks (GANs), and adversarial concept drift handling techniques. In **adversarial training**, the resilience to evasion attacks is achieved by training the model on a dataset augmented with adversarial examples. **Defensive distillation** is a training strategy that uses the knowledge inferred from a ML model to strengthen its own robustness to adversarial examples. Both adversarial training and defensive distillation implicitly perform gradient masking, which consists in making the model's gradient useless by, for instance, setting it to zero or changing its direction. Indeed, the absence of the real gradient complicates the generation of adversarial examples, allowing the model to exhibit improved robustness. However, this does not prevent that the model may remain vulnerable to adversarial samples crafted using transferability-based black-box attacks. Moreover, it is worth mentioning that the improved robustness brought by adversarial training and defensive distillation comes at the price of a decreased accuracy on clean data. Ensemble methods combine multiple models to build a robust model. **Ensemble methods** have the virtue of improving the model's robustness while increasing its accuracy on clean samples. Nevertheless, the merit of ensemble methods comes at the expense of increased model complexity and computational cost. **Defence GANs** aim to denoise input samples from adversarial perturbations by projecting them on to the range of the GAN's generator before feeding them into the ML model. In other words, they aim to find the closest sample to the adversarial example that the GAN's generator is capable of producing and feed that as an input to the ML model. As the GAN's generator is trained to learn the distribution of the real data, the generated sample will be cleaned from added perturbations. Defence GANs have proven their effectiveness to counter both white-box and black-box attacks. The adversarial perturbations introduced to data result in concept drift; that is, the change in data distribution leading to drop in the ML model performance. Thus, **adversarial concept drift handling techniques**, such as ensemble learning, can be used to face down adversarial attacks by retraining the ML model once a drop in its performance is detected. For instance, an ensemble learning approach tracks the adversarial concept

drift by measuring the prediction disagreement between the ensemble models. In fact, an abrupt increase in the prediction disagreement is an indicator of concept drift that will trigger the retraining of the ensemble models on the new data.

- Defences against the model's API-based Attacks

To mitigate ML API-based attacks, various solutions have been proposed, including:

  - *Learning with differential privacy* (DP) to prevent the disclosure of training data by making the model prediction independent of an individual input. A differentially private ML model guarantees that its behaviour hardly changes when an individual sample is added to or removed from the training dataset. Thus, by looking at the model's output, an adversary cannot ascertain whether an individual input was included in the training dataset or not. To achieve DP, a small, con- trolled noise is added to the model during its training.
  - The use of *homomorphic encryption* which enables model training over encrypted data, thus guaranteeing data privacy. It is worth noting that the major challenge in using this countermeasure is the induced computational complexity.
  - The limitation of sensitive information provided by ML APIs by releasing only class labels, filtering out the prediction probabilities of low-probability classes, and rounding the class probabilities. In fact, the danger of revealing the prediction probabilities by the inference API stems from the fact that those probabilities are calculated as a function of the input and the ML model's parameters. Thus, collecting a sufficient number of prediction probabilities and their corresponding inputs, an adversary can easily extract the model's parameters by solving a system of equations where variables are the unknown model's parameters. By hiding the prediction probabilities, revealing only part of them and/or rounding them to a fixed number of decimal places, the adversary is defeated from achieving the goal of building a surrogate model approximating the real one.
  - The addition of noise to the execution time of the ML model.

2. Moving Target Defence

Given its potential in increasing the attacker's uncertainty, MTD has recently emerged as an effective paradigm in addressing the security concerns of AI, specifically ML techniques. In cur- rent practice, a ML model remains static over a long period of time once deployed, which gives the attacker the advantage of time to devise effective adversarial attacks. Thus, introducing dynamicity in a ML system by constantly changing, for instance, the ML algorithm, the features used for training, the model's parameters, helps to improve its robustness. In this vein Song et al.[120] proposed a MTD strategy that dynamically generates new models by retraining independently perturbed versions of the base model after its deployment. To leverage the promising MTD capabilities for thwarting adversarial attacks, a major challenge is to come up with MTD strategies that make the ML model robust without sacrificing its performance and with reduced moving cost. Hence, further research efforts are required in this direction.

2.4 Advanced CyberSecurity Techniques

5G and beyond networks promise a converged ICT infrastructure and thus plan to support challenging use cases such as smart healthcare, autonomous vehicles, Industry 5.0, and extreme-scale connectivity in a secure and trustworthy way. Although disruptive concepts such as full network softwarization and smart networks are adopted, the requirements for advanced digital services necessitate advanced cybersecurity techniques (ACT) which can monitor, protect and defend such systems. These techniques rely on situation awareness, agility and threat intelligence, i.e., a cognitive network management approach. Therefore, CTI sharing, optimized network monitoring for security

and Moving Target Defence (MTD) are important elements in ACT.

Novel technologies being integrated into 5G and future networks such as AI/ML-driven management, programmability, MEC [121] and massive-scale IoT lead to new vulnerabilities and security issues. These phenomena are becoming even more important with the traffic surge and diversity in 5G and beyond systems, and new critical applications served by the network. The sharing of CTI and its automated use are crucial to prevent and efficiently mitigate such threats. However, these CTI, monitoring and MTD techniques need to be examined and adapted considering the requirements and architecture of 5G and beyond networks. To cope with the challenges of developing and deploying ubiquitous monitoring, optimizing the resource usage is a key requirement. This is also valid for CTI and threat sharing techniques. CTI functions have two main aspects: CTI gathering and CTI sharing. Both of these functions have to be optimized. Moreover, optimizing deployment and delivery of ACT is important, which is driven by network softwarization, and also depends on location awareness, content adaptation and caching.

Cyber Threat Intelligence (CTI) and threat data sharing: The sharing of CTI and its automated utilization of it are crucial to prevent and better respond to current and emerging security threats and incidents. When looking at the cybersecurity and cyberterrorism landscape, one can easily recognize a strong and continuous evolution at every level, from the vulnerabilities and the attack surface to attack techniques and tools, as well as the number and type of attackers and their motivations. This situation affects 5G networks and beyond and increases the need for solutions able to rapidly adapt to changing the threat environment and recognize cyberthreats and cyber-actors, emphasizing the strategic role of Cyber Threat Intelligence (CTI). Many solutions and services have been provided that vary in scope. On one hand, there are threat exchange specifications that enable CTI to be shared among interested parties[123], such as: OpenTAXII[124], an open-source implementation of TAXII, a specification for CTI message exchange; Collective intelligence frameworks (CIF) [125] for integrating and collating CTI feeds from multiple sources; and, OpenTPX[126], specification and tools for sharing CTI data. On the other hand, there are complete CTI platforms including data collection, correlation, analysis and visualisation, often involving hardware installation and typically labelled as an SIEM solutions. Some of the most popular CTI solutions are: YETI[127], a platform for integrating CTI indicators and events into a single database; GOSINT[128], a framework for integrating and collating CTI indicators; MISP[129], a full-featured CTI platform for collecting, correlating, storing and sharing indicators, feeds, binaries and more; and, AlienVault OSSIM[130] (now owned by AT&T and called AT&T Cybersecurity), a full-featured CTI and SIEM platform for attack detection, vulnerability correlation, monitoring, and extensive visualisation features.

All of these platforms are designed to be open and generic in order to ease the integration with other third-party feeds and services. In some cases, they address security in IoT[122] and mobile networks using for instance specialised honeypots, but dealing with 5G and beyond specific network threats remain a gap that needs to be filled. In INSPIRE-5Gplus, the CTI framework serves for collecting and aggregating data from different sources (Honeypots, Darknets, OSINT, commercial data), and analysing it to obtain threat intelligence that can be used for preventing attacks on one's network. It will integrate the analysis of network wide routing anomaly detection and 5G attack intelligence in different domains and levels. The goal is to offer a unique online service that covers data collection, visualisation and automated support for incident response.

Moving Target Defence (MTD) techniques: Moving Target Defence (MTD) is the technique of changing properties and configuration of an ICT environment, such as the topology and the address space layout, by potentially modifying instruction sets, IP addresses, port numbers, proxies, virtual machines, operating systems, software programs, protocols and packet headers resident in a network. The MTD enablement can be interacting with different 5G components such as Slice Manager and network security management system in order to implement the security policy and perform the mitigation actions conformingly. It may employ a cognitive system that dynamically determines what to move, where to move and how to move, based on the received input and on the action costs, in order to perform an optimal mitigation action. To this end, Machine Learning (ML)

will enable MTD intelligence on how to evaluate the cost of the different actions, based on the actual state of the network and on the gravity of the threat. To orient the MTD towards the optimal policy, for instance, one can consider the usage of a Deep Reinforcement Learning algorithm, which will allow the system to continuously optimize its actions and adapt to changes of the attacker's strategies and the network's advancement. Accordingly, RL can be used to train the cognitive models for different components, like the MTD decision making, which will use a tuned learning algorithm.

Security Monitoring Optimisation: In virtualized infrastructure environments characterized by dynamic topologies, e.g., vehicular communication, the addition or removal of a network element (software or hardware) may introduce new attack vectors causing the violation of network integrity. Security monitoring should thus focus on the timely detection of security policy violations and abnormal behaviours in data traces from multiple virtualized and non-virtualized resources and deployed services. In this context, techniques, such as monitoring changes of technical identity, statistical deviations in resource usage, network volatility spreading, complex event processing and graph-based vulnerability analysis, are of particular importance.

Another possible approach to monitor and mitigate security incidents in such virtualized systems lies in the exploitation of ML/AI techniques able to control security service function chains. A challenge here is that fast parameter changes, due to frequent topology changes for example, introduce the problem of transients, requiring the ML/AI module to predict only the short-term state evolution of the system as well as the actions the ML/AI module itself submits to the system. An additional challenge refers to the management of different monitoring ML/AI modules, since a conventional "divide-and-conquer" approach, although breaking down the problem into many sub-problems of manageable complexity, would prove ineffective for ML/AI monitoring entities dealing with different learning objectives. A promising way to circumvent these challenges is resorting to reinforcement learning techniques, as the main functional framework for ML/AI, which provide the necessary capabilities to deal with transients; however, it remains challenging to deploy such modules in fragmented SDN/NFV environments [131].

Predictive analytics empowered by ML/AI techniques offer an additional security monitoring option for the proactive identification of threats by leveraging on data logs that are available from multiple sources. As security threats continue to rise rapidly, it is essential to forecast attacks proactively rather than reacting after they occur; therefore, monitoring functions can greatly benefit from predictive analytics to proactively identify impending security threats ahead of time before any serious effects occur [132]. In this context, the exploitation of spatiotemporal cross-correlations among ambient measurement trajectories holds the promise of extracting the underlying dynamics which govern data behaviour in an effort to detect abnormal and misbehavioural patterns. Dynamical systems, capable of exploiting spatiotemporal correlations among data streams [133], can be utilized in an iterative strategy for extracting contextual monitoring information and regaining perspective on the mechanisms that causally induce vulnerabilities, e.g., in false data injection scenarios.

In addition to works in the technical literature and academia, there have been various efforts in the past as part of international research projects which can have an impact on INSPIRE-5Gplus work. Here, we provide a concise summary of the most relevant ones for the ACT enablement:

- **5GENESIS (https://5genesis.eu/):** The objective of 5GENESIS is the validation of 5G KPIs for various use cases, in controlled setups and large-scale events. 5GENESIS includes 5G facilities in distributed sites across Europe, capable of enabling well-articulated, open and flexible experimentation frameworks. The experimentation framework provides a Security Analytics Framework that ingests the network telemetry from the RAN, Core, Transport and Cloud domains, enabling security AI/ML models to detect anomalies that could potentially affect the network's performance. This effort is important for the MTD implementation and monitoring and detection capabilities to be developed as ACT in INSPIRE-5Gplus.
- **5G VINNI (https://www.5g-vinni.eu/):** As a security asset, the network telemetry framework designed to cope with 5G KPI measurements in 5G VINNI project may be utilized to enable

security AI/ML models via collected data.

- **5G-CARMEN (https://5gcarmen.eu/)**: To address MEC related challenges in CCAM, 5G-CARMEN developed an Intrusion Detection and Classification module (IDCM) based on novel approaches in intrusion detection leverage pattern-based recognition of signals with Machine Learning (ML) techniques to improve runtime performance and resources. ML models are used to improve the efficiency of processing without increasing the latency of the system. The IDCM can reduce the attack surface of the CCAM, especially in the resource-constrained MEC environment. It makes use of machine learning technologies to determine the likelihood that an edge system component has been compromised. It supports low-computational analysis and machine learning techniques for resource-constrained devices common in MEC environments. The IDCM can detect novel and known attacks based on threat indicators elicited from its network probes. For example, it can detect Denial of Service attacks against specific components of the edge system, malware compromise, and specific APIs, or malicious use.

2.4.1 Risks and Challenges

There can be several risks or issues when advanced cybersecurity techniques (ACT) are deployed in 5G and Beyond systems. First of all, ACT go hand in hand with automation and autonomous security management. Therefore, several issues listed in “Automation & ZSM” and “AI” subsections such as adversarial AI are also applicable for ACT development and adoption in future networks. These **threats on automation and cognitive security management** are especially relevant for cases where minimal human-in-the-loop is targeted and minimal time-to-decide and time-to-respond objectives are pursued, e.g., automated threat data sharing. This aspect may limit the efficiency of the proposed solutions and even make them vulnerable as an attack point for nefarious agents. Moreover, monitoring overhead is another aspect to be carefully elaborated for performance and availability objectives. The data collection and processing can lead to performance issues harming availability and service quality requirements for the protected digital services. That issue is more apparent in large-scale systems like Beyond 5G systems where a ubiquitous ICT infrastructure with Internet of Everything (IoE) will enable various advanced and critical services. Therefore, **monitoring overhead potentially compromising availability** is another risk to be considered.

The ACT for monitoring, threat sharing and MTD envisaged in ACT enablement may also lead to **API vulnerabilities** since CTI and monitoring systems are designed as open systems for evolution and integration capabilities with external data feeds. The external facing integration risks also stem from **trust (or lack of trust) in CTI and collected monitoring data**. Those data streams are security assets on their own in addition to being feeds to more advanced security functions, e.g., MTD. Malicious activity can target to inject forged or fake threat and monitoring data to manipulate and mislead ACT functions. An important risk in that regard is **lack of visibility and explainability** for ACT operation (regarding operation of security controls as well as how security data are collected) when interpretation capability is needed to MTD can also be another point for attack if visibility and explainability are not maintained. The MTD actions may not be closely monitored and inefficient or invalid actions can be performed by the system wasting system resource without any gain in security and protection of network resources.

In addition to risks, the ACT utilization in the INSPIRE-5Gplus project context and also prospective 5G/B5G environment also face some major challenges as summarized below:

- **The autonomic operation and intelligence-related security challenges:** In the INSPIRE-5Gplus project, one of the main challenges related to ACT is that risks on automation have to be addressed as in the context of different ACT enablers. That is a wide-ranging challenge, also affecting other enablements in the project. For that purpose, best practices and robust AI/ML models will be adopted from the available body of work on computational intelligence. Please note that although intelligence-driven security can be a challenge, smart control and analytics for enhanced security operations can also provide more accurate

detections and mitigation.

- **Overhead minimization:** For ACT, overhead and performance penalty on the core services needs to be analysed from the security gain – overhead trade-off. This is due to the phenomenon that 5G will pave the way to Internet of Everything (IoE), producing a vast amount of data and service processing at different points in the network. However, ACT such as ubiquitous security monitoring or widely-applicable MTD may require a very big amount of computation, communication and storage resources. Therefore, a key challenge for ACT in practical systems is overhead minimization. For that purpose, efficiency-oriented approaches such as CTI feature reduction and optimized monitoring techniques will be investigated. Moreover, the specific requirements will be considered while deploying and controlling any ACT in a specific case (e.g., an autonomous vehicle-oriented use case could be more sensitive to communication overhead while resource-constraint IoT scenarios are challenged due to processing overhead in the first place.)
- **How to integrate ACT to different environments:** The ACT functions in the INSPIRE-5Gplus project have to be designed in an extensible and easy-to-integrate manner to be applicable in heterogeneous 5G and beyond environments. This challenge is essentially valid for any ACT enabler. For that purpose, INSPIRE-5Gplus will use OpenAPI approach and the shared integration fabric capabilities for integration and communication functions. Moreover, new technologies, e.g., SDN/NFV, and anything-as-a-service allow reducing the time and cost in deployment and delivery significantly in different environments. As new features are added or bugs are identified, new releases can be quickly on-boarded, tested again and deployed through a continuous integration/continuous deployment (CI/CD) chain.
- **The correct selection of security KPIs and their implementation:** The advanced cybersecurity monitoring and security actions should be driven by the appropriate security KPIs and their correct measurement. Therefore, it is important to determine the right set of KPIs to have efficient security functions. Thus, ACT in our project need to investigate and design the KPIs to measure/monitor the security as well as drive the security functions. However, this is not a trivial task considering the diversity of networked systems, requirements of different ACT, and characteristics of various use cases. This aspect is also linked to the overhead challenge described above and the test cases being developed in WP5 work.

2.4.2 Future Applications

The ACT in 5G (and also in prospective Beyond 5G systems such as 6G) will be integrated at different layers and for different security applications. Some envisaged applications for this enablement are:

- *Protection of verticals in 5G*: CTI and threat data sharing can be integrated with security monitoring among different service users in a 5G vertical. This is especially relevant since verticals have specific QoS and security requirements which need to monitored and maintained. CTI is also a general capability which can serve various cyber-attack detection and defence mechanisms by facilitating data sharing among different parties in connected systems. This also improves situation awareness against security attacks for different service consumers in a vertical since attacks usually propagate through different vertical elements exploiting common vulnerabilities in these systems.
- *Slice based service and resource protection*: For 5G security, MTD techniques can be integrated into slice protection focusing on MEC environments. This is an important application of MTD of 5G security since network slices are used to provide a wide range of services with specific QoS KPIs, e.g., a slice serving autonomous cars. Moreover, CTI is a potential input for MTD, allowing it to run efficiently in terms of what, when and how will be changed for creating a moving target.
- *Large-scale monitoring in heterogeneous networks for security:* Threat data sharing and CTI

intelligence can enable large-scale security monitoring in heterogeneous networks. This application of ACT enablement is beneficial since 5G networks are essentially an integral part of the Internet unlike previous generations with pervasive use of concepts such as IP networking, cloud computing and web technologies.

- *ML/AI-optimized software-defined security monitoring:* Security monitoring and mitigation of security incidents in software-defined systems is an important application for security monitoring optimization in 5G. In that regard, ML/AI techniques can control security service function chains in software-defined security. That is important since 5G systems are large-scale networks with practical scalability and efficiency concerns for network and security management.

2.5 Distributed Ledger Technologies

In a nutshell, Distributed Ledger Technologies (DLTs) are decentralized databases that rely on independent computers to record, share, and synchronize digital transactions. Blockchain is an example of DLT that enables users to interact and transact (store and retrieve data) with ensured data authenticity, immutability, and non-repudiation. The distributed nature of Blockchain allows the industrial entities and various 5G/IoT devices to exchange data, to and from their peers, eliminating the centralized operational requirement. The Blockchain-assisted 5G ecosystem can establish accountability, data provenance, and non-repudiation for every user. The first block in a blockchain is referred to as the genesis block, which does not contain any transaction. Each block thereafter contains a number of validated transactions and is cryptographically linked with the previous block in a chronological order (See Figure 4).

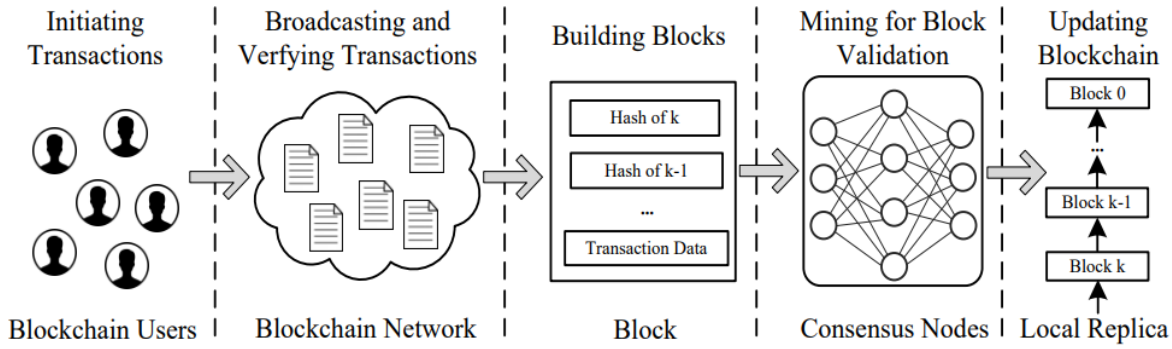


Figure 4 - An overview of the Blockchain workflow

Platform	Description	Ledger type	Consensus Protocol
Ethereum	The world's first smart contract platform which operates with public collaboration.	Private/ Public	PoW
Hyperledger Fabric	A private and enterprise blockchain platform innovated by the collaboration of IBM and Linux foundation.	Private	Pluggable
Corda	A privacy preserving blockchain platform which supports to deploy legally enforceable contracts	Private	Raft
NEM	A blockchain based cryptocurrency platform with value added features such as timestamping digital	Public	Proof of Importance

	assets		
Stellar	A blockchain platform which enables cross border financial transactions	Public	Stellar
Waves	An open source blockchain platform which enables user defined cryptocurrency	Public	Leased PoS

Table 2 - Overview of blockchain platforms

The role of blockchain as a security enabler is vital with a lot of potential capabilities. Especially when the primary aspects of the security are considered (including integrity and authentication), the entire concept of blockchain evolved based on storing cryptographically integrity verified transactions in an immutable manner. The decentralized operation eliminates the single point of failure and ensures the service availability. Incorporation of smart contracts ensures the decentralized and accurate execution of a program. These features open up a wide array of opportunities to utilize blockchain as a security enabler. Following are some key ICT projects where DLT is taken as an enablement.

MonB5G project (https://www.monb5g.eu/) brings NSBchain [134]. This proposes a novel network slicing brokering (NSB) solution, which leverages on the widely adopted Blockchain technology to address the new business models needs beyond traditional network sharing agreements. NSBchain defines a new entity, the Intermediate Broker (IB), which enables Infrastructure Providers (InPs) to allocate network resources to IBs through smart contracts and IBs to assign and re-distribute their resources among tenants in a secure, automated and scalable manner.

5GTANGO project (https://www.5gtango.eu/) enables the flexible programmability of 5G networks with: a) an NFV-enabled Service Development Kit (SDK); b) a Store platform with advanced validation and verification mechanisms for VNFs/Network Services qualification (including 3rd party contributions); and, c) a modular Service Platform with an innovative orchestrator in order to bridge the gap between business needs and network operational management systems. This service platform is called SONATA and is accessible via Virtual Infrastructure Managers (VIMs), abstracting from the actual hardware and software. The project introduces the NFV marketplace [135] in terms of interacting software components and entities. This can be integrated into SONATA orchestration platform to manage deployed VNFs. Three main blocks: (a) the dPortal, (b) the NFV Marketplace and (c) the blockchain-enabled Validation System.

5Growth (http://5growth.eu/) is an EU H2020 project with the goal of providing automated deployment and orchestration of customized slices with fulfilled requirements for specific vertical industries (eg, Industry 4.0, Transportation and Energy, etc.). The project has introduced 5Growth Architecture: Federation using Blockchain where the idea is to use a permissioned blockchain where each of the administrative domains runs a single node as part of the permissioned blockchain network. A single generic Federation Smart Contract (SC) is installed on the blockchain to act as a distributed authority. The federation using blockchain provides high level of security and trust. Each AD running a single node is running the same instance of the Federation SC and each line of code is executed at the same time in all nodes involved in the permissioned blockchain network. This adds significant security and trust among the participants.

2.5.1 Risks and Challenge

Some challenges ahead for the efficient integration of DLT, especially with AI/ML, are pointed out as follows:

- Regarding privacy, permissioned blockchain ledgers can ensure data privacy by enabling encryption and allowing controlled access of the ledgers. However, this will limit the access and exposure of the large amount of data that can be necessary for AI to process and preform accurate and correct decision making and analytics.

- The execution outcomes of smart contracts are generally deterministic[139]. This can pose a key challenge for decentralized AI in which AI and machine learning-based decision making algorithms get executed as smart contracts by the mining nodes, in which the execution outcome are not usually deterministic, but rather random, unpredictable and most often approximate. This entails a novel solution to deal with approximate computation and to devise consensus protocols for mining nodes to agree on results with a particular degree of certainty, accuracy, or precision, and with data input that might be highly fluctuating as that of IoT and sensory readings.
- It is envisaged that future quantum computing will have the ability to break public key encryption in which private keys can be determined. Current blockchain relies on digital signatures which use public key encryption. Many experts believe that quantum computing may render the underlying security of blockchain breakable by the year 2027 [140]. This entails serious research on quantum-resistant and secure blockchain that withstand such breakability, and still guarantees high performance and scalability [136].
- Fog computing is a paradigm that allows for localized processing capacity and storage close to the source of data being generated by customers, i.e. IoT devices [136]. In the context of AI and blockchain, future fog nodes have to be equipped with AI and machine learning capabilities as well as enabled with a blockchain interface, whereby localized management, access, and control of data are performed by the fog nodes.
- There is a lack of Standards, Interoperability, and Regulations as blockchain technology standards are yet to be devised. Work is in progress by IEEE, NIST, ITU, and many organization to put forward standards for blockchain interoperability, governance, integration, and architecture [141] Moreover, at local and global level, governmental and institutional guidelines, rules, laws, regulations, and policies need to put in place for blockchain deployment. In the context of AI applications and especially for public blockchain transactions, policies should be carefully defined to assure the ethical rights of the communities.

2.5.2 Future Applications

Blockchain and AI are two technologies that can work together in order to create a more robust framework for future digital innovations in future applications.

On one hand, blockchain suffers from weaknesses such as security, scalability, and efficiency. On the other, AI has its fair share of issues with trustworthiness, explainability, and privacy [137][138]. Blockchain can power decentralized marketplaces and coordination platforms for various components of AI, including data, algorithms, and computing power. These will foster the innovation and adoption of AI to an unprecedented level. Blockchain will also help AI's decisions be more transparent, explainable, and trustworthy. On the other hand, the design and operation of a blockchain involves thousands of parameters and trade-offs between security, performance, decentralization, and many others. Specially, blockchain and smart contracts may face the envisaged massive connectivity demand in future. The decentralized nature and the integration convenience of edge and fog computing nodes will improve the service strengths in those networks. AI can ease those decisions and automate and optimize blockchain for higher performance and better governance.

Some potentials of DLT for Beyond 5G networks/6G are pointed out as follows [142]:

- Blockchain-based solutions can allow for intelligent resource management [143]. The network resource management is challenging in the envisaged massive connectivity demands in the future telecommunication ecosystems. The resource management operations such as spectrum sharing, orchestration and decentralized computation [144][145] requires to be compatible with massively-large infrastructure.

- Application of data privacy is diverse in the complex security requirements in the future 6G network ecosystem. Blockchain can find different applications such as UAV communications and data handling for AI/ML algorithms for providing privacy in 6G networks.
- Blockchains can provide data integrity for applications where a massive data volume is generated.
- Service availability is a significant requirement in the next generation of communication ecosystems, especially with the broader threat surface and massive connectivity in the 5G ecosystem, the risk for DDoS attacks is comparably higher. Effective prevention mechanisms can be formulated with blockchain support.
- The accountability of the 5G and beyond network ecosystem is a key requirement. Being accountable indicates the responsibility for a certain action and its outcomes. For that blockchain can be used for identifying, monitoring and evaluation of 5G and beyond network services. The distributed ledger remains as an immutable and transparent log for each event which can be utilized in the auditing of events.

2.6 Dynamic Liability and Root Cause Analysis

Dynamic liability and RCA are relatively seldom investigated in the literature as an integral part of security management for 5G networks. The current work on this enablement is mostly related to general ICT systems or simply to the business aspects of network operation (especially, liability). However, liability is not a stand-alone concept but an interdisciplinary one closely linked to risk, commitments, responsibility and technical enablers such as trustworthiness, risk, reputation and root cause identification.

Dynamic liability mechanisms for multi-tenant environments: Liability is a multifaceted conceptualization with a large set of associated concepts and terminology from the perspectives of different domains such as Artificial Intelligence, construction contracts, Access Control, software development, trust modeling or insurance [147]. For instance, trust and reputation are key concepts to build a Trust and Reputation Model (TRM), whose goal is to distribute trust and reputation to assess the associated risk in engaging in an interaction between two entities (trustor and trustee). This risk is generally based on the experience perceived by the trustor from past interactions with the trustee.

Usually security management systems in 5G only consider security, trust or performance while not focusing on liability and accountability. However, there are some works in the literature which can be linked to liability challenge, especially in multi-tenant environments. In that regard, one example is[148], where an Information System Security Risk Management meta-model including responsibility, accountability and commitment was used to create a multiagent system-based architecture for broadcasting forecasts and alerts in a power distribution infrastructure. In [149], an adaptation of this model was proposed for a decision mechanism for incident reaction in telecommunications network but it is not adapted for the 5G Slicing context. A Security Panel was proposed in [150] as a platform regrouping risk managers and experts throughout the eSIM ecosystem and allowing them to collect the information required for their risks analysis.

Giaretta et.al propose to use Security-by-Contract paradigm for fog-based IoT management [151]. The decision to add an IoT device in the local network, update or monitor it is taken by matching the IoT device's manifest with a security policy. Costa et. al. [152]show that Security-by-Contract paradigm can be extended to include models and KPIs for quantitative trust management. However, responsibilities are implicit.

Smart contracts, Proof of Transit and TLA compliance schemes for liability:

Smart Contracts: A Smart Contract is a program stored inside a blockchain, which offers certain predefined business logic. When that code is invoked (addressing a transaction to it), the Smart

Contract executes its code and saves the result of the operation inside the blockchain itself. In this way, both the operation performed (including the input data) and the result obtained is stored. Thus, since certain events can be recorded in a non-repudiable way (as every result is contained inside the blockchain), it is easy to trace the events, thereby ensuring liability. That means that when an incident occurs, it will be easy to find the entity (or entities) responsible for the event. Furthermore, due to the inner nature of a Smart Contract (an evolution of a traditional contract), it is trivial to ensure some requirement has been met (or has not), as we can check the result of the execution of the Smart Contract.

Proof of Transit: Proof of transit (https://tools.ietf.org/html/draft-ietf-sfc-proof-of-transit-08) is a mechanism to securely prove that traffic transited one specific defined path. Several technologies such as traffic engineering, service function chaining, or policy based routing, are used to steer and secure traffic through a specific, user-defined path. One of the proposed techniques for that is "In-situ" OAM that allow to record OAM and telemetry information within the data packet while the data packet traverses a network. Proof of transit measurement can be integrated in the in-situ OAM, so in case of manipulation of the data path to avoid specific nodes, the verification will fail, and the node can discard the packet.

TLA Compliance: The main purpose of TLAs (Trust Level Agreement) is to define a required Trust Level between different entities, to ease the interaction between parties. In this way, both agree on a minimum level of "trust" that they commit to fulfilling, as well as the responsibility of each of them in case of TLA violation. These TLAs are defined within a Smart Contract, so for every invocation of the Smart Contract, the TLAs are checked to ensure compliance. In case of violation, it is easy to check how the TLA has been breached and what is the responsibility of the faulty entity.

Root Cause Analysis (RCA): Root Cause Analysis (RCA) is a systematic process for identifying root causes of problems or events, here concerning security breaches, and an approach for responding to them. RCA is based on the idea that effective management requires more than merely putting out fires when problems are detected, but also finding ways to correct and prevent them.

In the context of INSPIRE-5Gplus, one family of the RCA enablement techniques relies on Machine Learning algorithms to identify the most probable cause(s) of detected anomalies based on the knowledge of similarly observed ones. In the literature, there has been very little work published specifically targeting RCA for 5G networks, and none specifically addressing security. Terra and al. [153] study the application of explainable AI techniques for analysing the root-cause of Service Level Agreement violation prediction in a 5G network slicing by identifying important features contributing to the decisions. In order to cope with the increased complexity of 5G network management based on self-organizing network (SON) principles, Luengo and al. [154] propose a system for analysing the temporal evolution of the many different metrics and searching for potential interdependence under the presence of faults. This could eventually be applied to detect DoS but will not necessarily allow determining if the cause is related to security. Similar approaches are proposed by Rodriguez et al. [155] to detect the outage of cellular stations; Mfula et al.[156] that propose using bayesian networks to perform automated evidence-based RCA with the goal of maintaining the quality of the services; and Andrades et al.[157] that propose an automatic diagnosis system based on unsupervised techniques for LTE networks using self-organizing maps (SOMs) and Ward's hierarchical method, analysis of the statistical behaviour of each cluster, and an adjustment process based on the most similar cause. More recently, Bouattour et al.[158] apply RCA techniques for identifying the noise source in a virtualized infrastructure; and, Reshmi et al.[159] propose an automated network diagnostics and self-healing technique for 5G environment using predictive analysis.

The second family of RCA techniques is based on reputation and trust relationship evaluations (in different contexts, using various parameters or measurements, e.g., location, past activities as well as social networking activities, behaviors and experiences[160]). In this regard, social trust relationships can be established and assessed in a digital world [161] while reputation can be assessed based on feedback and Quality of Service (QoS) of an entity[162]. The exposal of responsibilities based on reputation values of partners of a service delivered across different domains allows to compute an

estimation of the domain responsible for a given service failure.

The most relevant 5G PPP project outcomes related to our liability and RCA work in the INSPIRE-5Gplus project are listed below.

- 5G ENSURE Project:
    - Trust Builder: This enabler provides system designers with a way to model and analyses their systems by automatically identifying the relevant threats and enumerating strategies to manage them. The trust model will be realised as an ontology which will encode the identified assets, threats and controls in a knowledge base. Based on the ontology and the system model, this enabler will be able to identify the relevant threats to the modelled system architecture, enriching the designed system model with the threat information. It will also allow the designer to select a management strategy based on controls automatically identified for a specific threat.
    - Trust Metric Enabler: The enabler provides means to achieve 'good enough' security by selecting the optimal security enablers and to enable visibility and configurability of 5G security controls. The optimal set of enablers depends on the application, current 5G setup and environment. New security features will not be developed as such, but existing redundant security features may be disabled based on this enabler.
    - VNF Certification: The enabler delivers a Certification process and tools to provide the Digital Trustworthiness Certificate (DTwC). The following schema illustrates the usage scenario of the enabler. This scenario describes the different mandatory roles, regardless of the implementations. For example, the evaluation laboratory could be instantiated inside the Software provider itself. Another possibility could be to have a Certification Body, only if an audit is requested; in this case, the certification would be a self-certification.
- **FI-PPP FIWARE project:** Thales Security analysis and remediation enabler builds upon CyberCAPTOR enabler (https://github.com/fiware-cybercaptor/) that has been developed within the FI-PPP FIWARE project. The main goals of CyberCAPTOR are to better understand the actual risk exposure of a Future Internet system through the detection of potential attacks based on NIST vulnerability database, or non-authorized usage in order to propose possible remediation. For PulSAR, components have been slightly redesigned in the following way:
        - Cyber data extraction: Topological and vulnerabilities data
        - Attack graphs and scored attack paths: Nice! The security operator can enter her own scores.
        - Remediation: To remediate possible attack paths
        - Dynamic Risk Analysis: Using a Security information and event management (SIEM) report as input, the feature dynamically computes an up-to-date risk picture.
        - Countermeasure: To cut an on-going attack
        - Visualization
    - Component-Interaction Audits: Networks comprise multiple components. Security policies specify both how these components should behave and how they must not behave. Similar, workflows specify how an entity should react to certain events. Detecting non-compliant behaviour of components with respect to a given policy or workflow is an important task to ensure the correct and save operation of a network. In particular, in a network in which (physical and virtual) components are managed by different tenants and directly or indirectly interact with each other, the detection

of non-compliant behaviour of a component is a major concern for the network operator. It helps the operator to protect the network, e.g., against misbehaving components and misconfigurations.

- **ETICS Project:** In ETICS approach [146], the network operator acts as intermediary between its customers (residential users and enterprises) and the different third-parties necessary to provide those high-value services. It becomes both provider and client (tenant), thus with different responsibilities and rights in this high-value chain. This model implies that responsibility in multiparty services is distributed among all partners. Indeed, in this context, in addition to cooperation among partners, a minimal level of transparency on how each partner manages its domain is crucial. Trust and reputation mechanisms or security-by-contract approaches can help to increase confidence between partners. The Etics project defined an alliance concept [146]. In this alliance, each partner is an independent entity, i.e. it has the sufficient autonomy to manage its domain. However, the combination of autonomous domains may lead to unpredictable and uncertain consequences regarding the end-to-end service quality level offered to customers, mainly due to the interaction of heterogeneous orchestration mechanisms of each domain. With a liability perspective, one is particularly interested in identifying the domain(s) or partners responsible for fault(s) and outages in order to hold those domains responsible for the damage inflicted upon customers.

2.6.1 Risks and Challenges

Dynamic liability and RCA enablement has some common risks regarding the implementation and their practical deployment in 5G as well as future B5G networks.

Scalability: The complexity of the liability and RCA with respect to varying problem sizes (hardware resources, dependency links, service components and liability relations) is a risk for practical implementations. In many practical cases, the number of components/indicators to be taken into the analysis can be very large. This situation can lead to a big volume of data processed and very complex algorithms to run. Similarly, the historical data and liability model have to be managed for size and be kept concise.

Data quality: The statistics and monitoring data that can be collected from the system fundamentally impact the efficiency of the enablement. For learning based approaches, for instance, it consists of the learning dataset during the off-line knowledge acquisition phase and the data gathered in real-time during the monitoring phase for analysis. Liability analysis and RCA require sufficient relevant monitoring data attributes and significant domain/system knowledge that can reflect the changes in the monitored system. Specifically, the granularity, frequency and out-of-order-ness of collected data are challenges which this enablement has to tackle.

The accurate and high-fidelity model representation for dynamic network infrastructure: The representative strength of the network model is another challenge for liability modelling and RCA in 5G and Beyond systems. These systems are large-scale and heterogeneous with dynamically changing topology, services and connected users. This situation poses the risk of having an unrealistic or obsolete system model which these algorithms deal with. That challenge is also related to how network model generation is performed for this enablement (model creation and definition capabilities). For machine learning based approaches, the identification of the most relevant learning and diagnostic methods/approaches considering the network characteristics is another challenge.

Performance metrics related challenges: One challenge for this enablement is the stringent performance requirements for a reliable operation since liability and RCA may lead to additional concrete outcomes such as financial penalties. In that regard, high precision and reliability require various performance indicators to be met such as *Precision at top K, Mean Average Precision (MAP)* and *response time* over the set of analysed anomalies and incidents.

Identification and utilization of informative attributes: For complex systems, it is common that the data collected is too complicated or even redundant. Basically, there might be some irrelevant or less

important attributes contributing less to the decision making. Therefore, it is essential that the optimal feature selection is done automatically using right schemes or manually by system experts. However, this brings along a risk of complexity on one hand and human bias on the other hand.

2.6.2 Future Applications

The evolution from trusted infrastructures to trustable or liable infrastructures[8] alters all existing assumptions and models about trust, in network node stack layers, and among network nodes, all mostly untrusted. The investigated models will have to take into account the convergence of digital and physical infrastructures (cyber-physical systems), the impact of security on safety (cyber-resilience), network heterogeneity and mobility (e.g., for large-scale vehicular communications), national security and sovereignty, and policy compliance requirements.

To adapt to the expansion of 5G threat surface and complexity, threat management will have to become more dynamic to match the 5G topology dynamicity. As a direct implication, future proposition for liability and RCA will have to adapt and become more dynamic, too.

As the liability management aims to distribute and allocate responsibilities between Domains, Services and tenants for each delivery of specific 5G end-to-end service, we can say liability is more related to a *Security/Responsibility By Design* approach. Therefore, its future applications are more applicable to the design phase where specific mechanisms and tools are integrated into 5G infrastructure. In case of trouble or during post mortem investigation, one tries to allocate and identify which part of the end-to-end chain of services and associated responsibility has failed. Therefore, in this approach we can assume RCA technologies are more related to a *Security/Accountability By Operation* approach and thus related applications.

2.7 SSLAs and Policy Management

SSLAs[168][165][166][167] and Policy Management are intended to introduce the business and security requirements as established by humans into a fully automated environment, therefore driving the behaviour of the system. On the one hand SSLAS establish a contract between operators to ensure a certain level of security that subjugates the system. On the other hand, Security Policies provide the abstraction and the formalism to enforce such SSLAs or other security restrictions either generated via Artificial Intelligence techniques (Section 2.3), either by human imposition.

Regarding Policy Management, Security Policies can be distinguished by its level of abstraction, High-level Security Policy Language Orchestration Policies (HSPL-OP)[163] and Medium-level Security Policy Language Orchestration Policies (MSPL-OP)[164]. These policies will be transformed by a refinement process from HSPL-OP to MSPL-OP and this later by a translation process to specific configurations to be performed by arbitrary security assets. Security policies can be generated in a proactive manner by the interpretation of the SSLAs, or in a reactive manner by system monitoring actions. During these processes conflict detection will be conducted in order to avoid system inconsistencies.

The SSLAs will be received as an entry point. They specify the required level of security as well as other constraints in cloud management (e.g. QoS). The SSLAs will be further refined to the required Policy Language that is being used (HSPL-OP/MSPL-OP) and then, it will follow the usual security policy enforcement cycle. The following previous projects have addressed to some extend the usage of Security Policies and SSLAs:

[8] In a **trustable infrastructure**, each stakeholder becomes liable to the others regarding its contribution to the end to end service. This becomes one of the major challenges to be addressed (with a relation with assurance guarantees of the infrastructure).

The H2020 MUSA project (Multi-cloud Secure Applications, 01/2015-12/2017 - H2020-EU.2.1.1.3, http://www.musa-project.eu/) had as main objective to support the security-intelligent lifecycle management of distributed applications over heterogeneous cloud resources, through a security framework that includes: security-by-design mechanisms to allow application self-protection at runtime, and methods and tools for the integrated security assurance in both the engineering and operation of multi-cloud applications. In this project Montimage was able to define SSLAs that allow specifying the properties that need to be respected in federated cloud environments.

The CelticPlus SENDATE project (02/2016-9/2019, https://www.celticplus.eu/project-sendate/) provided the technological concepts and solutions for a secure, flexible, low latency and locality-aware distributed Data Centre (DC) approach to support upcoming application scenarios such as Industrial Internet, mobile connected objects, Internet of Things, health applications, and 5G. The work in SENDATE focused on intra and inter-data centre –security, –control, –management, and –orchestration, placement, control, and management of VNFs, and high-speed transport networks to interconnect servers in a DC, DCs together, and the end users. Montimage contributed to this project by defining and building a Software Defined Monitoring and Security solution; and developing an initial prototype of the real-time SSLA assessment for SDN/NFV based Data Centres and 4G/5G Mobile networks.

The H2020 ANASTACIA project (Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures, 01/2017 - 12/2019 H2020-EU.3.7. H2020-EU.2.1.1., http://www.anastacia-h2020.eu/) focused on addressing the constant discovery of vulnerabilities in ICT components providing assurance security and trustworthiness by design. It designed and implemented a holistic security framework providing autonomous decisions using networking technologies (SDN/NFV) and dynamic security enforcement and monitoring methodologies and tools. In particular ANASTACIA evolved the SECURED HSPL/MSPL proposal adapting the model of security capabilities for NSFs proposed within the IETF. Anastacia already provided initial studies on 5G Verticals.

The FP7 SPECS project (Secure Provisioning of Cloud Services based on SLA management, 11/2013 - 04/2016, FP7-ICT-2013-10, https://cordis.europa.eu/project/id/610795) aimed at designing and implementing a framework for the management of the whole Service Level Agreement life cycle, intended to build applications (SPECS applications) whose security features are stated in and granted by a Security SLA.

2.7.1 Risks and Challenges

Concerning the risks on policy based enforcement in a zero human intervention environment, conflicts are included as one of the main risks. Conflicts can be found at different policy abstraction levels and can only be addressed by means of offering multiple alternatives. These alternatives are usually seen as the offer of multiple assets addressing the same security threat but also by the broadness of the scenario/deployment on which the system is acting. The limitation of any of these two implies a reduction on the alternatives to avoid the aforementioned conflicts. The risk of no alternative is therefore of primary relevance when policy based policy enforcement is employed. Besides, complex scenarios like multi-domain scenarios require special effort in E2E policy-based orchestration to ensure each involved domain will use common technologies to enforce the required security policies (e.g. An E2E channel protection solution requires that all involved parts use the same security protocols and parameters).

Furthermore, policy-based architectures, requires an extra level of system monitoring to keep available as much information as possible about the current status of the infrastructure. This information is essential to make good enough decisions during policy management processes such as policy conflict detection or orchestration processes like dependency resolution. An out-to-date information could introduce new conflicts during the enforcement of new security policies. Finally, it is also important to consider that policy-based infrastructure and operations do not generate a significant extra cost, not only in resources but also in time. Therefore the cost of applying the policy-based system should not outweigh the benefits it provides.

Regarding the challenges that INSPIRE-5Gplus needs to address in the context of security policy enforcement one of the main challenges is related with the adoption of a ZSM approach which introduces the multi-domain policy delegation concept. Within the project, the models inherited from state of the art solutions need to be extended taking into account the conflicts that may arise by delegating the decisions to other Security Management Domains or avoid them by relying on the intelligence and global view of the E2E Security Management Domain as specified in the ZSM architecture.

There is also a need to combine the SSLA with the security policies, establishing the hierarchy between them.

The security models employed in some previous research projects were not yet fully oriented to support 5G networks. INSPIRE-5Gplus needs to evolve these models to cover not only the particularities of 5G but also propose extensibility mechanisms to support next generations as well as the multi-access capabilities inherent to 5G.

Finally, an additional long-term challenge is going to be the tracking and accountability of SSLAs and their implementation through policies.

2.7.2 Future Applications

Policy Management will be aligned with the multi-level ZSM approach by using different abstraction policy levels, High-level Security Policy Language Orchestration Policies (HSPL-OP) for E2E Domain, and Medium-level Security Language Orchestration Policies (MSPL-OP) for end Management Domains. A conflict detection procedure is performed at each level. Assets in the scenario will be identified by its capabilities thus will be used for offering multiples alternatives to detected conflicts. A monitoring system will allow real-time transmission of information to E2E/end Management Domains to keep updated information of the current system status, thus maintaining the system information updated and enabling correct execution to solve dependencies. Policy Management is in charge of receiving the SSLAs and performing the translation to the required Policy Language (MSPL-OP/HSPL-OP). Policy Management decouples the complexity of hardware from management, allowing independent implementation of security assets, thus enabling the integration of current and further technologies into the system.

Policy Management will be enveloped by the Policy Framework that forms part of the E2E Management Domain handled within High-level Security Policy Language, and of end Management Domains that requires Medium-level Security Language, aligned with the multi-level ZSM architecture. The Policy Framework will do the refinement/translation process and also perform conflict detection at the different levels. Assets in the scenario will be identified by its capabilities thus will be used for offering multiples alternatives to detected conflicts. The Integration Fabric will allow the real-time transmission of information to E2E/end Management Domains to keep updated information of the current system status, thus maintaining the system information updated and enabling correct execution to solve dependencies. Policy Framework will receive the SSLAs and will perform the translation to the required Policy Language (MSPL-OP/HSPL-OP). The Policy Framework decouples the complexity of hardware from management, allowing independent implementation of security assets, thus enabling the integration of current and further technologies into the system.

Regarding the track of security policies, as the ZSM closed-loop may tweak them dynamically, it is important to save and to provide a clear and robust history of their changes. In this regard, a mixed solution with the previous ledger technology could be envisaged in the future.

Finally, SSLAs and Policy Management will play an important role in the context of beyond 5G. As the 5G and its descendants will infuse industries and consumers, the overall connectivity fabric will evolve in a fuzzier agglomeration of domains and resources. For example, the next 3GPP release 17 oversees the adoption of a common core infrastructure supporting wireless and fixed access: Fixed Network Residential Gateway (FN-RG). It will allow ISPs to converge assets into a common pool of resources and allow for sharing common management functions (for example policy and subscriber

databases). This convergence will be guaranteed that standard SLAs are applied onto shared users and heterogeneous resources while using different access point from the conventional 5G RAN. In this future, the traditional ISP home fibre box could be replaced by a shared programmable box, controlled by a 5G core and enabling the users to seamlessly connect to various networks and also to provide a new pool of resources beyond the MEC frontier. The SSLAs and Policy Management enablement will set a common standard applied across all the domains while ensuring that the policy will ensure the correct integration of resources into the system.

3 Initial Set of Use Cases

This section introduces a preliminary list of security Use Cases (UCs) and their relation with the previously introduced emerging enabling technologies. The process of defining and collecting illustrative use cases that demonstrate the potential of envisaged security assets and mechanisms started in parallel with research on INSPIRE-5Gplus security enablements. From the list of about 20 UCs the initial set was selected using 4 criteria: (1) coverage of 5G-PPP projects (security requirements related to ICT-17, ICT-18 and ICT-19 projects), (2) coverage of envisaged enablers of WP3/WP4, (3) usability/feasibility of UCs, and (4) complementarity between UCs (desirable but not mandatory).

The selected UCs were further developed into test cases in WP5 and described in D5.1[173].Subsection 3.11 provides a clear mapping between the illustrative use cases (IUC in short) presented below and the enablements presented in Section 2. The final set of use cases covering enablers developed within INSPIRE-5Gplus project will be presented in D2.3 to be delivered in M30.

3.1 IUC1 - Secured and Sliced ACCA (Anticipated Cooperative Collision Avoidance)

3.1.1 Problem description

Vehicular communications are expected to generate a considerable traffic volume in the near future, because of the different communications that may occur within and around a vehicle (i.e., vehicle to vehicle, vehicle to pedestrian, etc.). Security becomes important not only for the data but also for the safety of the people. This IUC is based on the experience obtained during the development of the Anticipated Cooperative Collision Avoidance test case belonging to the EC 5GCroco project and will be implemented as part of the test case number 1, as described in D5.1[173].

This IUC (Figure 5) proposes a road scenario with two Road-Side Units (RSUs) and a Central Node (CN) using an application to exchange messages. The RSUs gather the information send by a set of vehicles moving across a road and send it to the CN. By sharing information, vehicles may communicate with each other and inform about the road status (i.e., accidents, traffic jams, etc.) and so each vehicle may adapt its travel.

The focus of this IUC is on the use of Network Slicing and the re-configuration of its elements. More specifically, this IUC aim to deploy a network slice for a communications vehicle application between the two RSUs and the CN with a set of Security Functions (SFs) containing a Firewall for each RSU and an Intrusion Detection System (IDS) in the CN. The traffic coming from the RSUs will be analysed and the IDS will determine whether a vehicle can be trusted or not. Depending on it, its traffic will be blocked by the firewalls. The main goal is to re-configure an End-to-End (E2E) Network Slice using Security Service level Agreement (SSLA) to block the fake traffic generated by a malicious vehicle.

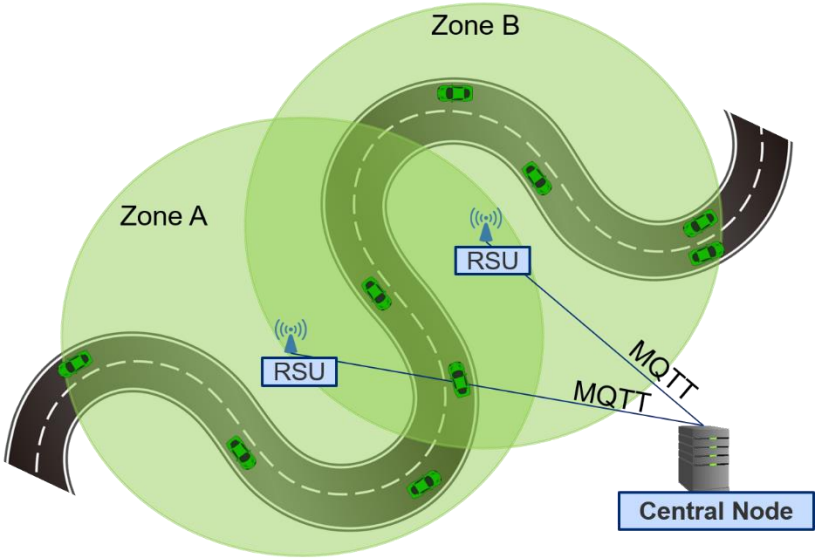


Figure 5 - Use case scenario A diagram.

3.1.2 Actors

- Service Provider (SP)
- A set of vehicles (Ann, Bob, Mallory, etc.)
- A malicious vehicle (Rob)
- Mobile Network Operator (MNO) -> Owner of the RSUs and Central Node.

3.1.3 Preconditions & basic flow

An E2E Network Slice must be deployed in order to generate the ideal situation to attack.

The basic flow consists of the following steps:

1. The SP has deployed over the MNO a Network Slice with an ACCA vehicle service. When deploying the Network Slice, a Security Service level Agreement (SSLA) will be associated.
2. The SSLA will imply the deployment of a Security Function (SF) -i.e. probe- with a V2X intrusion Detection System.
3. Once everything is deployed and all vehicles (Ann, Bob, Mallory, etc.) may move along the road using that service, at some point, a malicious vehicle (Rob) will start to generate fake information describing a car accident to disrupt the normal flow of the traffic on the road.
4. Using the SSLA and the V2X IDS, the services within the Network Slice should be re-configured in order to block the malicious data reaching the Road Side Units (RSUs) generated by the Rob to avoid the rest of the vehicles to receive the malicious information of a fake accident and so, they can keep moving normally.

The final result should be a re-configuration of the E2E Network Slice and the Security Function containing a Firewall, so the new information is added in order to block the traffic coming from the evil vehicle.

3.1.4 Success criteria

The goal will be achieved if after the intrusion is detected, the Network Slice is re-configured and the malicious traffic generated by the intruder's IP address is blocked and not shared among the other nodes.

3.1.5 Use case summary

This UC aims to solve security situations generated on a vehicular scenario by using SSLAs to react against an attack that tries to generate fake information. Showcasing SSLAs and Policy Management (Section 2.7) is the main objective. In this IUC, the use of SSLAs at a Network Slicing level will allow to deploy security elements around the Network Slice for an automotive vertical. By using SSLAs, this IUC presents how a set of security resources will be configured and then monitored, in order for the whole system to react when a malicious action appears and finally solve it.

3.2 IUC2 - Trusted and Collaborative Cross-border ACCA (Anticipated Cooperative Collision Avoidance)

3.2.1 Problem description

This IUC keeps the vehicular environment like the IUC before, but this time its focus is on the deployment of E2E Network Slices in a cross-border scenario. In there, the co-existence of different operators might need to be managed. While the normal tools on this kind of scenarios is the use of contracts and agreements, this IUC proposes the use of Blockchain to generate trust among the different operators and other actors and allow the collaboration among them to deploy E2E Network Sliced composed by certified elements. Like the previous IUC, this is also based on the experience obtained during the development of the Anticipated Cooperative Collision Avoidance (ACCA) Test Case belonging to the EC 5GCroco project and will be implemented as part of the test case number 1, as described in D5.1[173].

This IUC (Figure 6) aims to add trustworthiness to any deployed network slice by ensuring that all the components composing a network slice have been previously certified and its related actions are shared and publicly known among all the players through a Blockchain network.

Blockchain becomes the tool to keep track and make public the E2E Network Slices and their elements -i.e., network services and functions-. The Blockchain network will be composed by Network Slice Managers (NSMs) and Software-Defined Network (SDN) Controllers belonging to the different operators.

The other important aspect in this IUC is the use of certified network Slice components to be trusted by all the peers. To do so, a certification tool will be implemented and used.

The scenario for this IUC aims to use a vehicular scenario in which different cross-border operators work together to deploy an E2E Network Slice for an automotive service by collaborating with each other using Blockchain to control the multiple steps. The deployed E2E Network Slice will be composed only with certified resources.

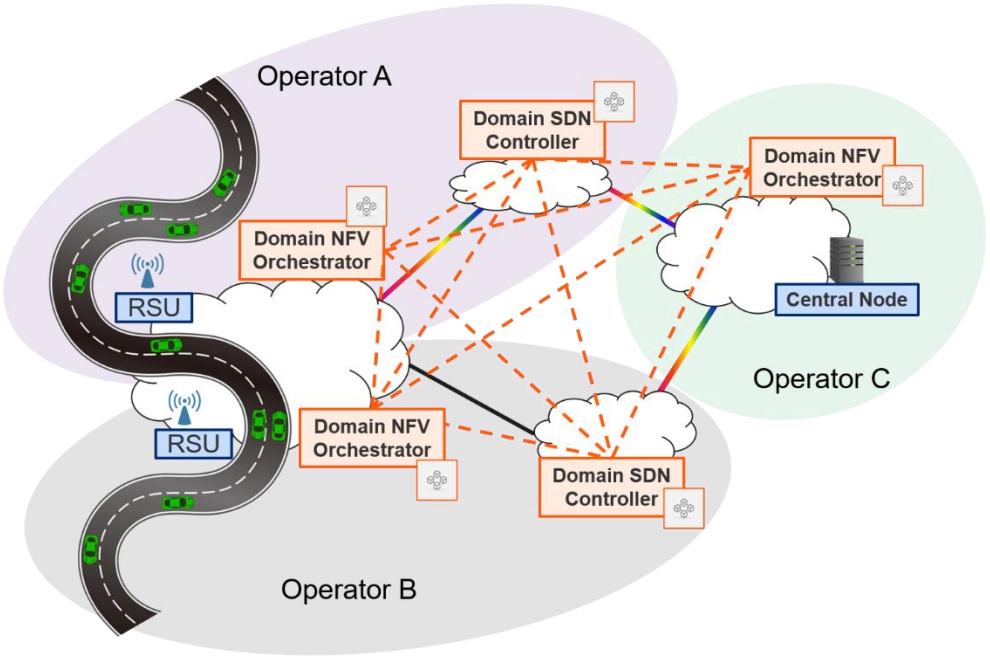


Figure 6 - Use case scenario B diagram.

3.2.2 Actors

- Service Provider: The owner of the deployed service.
- Service Developer: The designer of the deployed service.
- (Cross-border) Operators: Owners of the RSUs and Central Node.

3.2.3 Preconditions & basic flow

A Blockchain must be configured and working having as peers a set of Network Slice Managers.

The basic flow consists of the following steps:

1. A private Blockchain is composed by a set of Network Slice Managers from different network operators.
2. A Service Developer designs and checks with the Component Certification Tool the designed descriptors, if they are certified, they can be shared in the Blockchain so the other peers may trust them and requests a deployment of those resources.
3. A Service Provider may deploy Network Slices using resources from the different cross-border operators in order to offer the automotive communication service.

The results should be the acceptance and deployment of those NSTs and its components that were previously validated and tagged as trustworthy.

3.2.4 Success criteria

The goal will be achieved only if the trustworthy NTS and components are accepted and deployed and any Service Provider is able to deploy a non-trustworthy NST using a Network Slice Manager participating in the Blockchain system.

3.2.5 Use case summary

This UC aims to solve security situations generated on a vehicular scenario by using Blockchain share publicly which elements may be trusted and non-trusted elements. It shows a scenario in which

trust among different actors is an important aspect. To generate this trust among them, this IUC makes use of Distributed Ledger Technologies (Section 3.2). In this IUC, DLT is implemented to manage in a collaborative way the deployment of Network Slices in a cross-border scenario. The key element to implement this collaborative procedure is the use of Smart Contracts. Smart Contracts will allow the exchange of information and to trigger different procedures in a public and transparent way, so all the peers involved in the Blockchain network will be aware of any action in the deployment procedure.

3.3 IUC3 - Definition and assessment of Security and Service Level Agreements

3.3.1 Problem description

The ability to define and manage Security-oriented SLAs (SSLAs) is essential for operators offering managed services. Similar to the SLAs concerning performance, SSLAs is a contract between an operator and a customer that defines the services and the security levels that both parties expect. In other words, SSLAs are needed by operators, service providers and end-users to “contractually tie” the requirements related to security capabilities of the provided networks, slices and services. The defined SSLAs allow controlling that the security functions are correctly implemented and that the security properties are not violated.

To better automate the process of defining and enforcing SSALs, real-time monitoring of network, application and system activity based on distributed probes is needed. The probes, or Security Agents, capture the data, meta-data and statistics that allow measuring the parameters implicated in the specified SSLAs. Then, complex event processing and machine learning can be used to analyse and detect breaches at the local level by the Security Agents or at the domain or cross-domain level by the Security Analytics Engine. Finally, when breaches are detected, corrective actions (e.g. self-healing or self-protection techniques) need to be taken. These actions can be triggered manually by the operators, or automatically by the Decision Engine that interacts with the Orchestrators and Controllers to perform the necessary actions.

SSLAs are defined for assessing and controlling that:

- the security functions are correctly implemented
- the security properties are not violated
- the violations trigger self-healing and self-protection strategies

SSLA metrics examples:

- Data and service availability
- Geo-localisation of data/services
- Frequency of security analysis
- Number of GTP per subscriber
- Isolation access from other slices
- Security enforcement techniques (Time to deploy new technique, Delay in applying patches, Delay in reconfiguring, Delay in revoking users/operators, Delay in replicating services and switching instances)

The main goal of this IUC, the definition and enforcement of SSLAs, is to facilitate the agreements between different constituents concerning the expected cyber-security level and remediation strategies.

3.3.2 Actors

Involved stakeholders:

- Network operators
- Slice managers
- Service providers
- End-users

3.3.3 Preconditions & basic flow

The preconditions include:

- The specification of the SSLAs.
- The rules, algorithms and strategies need to be specified and deployed in the different components (depicted in Figure 16), i.e., probes (called Security Agents) that capture the necessary meta-data, the security analytics application (called the Security Analytics Engine) that will use the SSLAs defined to detect if they are respected or not, and the decision algorithm (called Decision Engine) that will determine what needs to be provided to the orchestrators (called Security Orchestrator) to modify the configuration or the topology of the network.

The basic flow consists of the following steps:

- Step 1: The SSLAs need to be specified and verified. They need to be managed by a policy management application.
- Step 2: Probes need to be provided that can extract the metrics required by the SSLAs, and integrate local analysis functions. They need to be able to perform real-time capture of metrics. Possible data the needs to be processed by the probes is: network data/control plane traffic, system logs, and application traces. The probes should have the ability of analysing the data using specified rules extracted from the SSLAs, and eventually analysing statistics and behaviour using machine learning techniques.
- Step 3: The probes are deployed and configured to assess the SSLAs.
- Step 4: Metrics and notifications provided by the probes need to be communicated through some channel to the Security Analytics Engine.
- Step 5: The Security Analytics Engine needs the rules and algorithms that allow it to detect breaches and notify the Decision Engine when they occur.
- Step 6: The Decision Engine needs the rules and algorithms that define the strategy that needs to be triggered to remediate a detected breach. The strategy can be implemented using pre-existing or generated scripts, generated Tosca or MSPL descriptions, embedded functions, or generated alarms/notifications that will be addressed manually.

The results obtained:

- SSLAs are verified (respected or violated) and the remediation strategy is correctly carried out.

Figure 7 presents the functional architecture for the IUC.

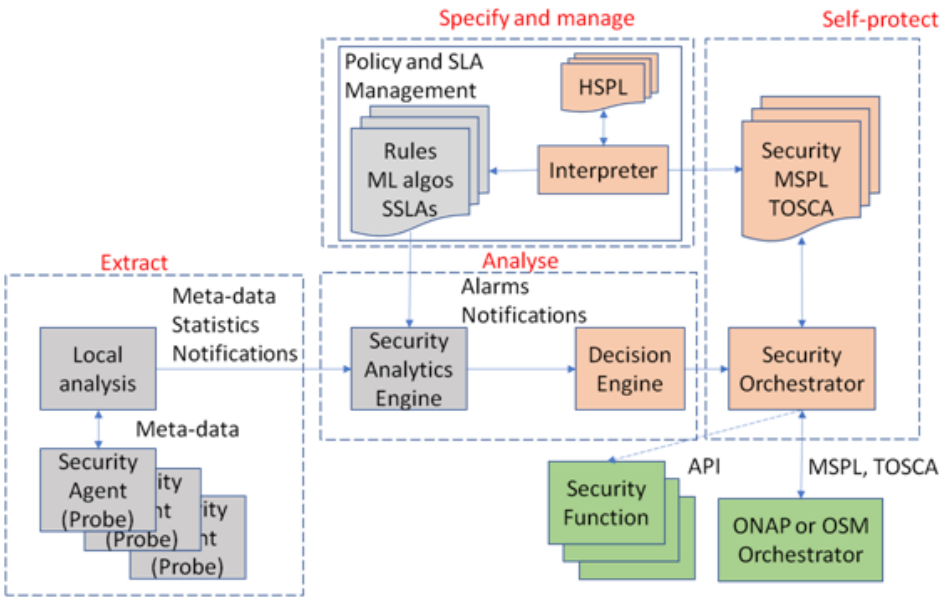


Figure 7 - Use case functional SSLA assessment architecture diagram

The main functions are depicted in orange. The probes (Security Agents) provide the data analysed locally and/or by a centralised application (Security Analytics Engine) that will notify the decision algorithm (Decision Engine). The Decision Engine will trigger the corrective actions that could involve interacting with an orchestrator (Security Orchestrator) or directly with the security functions (e.g., firewall, service chaining manager) and controllers (e.g., hardware appliances, routers).

3.3.4 Success criteria

The IUC is successful if the rates of false positives and true negatives are low, and the reactions correctly remediate the security problems detected, assuring that the SSLAs are applied at all times as far as possible. The security problems involve both detecting malfunctioning security functions and malicious attacks (e.g. DDoS, data exfiltrations, and evasions).

3.3.5 Use case summary

This IUC shows how SSLAs can be defined for formalising the requirements related to a wide variety of cyber-security issues and concerns. The definition and assessment of SSLA require the definition of the security requirements, policies and established agreements (in the case where several entities are involved). The requirements, policies and agreements need to be translated to rules involving the related metrics that allow detecting if the SSLAs are respected. The technologies and enablers required are the management function for dealing with policies and SSLAs (technologies Sec. 2.7) to derive and deploy the SSLAs assessment rules; the "optimized" probes or Security Agents (technologies Sec. 2.4) to obtain the necessary metrics and apply "local" rules; the some standard data store technology or DLT (Sec. 2.5) to provide historical metrics and metrics from different domains and providers; and, the security analytics application (using AI technologies Sec. 2.3) to analyse the collected metrics and apply "global" rules.

The IUC goes far beyond current intrusion detection and prevention systems, as well as policy control systems, in that:

- It is based on real-time metrics that allow fine-grained or more abstract assessment of the security requirements of the different stakeholder involved.
- It allows detecting security breaches as well as malfunction of security functions.
- It integrates remediation strategies that can be triggered automatically with the goal of enforcing the specified SSLAs (self-healing, self-protection).

3.4 IUC4 - Network attacks over encrypted traffic in SBA and security evasion prevention

3.4.1 Problem description

5G networks will increase the use of encrypted communications. 5G Core includes the concept of Service Based Architecture (SBA). It uses HTTP/2 as the protocol base to leverage all signalling traffic, instead of legacy DIAMETER protocol. Starting with Release 15, 3GPP mandates TLSv1.2 for RESTful APIs (as represented in Figure 11). On the contrary, data plane traffic between the RAN and the Core rely upon the use of GTP-U that is not usually encrypted. The reason is because encryption already is done at application level following the current tendency is expand E2E encryption over internet applications and services based on the use of TLS, e.g. DoH (DNS over HTTPS), QUIC (HTTPS over UDP). As a consequence, current cybersecurity network tools based on network monitoring will be ineffective in this environment, making it very difficult to detect some common attacks based on botnets, application layer attacks or DDoS, because they are evolving to support TLS as a channel of communication. This evolution introduces new threats over REST APIs channels that are hidden inside TLS. Potential attacks include malicious vulnerability scans, DDoS, application layer attacks on SBA microservices, roaming interfaces, interfering with SB Interfaces such as Naf, etc.

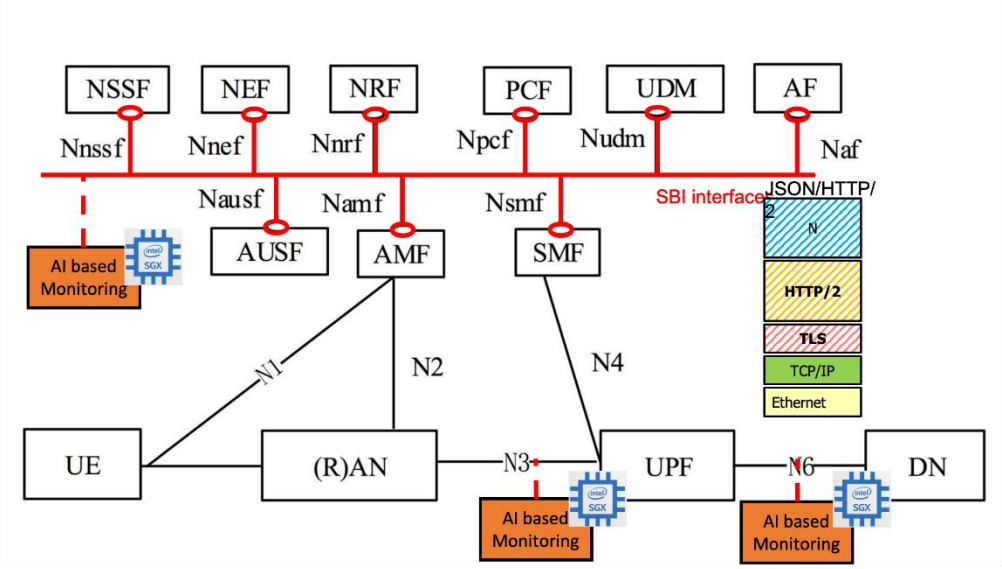


Figure 10 - Use case overview

Additionally, the massive adoption of microservices, NFV and Cloud approach in the deployment of 5GCore components and monitoring tools, will open the door for introspection attack (direct access on the software) that can be exploited by a malicious attacker and, in this way, access the software, reverse engineer it and find a way to disable the detection. Evasions will prevent the monitoring function from working correctly. This can be done by making it crash, by reducing its performance resulting in partial traffic analysis, or by introducing unknown attack techniques that remain undetected.

This use case proposes the evolution of the security monitoring tools to be capable of analysing encrypted traffic, so it can detect and mitigate attacks. Multiple probes could be allocated in different point of 5G network, to receive a copy of the traffic a generate alerts to be addressed by management and orchestrations systems. Additionally, this use case leverages the use of data and software protection techniques empowering Intel's SGX enclave[9] to prevent two types of attacks:

unauthorised access to data on the one side and detection of software characteristics and behaviour the other side.

3.4.2 Actors

The actors and roles involved in this UC are:

- 5G network administrator, such as Network/Security Operation Centres (NOC/SOC). This actor covers the role of the responsible of the administrative domain. Also, is capable to enforce specific policies in the network, e.g. using a NFV MANO to re-instantiate a component.
- Malicious party. Usually represented by the attacker, hiding their attacks in the encrypted traffic or attacking the monitoring software.
- Security monitoring probes integrated or adapted to the INSPIRE5g-plus framework to extract relevant information and push it to the analytics engines in charge of detect the attacks.
- Security Analytic engine that will visualize and report the attacks to the management entities (e.g. MANO NFV) to take corrective actions.

3.4.3 Preconditions & basic flow

This use case starts with a 5G network based on SBA 5GCore in normal operation (No attacks or aware of malicious activity). The administrator detects service performance impact, cause by degradation of some instances of the 5G Network Functions (e.g. a DoS attacks, malware spread, etc., generated by the malicious party), but do not know the cause or the remediation.

The administrator deploys monitoring agents in the network that can be activated to monitor control and data plane. i.e. a set of monitoring VNFs in the cloud or on-premises. Based on these probes (Security Agents or enablers) deployed at different points in the network, metrics are generated and aggregated from network traffic in suitable format, to feed them to inference engines trained using AI/ML to identify malicious behaviour patterns in the encrypted traffic. Identified malicious flows and activity will be reported to the administrator and it will take actions to mitigate the attack, using specific security policies such as, firewalls, or active probes. Alternatively, the affected functions (e.g. an infected container or virtual machine of 5G core), can be cleaned and re-instantiated (with a certificated by vendor version) to remove the problem.

To avoid Introspection attacks and reverse engineering, it is necessary to harden the integrity monitoring of the network functions using Trusted Execution Environments (TEE). The runtime integrity verification needs to be backed by a TEE embedded routine.

As a result of the detection over encrypted traffic, the normal operation of the network is restored, attacks identified and mitigated without loss of encryption capacity of the network, in terms of privacy and security enhancement.

3.4.4 Success criteria

Some attack examples will be used over encrypted traffic. Detection of them will represent the success. KPIs results from ones defined in Test Case number 3, presented in INSPIRE-5Gplus Deliverable D5.1 [172] will quantify the success criteria.

3.4.5 Use case summary

This Use Case concerns the detection of network attacks over encrypted traffic in Software-Based Architectures as standardised in 5G [3GPP TS 23.501]. It also includes attacks on monitoring software functions (e.g. reducing their performance, provoking malfunctioning), making attacks undetectable

by tampering its integrity. In order to be able to detect malicious activities and patterns from the network despite of the encryption, will need the use of Artificial Intelligence (AI) enablements (Section 2.3) focused in anomaly detection and classification and an automation component to mitigate the attacks such as the defined close loop framework by ZSM (Section 2.1). These enablements will also require data generation, i.e. network telemetry, as it is highlighted in Advanced CyberSecurity Techniques (section 3.4), mentioning some ICT-17 projects infrastructure, such 5GVINNI, that has focused in telemetry generation capacity. Finally, introspection attacks mitigation proposed in this IUC will require the applicability of TEE enablements (Section 3.2).

3.5 IUC5 - E2E Encryption TEE secured SECaaS

3.5.1 Problem description

5G verticals use slices across multiple domains to exchange sensitive data. E2E slices provide, to some degree, the privacy needed through traffic isolation; but E2E cryptographic protection is also needed to provide data confidentiality, integrity and extra privacy as well. Besides, the data protection in the different 5G network domains (Access, Transport, Core) is not always well managed. Static keys, or very long key and certificates refreshment, open more opportunities for attackers to access the content. In this context, there are two requirements to be fulfilled: endpoint authentication, and data encryption. Therefore Zero Touch VNF-based E2E encryption over 5G MECs is proposed following the centralized SDN control paradigm for key distribution and, at the same time, hardware-based enclaves on the MEC to protect cryptographic material usage.

As an extra secure communications layer, VNFs acting as proxies can be deployed dynamically to protect communications end-to-end. It is the case for IPSec and also for DTLS in case of UDP communications as is usually seen in IoT environments. The basis of both encryption systems is based on key derivation which in turn can be done centralized or on the hosts. To implement this approach, on the one hand, IETF proposes I2NSF (based on IKE); on the other hand, TSG proposes a fully software-defined security (SD-SEC) orchestration using cloud-native container orchestration API; however, both ways have important similarities.

While end-to-end communication may be encrypted, it is also true that latest computer processor vulnerabilities open the door to memory introspection to extract keys (such as AES). The idea here is to take profit of SGX enclaves to perform encryption-decryption operations transferring native code to the TEE, therefore protecting the delegated VNF security from other MEC node neighbouring VMs.

3.5.2 Actors

The actors and roles involved in this UC are:

- End-users
- System Administrator/NOC
- Security Intelligence Service (as a reaction to events)
- Long Term cognitive Decision Engine (as a long term decision based “may be” on system history)
- Network domains involved (Access, Core, transport, datacentres, MEC,..)
- Mobile end users with sensitive data.

3.5.3 Preconditions & basic flow

The UC requires the following pre-conditions:

- End- users are authenticated and given access to the 5G network

- There is a need for data path traffic protection (IPSec, DTLS) by administrator/NOC decision or as an incident response
- Edge nodes are located nearby the RAN to which end-users are connected. Need for traffic redirection capability.
- Intel SGX is available in the Edge nodes
- There is a need for a “SDN alike” transport network.

Figure 8 shows the UC subsequent actions:

1. Either the administrator/NOC (a), Security Intelligence Service or Cognitive Decision Engine (b) decides that there is a need for protecting traffic between two devices or between a device and the cloud.
2. An HSPL and probably a SSLA is generated that defines the E2E need.
3. There is a translation and conflict detection process.
4. Subsequent definitions are generated for each Management domain. At the very least two virtual domains; the transport network and the RAN, to divert traffic to the vdomain.
5. vIPSec enabler with Intel SGX is deployed, E2E connectivity and configuration of the vIPSec enabler from the centralized management entity (SDN Controller) is performed.
    a. Network Interfaces discovery
    b. SAD/SPD models enforcement
    c. Traffic E2E is protected.

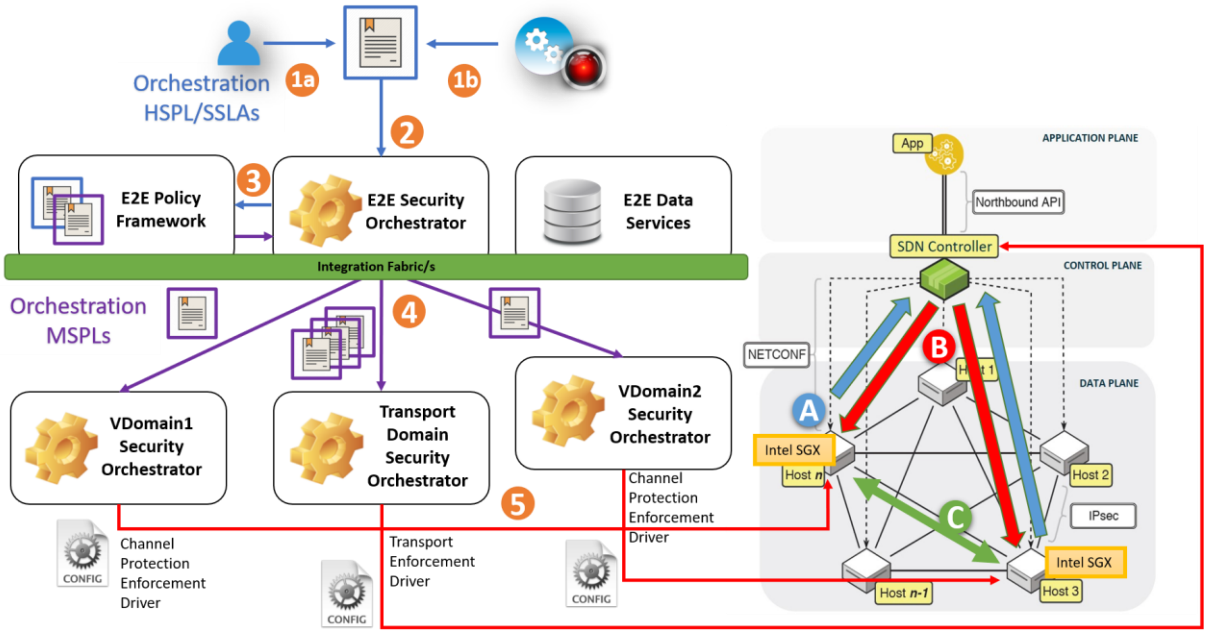


Figure 8 - Use case diagram

3.5.4 Success criteria

The connectivity is achieved over the transport networks. Monitoring the traffic will confirm that the traffic is encrypted with technological solutions designed (IPsec and DTLS). Additionally, key material is renewed and traffic re-encrypted from the centralized INSPIRE-5Gplus Control plane.

3.5.5 Use case summary

Traffic is protected/encrypted over the transport network in an independent slice transparently to the user equipment (UE). Operations are performed within the TEE Enclave. It illustrates a Zero-Touch encryption policy management and enforcement, in line with the ZSM enablements (Section 2.1). Besides, the cryptographic material and routines (using such material) are going to be implemented in virtualized network functions (VNF) and protected by Trusted Execution Environment techniques (section 2.2). Once the secure channels have been established, it is of utmost importance to really check that the information is really flowing through them encrypted. To that end, Proof of transits and smart contracts (Section 2.6) are envisioned to provide liability and trustworthiness to the operations. All of these are operated in a ZSM closed loop based on the definition of high-level security policies and possibly SSLAs (Section 2.7) that are enforced on a multi-domain scenario.

3.6 IUC6 - End-to-End Slice Protection based on Moving Target Defence and Anomaly Detection

3.6.1 Problem description

This UC aims at protecting network slices, one of the fundamental building blocks of 5G, that will allow the realization of advanced use cases in several Verticals not feasible with legacy mobile networks. However, such new capabilities enabled by 5G advancements come with various side effects, including the increased attack surface due to new flavours of technologies introduced, such as software-defined infrastructures, slicing with multi-tenancy, multi-actor service paradigms and complex/multi-tier architecture. Under certain circumstances, these could constitute potential sources of vulnerabilities, increasing the likelihood of security incidents.

This UC will investigate both proactive and reactive security mechanisms for E2E slice protection. One aspect includes the collection and joint analysis of heterogeneous data from multiple points of the 5G infrastructure for integrated monitoring, with specific focus on detecting and classifying anomalies associated with security incidents and their subsequent resolution by INSPIRE-5Gplus security enablers and related actors. Another aspect is the provision of Moving Target Defence (MTD) approach to dynamically reconfigure parts of the infrastructure, in order to increase the attacker's effort and cost in a smart way via AI/ML techniques. An important consideration of this UC will be to strike a balance between security effectiveness of MTD and the cost of reconfiguring the protected network.

The cooperation of the MTD mechanism and the Slice Manager is mainly based on network slice monitoring, especially of critical slices that will trigger their reconfiguration proactively and reactively based on a defined threat and cost model. This chain will be supported by additional enablers, including Security Analytics Framework, a Security Orchestrator and a Monitoring Framework, provided by INSPIRE-5Gplus.

In addition, MTD will provide protection of the security functions themselves in a slice to increase their robustness against reconnaissance and attacks, while maintaining their configuration integrity. All these actions will form a unified and closed-loop scheme based on a data-driven approach for E2E network slice protection.

The Moving Target Defence mechanisms deployed inside this Use Case should be adapted corresponding to the confronted threat. The level of MTD applied could range from no action to simple indirection and even to multiple stacked indirections. The end goal is to avoid penalizing legitimate users and progressively make the path to the protected resources more and more complex for malicious users.

This Use Case will provide the opportunity to explore a number of scenarios for protecting the

network slices, including Dynamic Service IP Mutation and Optimized Security Function Mutation. The Use Case will also make use of several INSPIRE-5Gplus enablers, in order to create an end-to-end ecosystem for demonstrating the specified scenarios.

3.6.2 Actors

The actors of this UC are the following:

- Mobile Network Operator (MNO): The owner of the infrastructure.
- Service Provider (SP): A Service Provider that deploys its services over the MNO infrastructure.
- Network Domains: The RAN, Core, Transport and Edge domains. The UC will utilize the relevant parts of the 5GENESIS[10] infrastructure.
- Network Administrator: NOC Department of Operator.
- Monitoring Framework: It will provide an E2E overview of the network to the Network Administrator.
- Security Agents: Probes and/or security functions dispersed over the network to collect incoming data from the infrastructure.
- Security Analytics Framework: The Anomaly Detection Service will process incoming data and detect abnormal traffic flows.
- Decision Engine: The Decision Engine will provide the mitigation actions (like slice re-configuration) based on incoming data and alerts.
- Slice Manager: The 5GENESIS Slice Manager (Katana)[11] will deploy network slices based on defined Network Slice Templates.

3.6.3 Preconditions & basic flow

The UC requires the following pre-conditions:

- An operational 5G SA implementation, including the COTS UEs, RAN, Core, Transport and Edge infrastructure.
- Two concurrent slices dedicated to an eMBB and a URLLC service, respectively. The URLLC service will be considered as a “critical slice”.
- An operational E2E network and service management platform instantiated by the Slice Manager, the MTD controller, the Security Analytics Framework, the Monitoring Framework, and the OptSFC (Defence Optimization Engine).
- A malicious node(s) that will cause attacks on edge services (e.g., DDoS) resulting in a compromised infrastructure.

The UC includes five steps of subsequent actions:

- Step 1 includes the collection of data by the Security Agents from several points of the network and provides them to the Security Analytics Framework.
- In Step 2, the Security Analytics Framework performs all necessary data pre-processing and ML inference to detect abnormal traffic, resulting from potential security incidents. In case of

[10] https://5genesis.eu/

[11] https://github.com/medianetlab/katana-slice_manager

detected anomalies, the Security Analytics Framework provides trigger alerts to the administrator and other security entities.

- Step 3 includes the mitigation actions decided by OptSFC, which is part of the MTD mechanism for the specific UC. It is important to note that the MTD mechanism does not necessarily get triggered by an alert from the ADS, in order to proceed to network re-configurations. It can also act in a self-driven manner to improve defence standing (specially to minimize attack surface and evade attacks) and to protect the 5G system proactively. However, these steps are numbered sequentially to provide a clear explanation of the action flow.
- Finally, in Step 4 the Slice Manager deploys the updated Network Slice Template, by communicating with the components of the Management and Orchestration Layer (MANO), namely the NFV Orchestrator (NFVO), the Virtual Infrastructure Manager (VIM), the Element Management System (EMS) and the WAN Infrastructure Management (WIM), in order to manage the functions in the network and perform CRUD operations on network slices.

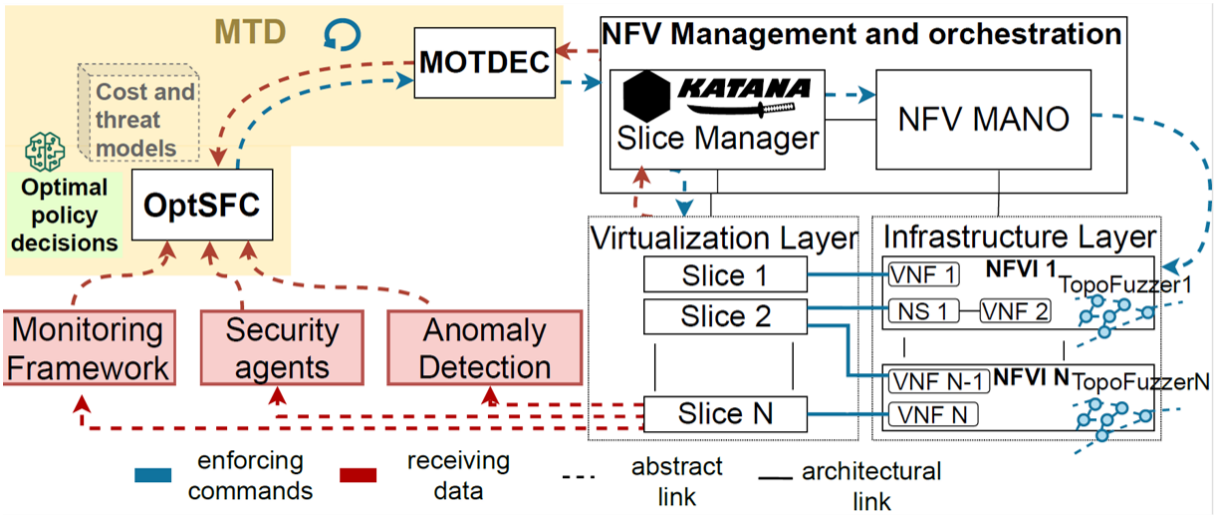


Figure 9 – IUC6 Diagram

The successful result of the UC lies on the following outcomes:

1. To proactively change the slice configuration to alter the attack surface and impede pre-attack reconnaissance advantages of attackers prior to attack stage.
2. To properly detect security incidents and alert the network protection chain for further mitigation actions.
3. To re-configure parts of the network, provided a trigger alert or not, based on an optimized cost model that will maintain the balance between security effectiveness and the cost of reconfiguring the network.

3.6.4 Success criteria

The success criteria will be quantified under the validation of the KPIs defined in the relevant Test Case, presented in INSPIRE-5Gplus Deliverable D5.1 [173]. The post-conditions will be interpreted by KPIs, including but not limited to Mean Time to Implement the MTD action, MTD action cost, protection gain of the MTD policy and Mean Decision Time for MTD action. In addition, the number of false positives and negatives will be considered regarding the feasibility of the anomaly detection system on detecting different types of attacks.

3.6.5 Use Case Summary

This Use Case will demonstrate the efficient protection of network slices through proactive and reactive security mechanisms by effectively detecting and classifying security anomalies and utilizing Moving Target Defence (MTD) paradigm to dynamically change properties and reconfigure parts of the 5G infrastructure. It highlights the application of Moving Target Defence (MTD) techniques to protect end-to-end slices. First, this use-case requires the collection and the analysis of data to monitor resources and detect anomalies. The advanced techniques on Security Monitoring Optimization highlighted in the Section 2.4 allow for a predictive and proactive detection of those anomalies. Second, the Section 2.4 explores the MTD mechanisms to adapt and modify a slice for mitigating a threat using the AI tools showcased in Section 2.3. Finally, this protection will be autonomous and implemented in a ZSM closed loop based on the Section 2.1 architecture.

3.7 IUC7 - GDPR aware counterparts for cross-border movement

3.7.1 Problem description

Each country in the EU has its own laws in terms of data privacy and the EU itself defined the GDPR as a mean to control data leakage and data transfer on third parties, making special distinction for cloud providers. There is a need to ensure that the data uploaded by roaming users complies with local laws and, where it does not, to be able to clear liabilities.

In this context, every communication established using GDPR protected devices must be GDPR compliant, when a lack of compliance is detected, actions must be registered for further clarification of liability.

vOBUs which are designed to address GDPR enforcement, must be flexible enough to migrate from one law context to other guaranteeing the channel protection between the UE/car and the cloud in heterogeneous and dynamic environment, where its actions must be trustfully and non-refutable stored in the operator infrastructure (see Figure 10).

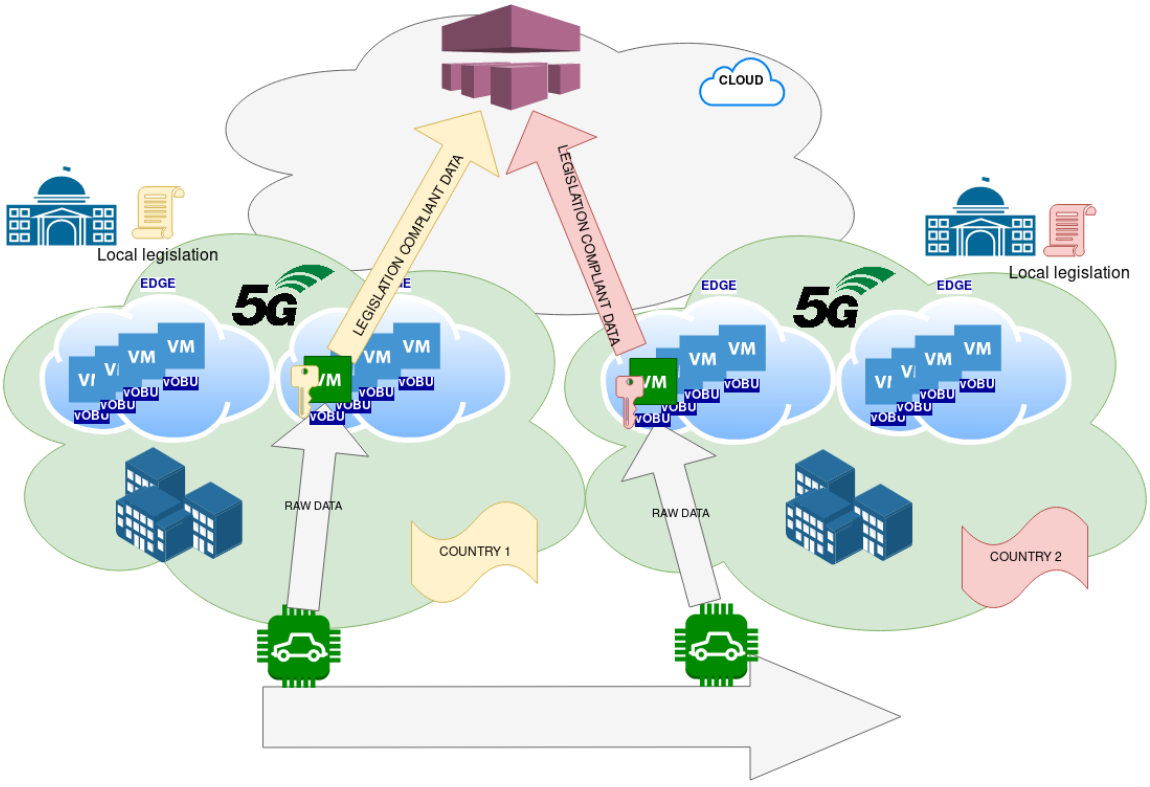


Figure 10 - Cross-border virtual counterpart migration concept

3.7.2 Actors

- Vehicle1
- Mobile Network Operator MNO1
- Mobile Network Operator MNO2 (or RAN in another country from MNO1)

3.7.3 Preconditions & basic flow

The UC requires the following pre-conditions:

- Two operational 5G SA/NSA implementation, including OBU UE, RAN, Core, Transport and Edge infrastructure TEE capable.
- A multi-domain integration fabric
- DLT with stewards, nodes capable to participate in the validation process and maintain the DLT.
- Trust reputation assessment based on historical behaviour of virtual and physical entities

The UC includes the following subsequent actions:

The car starts and gets connected to the 5G network. Car's on-board unit (OBU) is associated with a virtual counterpart or virtual OBU (vOBU) on the operator's EDGE capable of proxying any communication and analyse the content. The connection between OBU and vOBU is protected. The vOBU is trusted by the operator thanks to it being certified by the Trust Reputation Manager. That vOBU fulfils local laws.

The initial set of security policies to be applied to the connectivity of the UE can be determined by means of employing behavioural profiles, established by vendors and retrieved by the network in order to help in the customization of security policies per device type.

When the car moves to another country, a new virtual counterpart needs to be created, this new vOBU is entrusted with the fulfilment of the visiting country law. The Trust Reputation Manager employs historical tampered data stored in the Trustable Data Services to produce a score to not the vOBU image which needs to be instantiated on operator's edge, but also about the compute nodes themselves, therefore fostering the migration of the resources triggered by car movement.

Depending on the specifics of vOBU migration, it can be done as a full copy of the VM, so that the behaviour needs to be changed programmatically, by new VM with shared data that may contain or not the cryptographic material, in such a case, the migration of the cryptographic material can be oversee by TEE technologies. In any case the network needs to take care of the migration of the connection between the OBU and the corresponding vOBU.

The successful result of the UC relies on the following outcomes:

- The car has moved to a new location in terms of 5G connectivity.
- The vOBU has been migrated to the new location and a security association with the OBU remains valid with confidentiality warranted thanks to TEE.
- The network transparently redirects the packets to the new vOBU from the OBU.
- The vOBU traffic is analysed and is compliant with the GDPR and score of the source image is maintained.
- Score for compute nodes is updated based on the success of the operation.

3.7.4 Success criteria

The network has established customized security policies based on OBU vendor behavioural profile.

The OBU has established a security association with the vOBU which is maintained upon vOBU migration originated by OBU network movement.

Cryptographic material does not leave the enclave and the data non-compliant with GDPR or other business policies does not leave the vOBU.

The time for VM migration and security enablements calculations such as Trustiness level or communications encryption are unnoticeable and transparent to the end-user.

3.7.5 Use case summary

This use case will demonstrate a multi-domain policy enforcement ecosystem that evaluates trustworthiness of the enforcement therefore driving the decision and election of possible actions. It proposes a multi-domain scenario that relies on the definition of high-level security policies (Section 2.7) that are enforced on a multi-domain scenario with the consequent responsibility delegation that with the ZSM closed loop (Section 2.1) provided by the Inspire5G-Plus High-Level architecture (Section 4). The mobile devices will establish encrypted tunnels to their virtualized counterparts that will change with the location migration of the device, the cryptographic material protection is envisioned by means of Trusted Execution Environment (section 2.1) techniques. The information generated during the operations is stored inside a DLT (Section 2.5), thus being registered in a non-repudiable way. Smart Contracts are also used to provide some trust to the deployment, therefore providing a trustiness level related to the virtual counterpart, allowing the automated deployment system to decide whether it should be used or not.

3.8 IUC8 - Intelligent and Secure Management of Shared Resources to Prevent (D)DoS

3.8.1 Problem description

Dealing with security threats is a never-ending task where attackers continuously renew their strategies. The security provider needs to always find and adapt to new threats. This cat-and-mouse game leads to moments where attackers have the upper hand with offensive strategies that thwart deployed defences. For instance, the contemporary (Distributed) Denial of Service ((D)DoS) attacks are getting stealthier, having the ability to mimic genuine behaviour with low-bandwidth usage, which allows them to evade the detection mechanisms.

The goal of this illustrative use case is to demonstrate the ability to do damage control when a situation in a slice escapes direct threat detection and mitigation. In fact, the interdependence between slices due to virtual network functions and infrastructure resources sharing rises the risk of indirect (D)DoS; that is, the direct (D)DoS exhausts the resources of one slice, which may influence the resources shared with other slices, affecting the availability and performance of provided services. In this fuzzy context, the INSPIRE-5Gplus platform needs fallback / fail-safes mechanisms that protect shared resources from starvation.

This Use Case solves situations where undetected slice attacks trigger resource starvation in shared infrastructure that affect other critical slices. While the IUC8 don't directly mitigate the threat, it provides damage control to protect shared resources and minimizes the impact on uncorrupted slices. or services.

3.8.2 Actors

- Malicious party (Mallory)
- Mobile Network Operator (MNO):
    - RAN, 5GCore (CP + UP), Mobile Edge

- Legitimate mobile device users (Alpha, Bravo)
- Malicious mobile users (Yankee, Zulu)

3.8.3 Preconditions & basic flow

The main precondition for the IUC8 is that attacks are undetected and un-mitigated by the security enablers.

The attackers need to use un-disclosed security threats or manage to game the deployed security protection.

The direct victim and the indirect targeted slices are sharing the same physical or virtual resources.

The basic flow consists of the following steps (Figure 11):

1. Two services (A and B) are running inside a 5G core on the users' data path. The resources allocated to these two services are (logically) isolated in two respective slices that span from the devices, the RAN domain, to the Core Domain of the MNO infrastructure. These services are associated to specified SLAs.
2. The malicious party (Mallory) triggers an attack from compromised devices bound to the slice A. The compromised devices are used to launch a stealthy DDoS attack against service A;
3. The currently deployed security assets (e.g., firewall, IDS) are unable to (timely) distinguish the malicious traffic from legitimate traffic;
4. The attack affects the service's SLAs of slice A, which leads the system to trigger repeated auto-scaling operations, such as a scale-up (i.e., increasing resources for the VNF) or a scale out (i.e., increasing the number of VMs serving the VNF) to deal with performance degradation;
5. The repeated auto-scaling operations may result in exhaustion of resources shared with slice B: CPU, memory, network queues, application caches, disk I/O, file descriptors, etc. For example, the resource blocks managed by the RAN can be depleted in favour of the malicious slice;
6. A damage control component should then minimize the impact on the slice B by validating and potentially blocking the new resource allocations and emit stricter policies on the wild service with the constraint to preserve the SLAs.

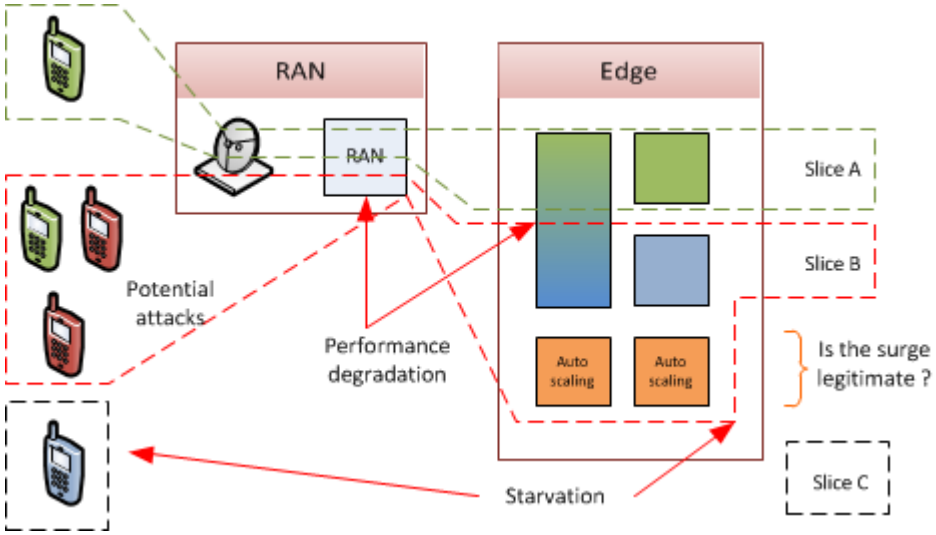


Figure 11 - UC diagram

3.8.4 Success criteria

The main success criteria are:

- The legitimate service's SLA are maintained.
- The resource starvation for critical or new-coming service is minimized.
- Over protection when a legitimate surge in resources consumption happens is avoided.
- The operator is notified and/or the security attack model is kept for future preventions

3.8.5 Use case summary

The main goal is to protect shared resources within slices under un-mitigated DDoS attack. In addition, provide a damage control mechanism to avoid resource starvation during undetected and un-mitigated attacks. It demonstrates the protection of resources in the event of over provisioning under an unmitigated (D)DoS attack. This over provisioning is created by the self-scaling ability of the infrastructure that horizontally scales the used resources attached to a slice to cope with the demand. The proposed mitigation: the protection of shared resources by harnessing the previous automation will be enacted by the ZSM closed loop (Section 2.1). To define what resources are critical enough to be protected, the ICU8 use case may need to tap into the SSLAs and Policy Management (Section 2.7) in order to sort priorities among slices. Finally, the predictive analytics techniques explained in Section 2.4 may help the ICU8 forecast the resources depletion and acts pre-emptively.

3.9 IUC9 - Security posture assessment and threat visualization of 5G networks

3.9.1 Problem description

The 5G infrastructure, services and assets result in complex multi-domain networks. The multi-domain nature of 5G networks increases their complexity increasing the difficulty of assessing their security posture. Additionally, the security posture of 5G networks is affected by human actors, policies and existing mitigation mechanisms. To properly assess the security of a 5G network, a security analyst needs to able to model all the components of the network.

In this test case, we present a software-aided process to facilitate the security assessment process of 5G network using the open source tool DiscØvery. This test case was derived from the 5G-CARMEN project[12]. 5G-CARMEN is focused on the Bologna-Munich corridor. The objective of 5G-CARMEN is to leverage 5G advances to provide a multi-tenant platform than can support the automotive sector. The aim is to deliver safer, greener, and more intelligent transportation with the ultimate goal of enabling self-driving cars. The test case is based on the Back Situation Awareness use case of 5G-CARMEN. In the Back Situation Awareness, the 5G-CARMEN promotes extended situation awareness by enabling vehicles and infrastructure to share the perception of the environment.

The following figures show the main components of the use case. The EmV communicates with the BSAF application through the MEC platform. The MEC platform hosts an instance of a BSAF application in the form of a container.

[12] https://5gcarmen.eu

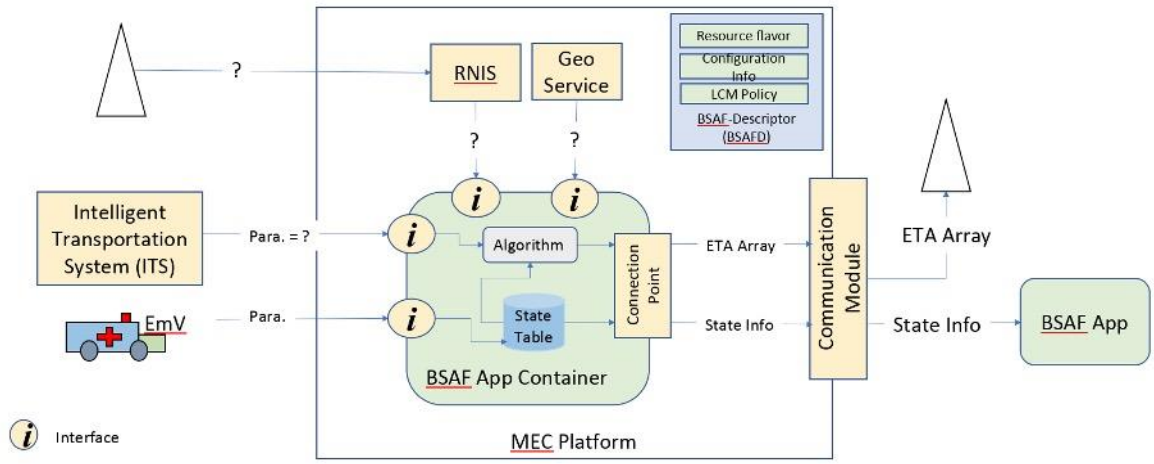


Figure 12 - IUC 9 diagram

3.9.2 Actors

The following actors are part of this use case (Figure 12):

- Vehicles A, B, and C
- Emergency Vehicle
- Malicious Actor
- Service Provider
- Mobile Network Operators

The Vehicles A, B and C are connected vehicles. The emergency vehicle is a connected vehicle capable to drive in emergency mode, such as an ambulance, a police vehicle or and an emergency response vehicle. The malicious actor is an actor that aims to compromise the 5G network. The Service Provider is the actor that provides the Back Situation Awareness service. The Mobile Network Operator is provider of the 5G network connectivity.

3.9.3 Preconditions & basic flow

The functional architecture of the test case is divided into the following components:

- The desktop application DiscØvery: is the application that will be used to perform security analysis on the 5G network. DiscØvery supports several algorithms and features for facilitating the assessment of a 5G network's security posture.
- DiscØvery's model generation algorithms: the algorithms that be used to automatically generate the components of a 5G network.
- DiscØvery's cyber-security insights: a list of custom suggestions and insights that are result of DiscØvery's automated security analysis processes. The insights are based on the unique characteristics of a network.
- A description of the 5G network under analysis: the description will include a detailed enumeration of the components of the 5G network, its assets, its security mechanisms and policies. The list will be used to create the components model of the 5G network that cannot be detected with the DiscØvery's automated algorithms. This information includes high-level policies, actors and assets.
- Network information from the 5G network under analysis: network capture files contain crucial information that can be used by DiscØvery's algorithms to automatically create

network models.

The use case will evaluate the features and functions of the software tool DiscØvery. DiscØvery is cross-platform desktop tool. It can be installed in the form of an application on Windows, MacOS and most Linux-bases distros. The compile the tool from its open source code, it requires the node.js runtime installed on the host system.

The Back Situation Awareness will have the following steps:

- Initial Condition: Connected vehicles A, B, C and the Emergency Vehicle are moving on a highway.
    - Vehicles B, C are on the right lane at moderate speed (90-100km/h) with some distance between them (e.g. 100m)
    - Vehicle A approached on the left lane (10 -20 seconds away) moving a bit faster (110 - 130 km/h, eventually overtake)
    - Emergency Vehicle is about 20 - 30 seconds away from Vehicle A at 130 km/h
- Event: Emergency Vehicle turns its emergency state on (electronically); DENM notification are sent periodically
    - This triggers an emergency vehicle warning with the Estimated Time of Arrival (ETA)
- Reaction: The overtaking lane needs to be cleared by the cooperative vehicles, therefore
    - Vehicle A needs to shift lane and the slowdown to a moderate speed
    - Depending on the ETA and speed differences:
        - ETA much bigger than overtaking time: Vehicle A ends the overtake
        - ETA much smaller than overtaking time: Vehicle A shifts lane and ques behind Vehicles B, C
        - ETA in between: Vehicles B, C keep on the right lane, and do a cooperative lane merge with Vehicle A
- Conclusion: Emergency Vehicle passes undisturbed on the cleared overtaking lane

The use case ends successfully once the emergency vehicle passes undisturbed after the Vehicles A, B, and C have cleared the overtaking lane, without being affected by the attempts of the malicious actor to compromise the 5G network.

3.9.4 Success criteria

The use case will measure the following criteria based on performance indicators:

- Automated model generation: DiscØvery's automated model generation algorithms are able to model only the network layer of a 5G network. Security policies or certain security mechanisms cannot be elicited by network information. For that reason, models automatically generated by network data will not represent all the components of the network. The aim is to identify the percentage of the actual network that can be modelled automatically.
- Automated vulnerability assessment: The automated assessment of network's vulnerabilities can result to vulnerabilities that cannot impact the system. For example, the attack vector for a vulnerability is not materialized in the network and the vulnerability cannot be exploited. It will measure the percentage of identified vulnerabilities that can be to used exploit the network.
- Automated threat identification: The automated identification of threats can result to threats that are may be out of scope of the network's security requirements. It will measure the

percentage of the threats that are necessary for the networks to be protected.

- Cyber security insights assessment: The derived cyber-insights may be addressed by existing security mechanisms or may be considered out of scope. It will measure the percentage of the cyber-insights that were used to improve the security posture of a 5G network.

3.9.5 Use case summary

The use case focuses on reducing the complexity of assessing the security posture of 5G networks. 5G networks are composed by several virtualized assets that provide services to end users and other service consumers. To facilitate the security analysis process, we provide a modelling language to express the assets 5G network for security assessment. The modelling language provides concepts to express users, service providers, policies and other concepts to describe the necessary components of a network that affect its security. Once a 5G network has been modelled, a security analyst will be able to deploy automated functions for assessing security. Example of such automated functions are, threat and vulnerability identification, suggestions for security policies and insights for security mechanisms

It demonstrates a cross-border situation awareness 5G scenario derived from the 5G-CARMEN project. The security assessment of the scenario will be supported by enablements from Artificial Intelligence (Section 2.3) and Advanced Cybersecurity techniques (Section 2.4) to facilitate the security analysis. The analysis will make use of software-aided techniques, as well as expertise of security analysts to provide a holistic view of the security posture of the scenario. The outputs of the security assessment will be assisted by enablements of the SSL and Policy Management (Section 2.7) as suggestions and policies to improve the security posture of the scenario.

3.10 IUC10 - Secure and privacy enabled local 5G infrastructure

3.10.1 Problem description

Local 5G network service providers may deploy their network infrastructure including the both BS and backhaul networks. Edge computing services are deployed closer to the IoT nodes for local data processing. IoT tenants offer various smart services or contents based on the data collected by IoT devices. IoT tenants may lease the networking and computational resources, and data processing services from multiple service providers/operators. The network slice provider may form a network slice by a brokering mechanism that allows different service providers/operators to come to a common platform and formulate a network slice.

We intend to use a hierarchical Blockchain network to develop a secure and privacy enabled federated slice brokering mechanism for IoT tenants under the umbrella of a multi operator platform. In our solution federation refers to the orchestration of services (i.e., network functions, computational resources, etc.) offered by multiple local operators. When an IoT tenant initiates a request for a particular service demanding a set of resources, it's the duty of the federated slice broker to orchestrate the life-cycle of the network slice in a secure, automated and scalable manner. In this case the slice broker performs as a mediator between IoT tenants and the local 5G operators. The key objective is to utilize the infrastructure offered by local operators in a secure way while protecting the privacy. This use case is referring the test case TC9 described in D5.1.

IoT tenant cluster represents a collection of IoT nodes and edge computing nodes that are restricted to a limited geographical area. Brokering mechanism maintains a common queue to store the past and anticipated service/resource requests emerging from the clients, the possible E2E slice formation that fulfils their requests, availability of networking and computing resources at the providers, traffic status, etc. Operator/Service provider cluster (Infrastructure cluster) denotes the virtual/physical resource/infrastructure providers which are also considered as local operators (Figure 13).

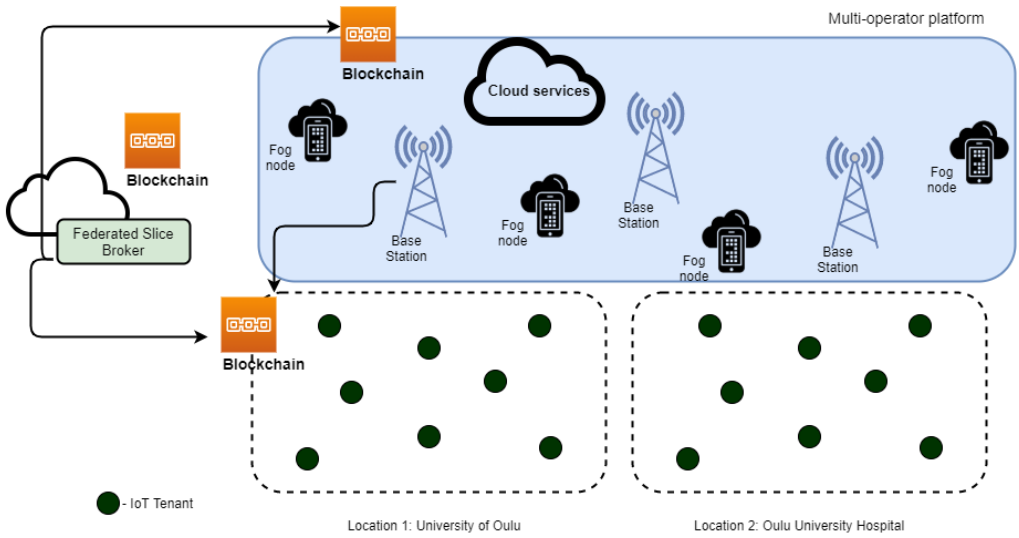


Figure 13 - Use case diagram

Based on the tenant request, received from IoT tenant, the broker will create a network slice that fulfils the requirements of the requested 5G services. This can be a multi-operator end-to-end slice where network and computation resources can be provided by different operators.

3.10.2 Actors

- IoT tenants
- Fog nodes
- Mobile Network Operator (MNO) /Local operator

3.10.3 Preconditions & basic flow

MNOs/Local operators should provide the available network/computation resources and their current status via the respective network slice managers. In addition to that, a reputation metric is assigned to each MNO and this value is taken based on the inputs given by the SSLA manager. These records are stored in a database maintained by the network slice broker. [1] The storage of these records in the blockchain network is intended to perform in a privacy preserved manner.

IoT tenants create the individual service/resource requests to fog nodes. An additional security service is provided by the slice broker to eliminate the possible DoS/DDoS attacks at this point.

Based on the demand asked by the IoT tenants, Fog nodes initiate the resource requests, create the network slice template using secure and federated slice brokering (SFSB) mechanism and broadcast the slice request to MNOs/ local operators.

SFSB mechanism maps the best match for a particular resource request with the network slice offer given by the respective resource providers.

Fog nodes grant access IoT tenants to consume the slice upon selection by the brokering framework.

3.10.4 Success criteria

Separate private permissioned Blockchains are maintained to keep the records among IoT tenant clusters, at brokering mechanism and among local operators.

3.10.5 Use case summary

The use case aims to use network slice brokering service to provide end-to-end network slices in a

secure, automated and scalable manner under a multi-operator platform. It proposes secure and privacy enabled local 5G infrastructure that support multi-tenant multi-operator scenario in line with the close loop framework by ZSM (Section 2.1). Secure network and resource allocation is performed by the network slice broker developed by DLT (Section 2.5) where the smart contracts are used to activated different functionalities of the slice broker. Secure Slice selection algorithm is designed using AI algorithm (Section 2.3) and the data bases are maintained in a privacy enabling manner. The slice broker communicates with the slice manager of the local 5G operator to receive the resource availability, pricing values, and slice creation. The process is also supported by a DLT based SSLA manager (Section 2.7) service which is running as an additional service on top of the main brokering service. The use case refers the test case TC9 described in D5.1.

3.11 Illustrative Use Cases and Enablements mapping

The list of illustrative use cases introduced in this section showcase all the enablements introduced in Section 2 covering the identified challenges.

	IUC1	IUC2	IUC3	IUC4	IUC5	IUC6	IUC7	IUC8	IUC9	IUC10
ZSM				X	X	X	X	X		X
TEE				X	X					
AI				X		X		X	X	X
ACST			X	X		X			X	
DLT		X	X				X			X
DL & RCA					X		X			
SSLAs & PoI	X		X		X		X	X	X	X

Table 3 - Illustrative Use Case and Enablement Mapping

As a result of the application of the different exposed enablements while analysing the proposed illustrative use cases and others out of the scope of this deliverable, the INSPIRE-5GPlus High Level Architecture is designed and presented next.

4 INSPIRE-5GPlus High Level Architecture

4.1 Design Methodology

An incremental and iterative process for designing INSPIRE-5Gplus framework has been adopted. The design process is taking as reference input the overall concept underpinning the project. In fact, INSPIRE-5Gplus aims to devise and implement a zero-touch end-to-end smart network and service security management framework that empowers not only protection but also trustworthiness and liability in managing 5G network infrastructures across multi-domains [174]. To achieve this goal, the design process starts by investigating the threat landscape and identifying the security requirements for 5G networks (presented in D2.1 [2] and summarized in subsection 4.2.1below). To meet our vision of empowering zero-touch security management, we have also investigated the ETSI ZSM reference architecture specification [3] The architectural functional requirements are then captured from the initial set of UCs (presented in Section 4) as well as the zero-touch security management vision. Those requirements are described in subsections 4.2.2 and 4.2.3, respectively. Based on the knowledge gained from the conducted investigation and the identified requirements, we defined the potential functional blocks that will make up the high-level architecture (HLA) at both the *domain* level and the *End-to-End* level. Sub-section 4.3 presents an overview of INSPIRE-5Gplus framework HLA, describing the main key design principles and features underlying the framework. The design process has then continued by describing the main role of each functional block within the INSPIRE-5Gplus framework HLA and identifying the envisioned services to be provided by each block. The macro-level interactions between the functional blocks at domain or E2E level, or with external entities are defined by specifying the potential consumers of the block's services. Subsection 4.4 details the role of the functional blocks composing the HLA and their respective services. Finally, we specified the closed loop model supported by INSPIRE-5Gplus framework and defined a typical INSPIRE-5Gplus closed loop showing a representative scenario on how the HLA blocks interacts at domain and E2E levels to intelligently and automatically enforce and control security policies. Subsection 4.5 provides details on the INSPIRE-5Gplus closed loop.

The design activities described in the subsequent subsections have been carried out in continuous collaboration between the consortium members involved in the task responsible of designing the INSPIRE-5Gplus HLA (i.e., T2.3) based on the outcomes of WP2's tasks (i.e., 5G security requirements (T2.1), potential enablements (T2.2) and initial set of IUCs (T2.3)). Furthermore, the design activities have been conducted in continuous feedback with technical WPs (WP3, WP4) in charge of developing the security enablers for empowering smart (i.e., intelligent, adaptive and flexible) 5G security (WP3) and liability-aware trusted 5G security (WP4). This continuous collaboration and the gathered feedback have helped in refining the list of requirements, the INSPIRE-5Gplus framework HLA and the supported closed loop. The close cooperation with technical WPs will ensure alignment between design and implementation activities.

Although the design of INSPIRE-5Gplus framework is considered stable from the perspective of the main functional blocks composing the HLA and their role, potential improvements are foreseen, especially with regard to the provided services and their capabilities. In fact, the list of services and their capabilities are likely to evolve based on the envisioned IUCs to cover the trust and liability enablers and the implementation activities in WP3/WP4.

4.2 High Level Architecture Requirements

This section details the requirements that drove the overall INSPIRE-5Gplus framework High Level Architecture (HLA) design. The requirements list has provided guidance to design of WP3 and WP4 security enablers.

We divide the system requirements into Functional and Non-Functional [172].

- Functional Requirements: defines a specification of a behaviour between inputs and outputs (function) of a system or its components.
- Non-Functional Requirements: defines specification criteria that can be used to evaluate the operation of a system. Non-Functional requirements impose constraints on the design or implementation of system such as performance, security or usability requirements.

The HLA design is guided by the following requirement categories:

- The 5G security requirements as identified in D2.1 [2] (summarized in Table 4).
- The requirements for enabling zero-touch liability-aware trustable 5G security management. Those requirements are identified from the initial set of UCs presented in Section 3 as well as the vision of empowering Zero-touch management.
- The elicited requirements derived from the Business and Organizational Questionnaire which is further described in the Appendix A.

The Business and Organizational Questionnaire provided valuable insights that were used to elicit several requirements of this document. The questionnaire was divided into three categories, 1) Business and Organizational requirements; 2) Regulatory compliance and reputation requirements and; 3) Background information. An output of the questionnaire is that the majority of the responders were not satisfied with their existing security infrastructure and called for improvements in several domains, such as third-party application management, virtualization, sandboxing and standard compliance. The questionnaire provided information for the elicitation of non-functional as well as functional requirements. Several non-functional requirements, namely SEC-REQ-[01, 04, 06, 07, 12, 13, 14] that were already anticipated to address specific stakeholders' requirements identified in the questionnaire. Functional requirements, such as FC-REQ-[01, 02, 03, 04, 10, 25, 31, 39] were motivated from inputs from responders of the questionnaire.

4.2.1 5G Security Requirements

Security Req. ID	Security Requirement Description	Requirement Type
SEC-REQ-01	The 5G network shall provide telemetry and other auditing information relevant to the security mechanisms of the system.	Non-Functional
SEC-REQ-02	The 5G network shall only allow authenticated users to consume the services provided by the 5G system.	Non-Functional
SEC-REQ-03	The 5G network shall warrant measurable level of availability of its services to the relevant stakeholders.	Non-functional

Security Req. ID	Security Requirement Description	Requirement Type
SEC-REQ-04	The 5G network shall ensure the necessary network capacity and network resources for the critical operations of the 5G services.	Non-Functional
SEC-REQ-05	The 5G network shall enable a secure platform for vertical services to be deployed.	Non-Functional
SEC-REQ-06	The 5G network shall enable the state management of its platform components.	Non-Functional
SEC-REQ-07	The 5G network shall be able to revert to previous states with minimal service disruption of deployed application in case of malicious compromise.	Non-Functional
SEC-REQ-08	The 5G network's security mechanisms should not impact the functional requirements of critical operations for vertical applications.	Non-Functional
SEC-REQ-09	The security mechanisms of the 5G network shall be able to be deployed in any potential 5G hardware provider without any impact on their performance or functionality.	Non-Functional
SEC-REQ-10	The security mechanisms of the 5G network shall be able to measure/evaluate trust level of its components and platforms and share this information with verticals in a safe and trustable way.	Non-Functional
SEC-REQ-11	The security mechanisms used in a complex 5G ecosystem shall be able to identify, distribute and allocate responsibilities between 5G ecosystem stakeholders.	Non-Functional
SEC-REQ-12	The 5G ecosystem shall be able to publish security KPI measuring the compliance of stakeholder with their Security Level Commitments.	Non-Functional
SEC-REQ-13	Technologies used to distribute over 5G ecosystem (end to end) and evaluate post security incident root cause of failure are trustable.	Non-Functional
SEC-REQ-14	The 5G system must provide security mechanisms to ensure that user (and endpoints) data are securely processed and stored wherever it is processed or stored. Both confidentiality and integrity guaranties shall be brought all along the full lifecycle of the data in transit, process and storage.	Non-Functional

Table 4 - 5G security requirements

4.2.2 UCs-related Requirements for Zero-Touch Liability-aware Trustable 5G Security Management

The functional requirements captured from the initial set of UCs are summarized in Table 5.

Functional Req. ID	Architectural Requirement Description	IUC1,2	IUC8	IUC3	IUC4	IUC5	IUC6	IUC7	IUC10	IUC9
FC-REQ-01	INSPIRE-5Gplus framework shall support the capability to collect up-to-date telemetry data.	X	X					X		
FC-REQ-02	INSPIRE-5Gplus framework shall support the capability to specify the SSLA to detect security breaches and assess security functions.	X	X	X					X	
FC-REQ-03	INSPIRE-5Gplus framework shall support the capability to ensure the SSLA during run-time.	X								
FC-REQ-04	INSPIRE-5Gplus framework shall support the capability to allow multi-domain interaction.	X						X	X	
FC-REQ-05	INSPIRE-5Gplus framework shall support the capability to ensure only validated/certified resources should be used.	X							X	
FC-REQ-06	INSPIRE-5Gplus framework shall support the capability to perform anomaly prediction based on the required KPIs of the managed network slices		X							
FC-REQ-07	INSPIRE-5Gplus framework shall support the capability to monitor different structured data (network, operating systems, applications, nsi).			X			X	X		
FC-REQ-08	INSPIRE-5Gplus framework shall support the real-time assessment of SSLAs.			X						
FC-REQ-09	INSPIRE-5Gplus framework shall support the generation of alerts that can be processed by the Security Orchestrator.			X						
FC-REQ-10	INSPIRE-5Gplus framework shall support the translation of high-level policies to verifiable SSLAs and actionable remediations.			X						
FC-REQ-11	INSPIRE-5Gplus framework shall support advanced techniques (e.g., ML) to classify and detect anomalies				X					

Functional Req. ID	Architectural Requirement Description	IUC1,2	IUC8	IUC3	IUC4	IUC5	IUC6	IUC7	IUC10	IUC9
	in encrypted traffic.									
FC-REQ-12	INSPIRE-5Gplus framework shall support passive access to continuous up-to-date traffic in the network.				X		X			
FC-REQ-13	INSPIRE-5Gplus framework shall support the capability to store telemetry data (or to steer their appropriate storage).				X		X			
FC-REQ-14	INSPIRE-5Gplus framework shall support the capability to (pre-) process and filter the telemetry data, and to perform cross-domain data aggregation.				X		X			
FC-REQ-15	INSPIRE-5Gplus framework shall support the capability to automatically deploy virtualized network functions software. (including virtualized security functions)					X	X	X		
FC-REQ-16	INSPIRE-5Gplus framework shall support automatic configuration of virtualized network function parameters. (including virtualized security functions)					X				
FC-REQ-17	INSPIRE-5Gplus framework shall support the capability of automatic verification of virtualized network functions normality after deployment.					X	X	X		
FC-REQ-18	INSPIRE-5Gplus framework shall support the capability to specify security policies.					X	X			
FC-REQ-19	INSPIRE-5Gplus framework shall support the capability to define the security policies in a technology independent policy definition language.					X	X			
FC-REQ-20	INSPIRE-5Gplus framework shall support the capability to at least store, delete, activate and deactivate security policies.					X	X	X		

Functional Req. ID	Architectural Requirement Description	IUC1,2	IUC8	IUC3	IUC4	IUC5	IUC6	IUC7	IUC10	IUC9
FC-REQ-21	INSPIRE-5Gplus framework shall support the capability to manage the defined security policies.					X	X	X		
FC-REQ-22	INSPIRE-5Gplus framework shall support the capability to detect security policy conditions. (we need to elaborate a bit what we mean by policy conditions)					X	X	X		
FC-REQ-23	INSPIRE-5Gplus framework shall have the capability to decide on security policy execution.					X	X	X		
FC-REQ-24	INSPIRE-5Gplus framework shall support the capability to trigger the actions defined in the security policies.					X	X	X		
FC-REQ-25	INSPIRE-5Gplus framework shall have the capability to detect conflicting security policies.					X		X		
FC-REQ-26	INSPIRE-5Gplus framework shall support the interoperation with the NFV MANO APIs for management of NFV network services.					X	X	X		
FC-REQ-27	INSPIRE-5Gplus framework shall support the collection of data on network slices status.						X			
FC-REQ-28	INSPIRE-5Gplus framework shall support the capability to take action to mitigate performance degradation due to security issues.						X			
FC-REQ-29	INSPIRE-5Gplus framework shall support automated management for compute, storage and network resources, VNFs, slices and services for an automated MTD operation.						X			
FC-REQ-30	INSPIRE-5Gplus framework shall support the detection of abnormal behaviours of the managed networks and services.						X			

Functional Req. ID	Architectural Requirement Description	IUC1,2	IUC8	IUC3	IUC4	IUC5	IUC6	IUC7	IUC10	IUC9
FC-REQ-31	INSPIRE-5Gplus framework shall support the capability to govern collected telemetry data.						X			
FC-REQ-32	INSPIRE-5Gplus framework shall support the capability to common access to the collected up-to-date telemetry data.						X			
FC-REQ-33	INSPIRE-5Gplus framework shall support stepwise introduction of ML-based management.						X			
FC-REQ-34	INSPIRE-5Gplus framework shall support the capability to store historical data needed for the prediction and analytics.						X			
FC-REQ-35	INSPIRE-5Gplus framework shall support the collection of data from ZSM managed entities to perform automated network and service security management based on AI.						X			
FC-REQ-36	INSPIRE-5Gplus framework shall provide cyber security insights that would be valuable to a security analyst.									X
FC-REQ-37	INSPIRE-5Gplus framework shall support the automation of security assessment based on identified vulnerabilities.									X
FC-REQ-38	INSPIRE-5Gplus framework shall support the threat identification based on best practices, network configurations, user activities.									X
FC-REQ-39	INSPIRE-5Gplus framework shall support the use of network related information to elicit its components and other relevant information for security analysis.						X			X

Table 5 - Functional Requirements from initial set of Use Cases

4.2.3 Requirements related to management principles

In addition to the requirements captured from UCs, in this subsection, we elicit additional functional requirements that allow enabling zero-touch security management in compliance with ZSM specification (Table 6).

Zero-touch Sec. Mgmt. Fct. Req. ID	Security Requirement Description
ZFC-REQ-01	INSPIRE-5Gplus framework shall support the capability of identifying root cause of a security incident in the network based on the analysis of collected data.
ZFC-REQ-02	INSPIRE-5Gplus framework shall support automated management (i.e., detection, identification, prevention and mitigation) of security incidents/attacks.
ZFC-REQ-03	INSPIRE-5Gplus framework shall support automated security management based on AI/ML techniques.
ZFC-REQ-04	INSPIRE-5Gplus framework shall support closed-loop security management.
ZFC-REQ-05	INSPIRE-5Gplus framework shall support open interfaces.
ZFC-REQ-06	INSPIRE-5Gplus framework shall support access control to services exposed by the security management domains.
ZFC-REQ-07	INSPIRE-5Gplus framework shall support security management of end-to-end services that cross boundaries between multiple domains.
ZFC-REQ-08	INSPIRE-5Gplus framework shall support bounding the automated decisions-making by the established SSLA and security policies.
ZFC-REQ-09	INSPIRE-5Gplus framework shall support the capability to register the security management services provided.
ZFC-REQ-10	INSPIRE-5Gplus framework shall support the capability to discover the security management services provided.
ZFC-REQ-11	INSPIRE-5Gplus framework shall support the capability to invoke the discovered security management services.
ZFC-REQ-12	INSPIRE-5Gplus framework shall support the capability of communication between the security service producers and the security service consumers.
ZFC-REQ-13	INSPIRE-5Gplus framework shall support the capability to check/validate the integrity of telemetry data.

Table 6 - Functional requirements enabling zero-touch management

4.2.4 Overall HLA Requirements

In this section, the identified requirements are classified according to six (06) classes representing the main categories for advancing 5G security assets, as identified in WP3 and WP4:

- **AI/ML driven Security Management**: this category explores the AI and ML models and techniques that can be used to advance 5G security.
- **E2E ZSM Security Management**: this category focuses on the automation of E2E security management and slicing based on Software-Defined Security and SECaaS paradigms.
- **Security Enforcement & Control**: this category is related to the previous one; it leverages Software-Defined Security (SD-SEC) to enforce security policies and SSLAs that are needed to be managed in a flexible, optimal and autonomic way.
- **Security Analytics**: this category explores the usage of data analytics and efficient AI and ML driven mechanisms for detecting threats in 5G networks, coming from the network elements and heterogeneous probes distributed across the 5G infrastructure (RAN, CN, TN).
- **Security Data Collection**: this category is important for the previous one since data collection is needed for analytics. It also explores ML relevant techniques for data usage.
- **Trust & Liability**: this category explores the techniques required to establish trust and liability.

The proposed classification (See Table 7) will serve as guidance to the design of WP3 and WP4 security enablers that will provide the services of INSPIRE-5Gplus framework, leveraging the potential of enablements presented in this deliverable.

Category	Related Non-Functional Requirements	Related Functional Requirements
AI/ML driven Security Management	S04, S05	F06, F07, F09, F11, F17, F23, F28, F29, F30, F33, F35, Z03
E2E ZSM Security Management	S05, S06, S07, S12	F02, F04, F09, F10, F15, F16, F17, F18, F19, F20, F21, F22, F23, F24, F25, F26, F28, F29, F36, F37, F38, F39, Z02, Z03, Z04, Z05, Z06, Z07, Z08, Z09, Z10, Z11, Z12
Security Enforcement & Control	S02,S05, S08, S09, S14	F05, Z13
Security Analytics	S04, S03, S06, S12	F03, F06, F07, F08, F09, F11, F17, F30, F35, F39, Z01
Security Data Collection	S01, S08, S09	F01, F07, F11, F12, F14, F27 F30, F31, F32, F35, F39, Z03
Trust & Liability	S10, S11, S13	F13, F36, F37, F38, Z13

Table 7 - Overall HLA Requirements (SXX -> SEC-REQ-XX, FXX -> FC-REQ-XX, ZXX -> ZFC-REQ-X)

4.3 Overview of INSPIRE-5Gplus Framework HLA

The main goal of INSPIRE-5Gplus is to devise and implement a zero-touch end-to-end smart network and service security management framework that empowers not only protection but also trustworthiness and liability in managing 5G network infrastructures across multi-domains. Guided by this overall objective and the set of requirements (See Section 4.2) that we have captured to meet this goal, we identified the main functional blocks composing INSPIRE-5Gplus framework HLA (see Figure 14) and the initial set of services to be provided by each functional block. To achieve our vision of empowering zero-touch security management, INSPIRE-5Gplus framework follows the key principles of ETSI ZSM reference architecture[3] (presented in Section 2.1 by supporting the separation of security management concerns and adopting a service-based architecture where the provided security services are exposed and consumed through the integration fabric. Indeed, the INSPIRE-5Gplus framework is split into several *security management domains* (*SMDs*), for robustness, but also to support the separation of security management concerns, e.g. for the Radio Access Network (RAN), Edge or Core Network. Each SMD is responsible for intelligent security automation of resources and services within its scope, and comprises a set of functional modules, e.g. a Security Data Collector, a Security Analytics Engine, a Decision Engine, a Security orchestration, Trust Management as well as Policy and SSLA Management. The various security management services provided by these modules are exposed within the same domain but also cross-domain through an *integration fabric*. A special SMD – the E2E SMD – is used to manage security of E2E services (e.g. E2E network slice) that span multiple domains. The decoupling of the E2E security management domain from the other domains allows escaping from monolithic systems, reducing the overall system's complexity, and enabling the independent evolution of security management at both domain and cross-domain levels. The functional modules operate in an *intelligent closed-loop* way to enable *AI-driven software defined security (SD-SEC)* orchestration and management in compliance with the expected Security Service Level Agreement (SSLA) and regulatory requirements. By adopting service-based and SD-SEC models, INSPIRE-5Gplus framework allows to build up sustainable security measures that can adapt to dynamic changes in threats landscape and security requirements in next-generation mobile networks. [174]

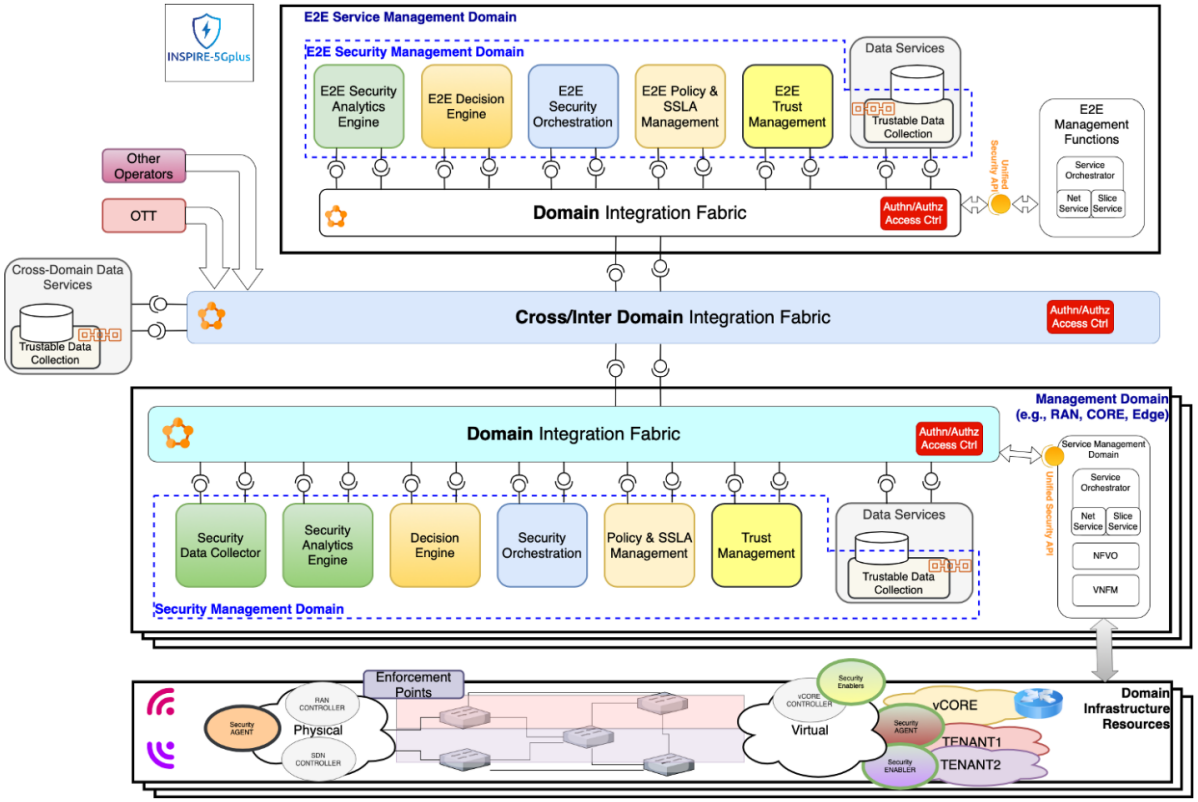


Figure 14 - INSPIRE-5Gplus' High-Level Architecture

4.4 HLA's Functional Blocks Description

4.4.1 Security Data Collector

4.4.1.1 Function

The main function of the Security Data Collector (SDC) is to gather all the data coming from the security enablers at the domain level, needed by the security management functions (e.g., Security Analytics Engine). The types of data collected by the SDC may include:

- Performance monitoring data (e.g., counters and statics data);
- Security monitoring data (e.g., traffic meta-data, packet capture, session data);
- Event/alarm data (e.g., system logs, application traces, system traces);
- Machine learning reference data sets;
- External data (e.g., Cyber Threat Intelligence, external data sets).

4.4.1.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Data Collection Service	This service sets up and launches the mechanisms for collecting data from the different security agents, security enablers and network devices.	Data translation	External/Internal	• Security Analytics Engine • Policy & SSLA Management
		Data fusion/aggregation		
		Data extraction or filtering		
		Data temporal persistence and transaction		
		Data capture		

Table 8 - Services provided by Security Data Collection Module.

4.4.2 Security Analytics Engine

4.4.2.1 Function

The main function of the Security Analytics Engine (SAE) is to derive insights and predictions on a domain's security conditions based on data collected in

that specific domain or even from other domains. In the context of INSPIRE-5Gplus, the SAE provides Anomaly Detection and Root Cause Analysis (RCA) services. The Anomaly Detection service has the capabilities of detecting and/or predicting anomalous behaviours due to malicious or accidental actions by identifying patterns in data or behaviour that do not conform to the expected normal behaviour. It leverages data aggregated by the SDC from the managed entities of the domain, including performance and security monitoring data, events and alarms, generated by system logs and packet traces. The RCA service identifies the cause of the observed security incidents by analysing and correlating data from other services (e.g. Anomaly Detection service). The Root Cause determines the origin of the anomaly and the location in the network where a corrective action should be applied to prevent the problem from occurring. As a result, the RCA service may provide recommended actions to correct or prevent the security incidents in a 5G environment.

4.4.2.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Anomaly Detection Service	This service has the capabilities of detecting and/or predicting anomalous behaviours due to malicious or unintentional actions.	Publish results to subscribers Notify consumers of detected anomalies	External/Internal	• Domain Decision Engine • Domain Data Services • Operators
Root Cause Analysis Service	This service identifies the cause of the observed security incidents by analysing and correlating data from other services (e.g., Anomaly Detection Service) and learning from past experience.	Publish results to subscribers Notify consumers of probable causes of security incidents	External/Internal	• Domain Decision Engine • Domain Data Services • Operators

Table 9 - Services Provided by Security Analytics Engine Module.

4.4.3 Decision Engine

4.4.3.1 Function

The Decision Engine (DE) functional block oversees the different actions emitted by the security assets and the SAE to select the best decisions which can be applied for securing a running targeted service. This central component acts as an arbitrator between security assets and the rest of the platform that manages domains.

The DE delegates the creation of actual mitigation actions to **Cognitive Long-Term** and **Reactive Short-Term** assets. These assets contain the algorithms to build a coherent mitigation plan given a detected threat:

- The Cognitive Long-Term assets will be based on advanced AI techniques and may use historical data from several sources to internally deduce correlations, potential forecasts and propose elaborated mitigation plans to the DE.
- The Reactive Short-Term assets will rely on simple rules to provide quick and mundane reactions to specific events. These rules will be akin to what a human operator would do in the given a situation. Due to their simple and streamlined structure, the mitigations resulting from these assets can be rapidly computed and enacted.

The DE relies on multiple "third-party" assets running concurrently and waits for them to emit a mitigation decision. These decisions can then be transmitted to the Decision Engine without following any given order and sometimes may even be conflicting. For example, a Reactive Short-Term asset may evaluate a device as legitimate and thus authorise its traffic. On the contrary, a Cognitive Long-Term asset may later identify that this same device as a potential DDoS source. In such situation, the DE has to arbitrate the conflicting reactions either by using a confidence level and/or by looking at a statistically built priority list. Finally, as mitigation may take time to be applied by the underlying Security Orchestrator, the DE has to track selected reactions and may ignore newly received mitigation decisions to let the protected system to stabilize.

4.4.3.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Security Decision Service	This service manages decisions inside a domain. A decision is a set of securities policies to be applied when some kind of an alert is triggered. The DE should generate this policies either using basic hard-coded rules or through complex ML techniques.	Create/Update/Delete/List a security policy decision Trigger a decision (from an underlying alert)	Internal	• Security Enablers • Security Analytic Engine (push mode)
Security Decision Priority Service	This service allows a human operator (eventually a security enabler with a feedback loop) to set the priorities attached to registered decisions. As the framework may contain multiple potentials decisions for a given threat, the DE needs a way to prioritize them for selection. For now, such service can be implemented as a simple ordered list but we can suppose that an enabler / an extension to the DE could provide the selection of the best mitigation. For example, a decision using forecast to infer	Create/Update priorities on decisions. Provide a read API for (optional) external GUI	External/Internal	• External UI / Operator • E2E Decision Engine

	the system in 2 hours, may think that the system is going to enter a low volume period and proactively trigger a scale down on resources. Whereas, a decision done in the present state may keep the amount of resources large due to a high usage.			

Table 10 - Services provided by Decision Engine module.

4.4.4 Security Orchestrator

4.4.4.1 Function

The Security Orchestrator (SO) oversees the different security enablers to enforce the security requirements specified by the adopted security policies. The SO drives the security management by interacting, through the integration fabric, with different SDN controllers, NFV MANO and security management services. The SO will enforce proactively or reactively the security policies through the allocation, chaining and configuration of virtual network security functions (VSF), such as virtual Intrusion Detection System (vIDS), vFirewall, virtual Authentication, Authorization and Accounting (vAAA). The SO will be fed with the evolving system model, that is derived from the structural information coming from the network administrators the monitors that inspect the deployment for any changes, the trust and reputation indicators coming from the Trust Management (TM) component, as well as the insights and evolved plans inferred by the DE. This cognitive behaviour will provide self-healing and self-protection capabilities to the entire managed system, allowing the orchestrator to react automatically according to the actual context, and timely trigger the adequate countermeasures to mitigate the ongoing attacks or prevent foreseen threats. Potential reactions encompass, among other, applying security policies to control the traffic (e.g. by dropping or diverting it) through an SDN controller, and deploying, decommissioning, re-configuring or migrating the VSFs.

4.4.4.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Security Policy Enforcement Service	This service enforces and controls security policies for the Domain. It ensures to deploy the necessary security policies.	Create security policy Enforce security policy Enforce MTD policy	Internal/External	• Decision Engine • E2E Security Orchestrator

Table 11 - Services provided by Security Orchestrator module.

4.4.5 Policy and SSLA Management

4.4.5.1 Function

The Policy and SSLA Management (PSM) component transforms the abstract Protection Level and Security Level requirements and constraints expressed by consumers and providers into specific parameters that indicate, to the Security Orchestrator, the security services to configure, deploy and manage. The PSM provides a framework defining the language and semantics to define Security Service Level Agreement (SSLAs) based on policies. These policies will be refined from a high abstraction level description to deployment-ready representations. These values will finally be enforced in real time in cooperation with other INSPIRE-5Gplus functions. The SSLAs provide the means to specify the security requirements or policies and the means for assessing or enforcing their fulfilment to obtain the desired security level.

4.4.5.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
HSPL Refinement Service	This service refines HSPL (High-level Security Policy Language) policies into MSPL (Medium-level Security Policy Language) policies.	Convert	Internal	• Security Orchestrator
MSPL/TOSCA Refinement Service	This service refines MSPL policies into precise configurations, API calls, specific low-level configurations needed to interact with the enablers. It could also translate MSPL to TOSCA to be compatible with some orchestrators (e.g., OSM, ONAP) that support TOSCA.	Convert	Internal	• Security Orchestrator
Security Policy Storage Service	This service stores policies enforced by other domain entities to keep track of them. It could be implemented using DTL to assure liability.	Store	Internal	• Decision Engine • Security Orchestrator

Table 12 - Services provided by Policy & SSLA Management module.

4.4.6 Trust Management

4.4.6.1 Function

The Trust Management (TM) contains various internal services for the trust related functions in the INSPIRE-5Gplus security framework. It provides services for trust and reputation calculation (at the component or slice level) as well certification based on trust metrics. For trust in how data flows traverse a network and how they are processed spatially, its Ordered Proof of Transit (oPoT) service verifies the correct order of nodes on the network path followed by a flow. The TM also provides a wrapper service that produces the modifications on the binaries (executable files) delivered by an obfuscation-based protected security routine embedded and added on the protected program. A metadata file or data structure is enclosed in the protected VNF package and describes the various security functions applied with their parameters.

4.4.6.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Trust Reputation Manager	This service assigns trust and reputation values to monitored 5G entities and provides this information to security management entities and end users in 5G virtualized networks	Compute trust and reputation	Internal/external	• Security Orchestrator
Component Certification Service	This service works at the component level and provides a static evaluation of different 5G network components by measuring trust metrics.	Certificate components using trust metrics	Internal/external	• Security Orchestrator
Slice Trustworthiness Service	This service ingests slice-related data (static and dynamic properties) and scores the slice, based on parameters that can be used by the end-users or other system components.	Compute slice trust score	Internal/external	• Security Orchestrator
Ordered Proof of Transit Service	This service verifies the correct order of nodes on the network path followed by a flow. It provides trust in the guaranteed confinement of flows in a specific slice or slices, or for inter-domain trust.	Compute network path verification	Internal	• Security Orchestrator

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Trust Manager Service	This service calculates the trust and reliability of a cloud infrastructure or the services deployed on it, based on multiple values for both the infrastructure and the services. It is designed as a smart contract.	Calculation of Trust	Internal/External	• Security Orchestrator
Wrapper Service	This service produces the modifications on the protected binaries with the aim of hardening the code against confidentiality, integrity, illicit usage and vulnerability exploits risks.	Protection of binaries for confidentiality and integrity against modification, illicit usage and vulnerability exploits	Internal/External	• Security Orchestrator

Table 13 - Services provided by Trust Management module.

4.4.7 E2E Security Analytics Engine

4.4.7.1 Function

The E2E Security Analytics Engine (E2E SAE) derives cross-domain insights and predictions based on data collected from different domains. It has a role similar to the SAE but at the cross-domain level. This function is necessary for analysing the data provided by the SDCs from different domains or stored in the Cross-Domain Data Service to detect any anomalies that can only be detected using information from more than one domain (e.g. SIEM-type analysis that correlates events captured in logs). It generates notifications that will be used by E2E Decision Engine to trigger the necessary remediation or prevention procedures.

4.4.7.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Anomaly Detection Service	This service analyses the data provided by the different domain SDCs or stored in the E2E Data Service to detect anomalies that can only be detected using information from more than one domain. Similar to a SIEM (Security Information Management System).	Complex event processing Policy compliance analysis	External	• E2E Decision Engine

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Root Cause Analysis	Similar to the RCA service defined in DE but operates at E2E level to identify cascading effects between different domains.	Publish results to subscribers Notify consumers of probable causes of security incidents	External/Internal	• E2E Decision Engine • E2E Data Services • Operators

Table 14 - Services provided by E2E Security Analytics Engine module.

4.4.8 E2E Decision Engine

4.4.8.1 Function

The E2E Decision Engine (E2E DE) manages the high-level security at the E2E level. This component consumes events from the E2E SIE or from the underlying domain-level DE to adapt and propagate the security decisions across multiple domains. The E2E DE contains at least the same service as the Domain DE.

4.4.8.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Security Decision Synchronization Service	This service synchronizes the decision taken by the DE at domain level with the E2E DE for further validation and optimization.	Push applied domain decision in the E2E domain	Internal	• Domain Decision Engine
Security Decision Service	Similar to the service defined in the Domain DE but operates at E2E level. Inside the E2E domain scope, some security enablers may receive data from several underlying remote domains and using this global view, they generate events for the E2E Decision Engine.	See Domain DE	See Domain DE	• Security Enablers • E2E Security Analytics Engine • E2E Security Analytics Engine

	Given this aggregated alert, the E2E Decision Engine will have to generate and split a "global" mitigation between the concerned remote domains. Moreover, given the hierarchical role of the E2E DE, this service may not only list the decisions at the E2E level, but also all known decisions living inside each underlying domain.			
Security Decision Priority Service	Similar to the service defined in the Domain DE but operates at E2E level.	See Domain DE	See Domain DE	• External UI/Operator

4.4.9 E2E Security Orchestrator

4.4.9.1 Function

The E2E Security Orchestrator (E2E SO) is responsible of orchestrating and managing the different security enablers from multiple domains to cover the security configuration requirements specified by the defined E2E security policy. The E2E SO maps the E2E security policy into the domain-specific policy and interacts with the SOs to apply the corresponding security policies and deploy and manage the life-cycle of the required security enablers at domain level.

4.4.9.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Security Policy Enforcement Service	This service enforces and controls security policies cross-domain through interaction with SOs at domain level.	Create	Internal/External	• E2E Decision Engine • Other Operators

Table 15 - Services provided by E2E Security Orchestrator module.

4.4.10 E2E Policy and SSLA Management

4.4.10.1 Function

The E2E policy and SSLA management (E2E PSM) block provides multi-level SSLA, HSPL, MSPL and final enabler configuration translations. Policy conflict avoidance is enforced by this block to prevent contradicting policies or requirements of previously deployed security services.

4.4.10.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Security SLA Refinement Service	This service refines SSLAs into HSPL policies for orchestration.	Convert	External	• User/System Operator • Other ISPs • E2E SIE
HSPL Refinement Service	This service refines HSPL policies into HSPL policies intended for the domains underneath or MSPL policies.	Convert	External	• E2E SO
Security Policy Storage Service	This service stores policies enforced by other domain entities to keep track of them. It could be implemented using DTL to assure liability.	Store	Internal	• Internal • Decision Engine • Security Orchestrator

Table 16 - Services provided by E2E Policy & SSLA Management module.

4.4.11 E2E Trust Management

4.4.11.1 Function

The E2E Trust Management (E2E TM) facilitates E2E trust services across multiple domains, relying on the domain-resident TMs. It can provide across-domain versions of trust functions by aggregating trust outputs of TMs in different domains and enriching them with inter-domain parameters. For this, it

interacts with the E2E PSM and E2E SO to operate in compliance with E2E security requirements, policies and SSLAs.

4.4.11.2 Provided Services

Service Name	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Trust Reputation Manager Service	This service works as a regular TRM, calculating trust and reliability, but using as input the output of the TRMs deployed on different domains.	Data aggregator Calculation of trust	Internal	• TRM

Table 17 - Services provided by E2E Trust Management module.

4.4.12 Domain-Level and Cross-Domain Data Services

4.4.12.1 Function

The Data Services allow the different functions to persist data that can be shared by functions in one or more domains. They need to manage the access to allow only authorized consumers. By introducing this service, the data persistence and data processing are separated, i.e. enabling stateless management functions and eliminating the need for per-function data persistence and per-function processing.

The Data Services should support different types of storage techniques (e.g. DBMS, DLT, persistent data bus) depending on the needs. The mechanisms or technologies used could eventually be dynamically selected.

The data is collected by the SDCs and should be normalised either by the SDC or by an adaptor so that the consumers of the data can use it. It should be handled either within the domain where it was produced or by a well-defined and controlled entity. The Data Services need to implement access control, data security policies, and eventually transactions to assure ACID properties (Atomicity, Consistency, Isolation, Durability), particularly if multiple producers and consumers are involved.

The Data types are those collected by the SDC (see the examples list in Sec. 2.3.1). Standard formats should be used, e.g. PCAP for network traffic, JSON with schema for data interchange, STIX for sharing Cyber Threat Intelligence. The captured data can be either real-time data or historical data needed for security-related analysis (e.g. analysis of risk, liability and root cause, and detection of vulnerabilities and intrusions).

The data can pertain to one domain or can be shared between domains for cross-domain security analysis and control. It can be stored and used by different security management functions, such as the SAE, DE, and SO.

4.4.12.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Data Access Service	This service stores data collected by the SDC and makes it available to different security enablers.	Access control Data persistence Data life cycle and data security policy management Data retrieval, transaction-based	Internal/External	• SAE • E2E SAE

Table 18 - Services provided by Domain-Level and Cross-Domain Data Services module.

4.4.13 Integration Fabric

4.4.13.1 Function

The integration fabric facilitates the interoperation and communication between services provided by the different functional blocks, within a domain and across domains. It provides services to register, discover and invoke security management services.

4.4.13.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Registration Service	This service enables the registration/Deregistration of security management services into/from the service registry (catalogue). For each registered security management service, the list of supported capabilities is included as part of the registration.	Register/Deregister	Internal/External	• Exposed security management services
Discovery Service	This service allows the discovery of registered security management services and their capabilities.	Service list Service capabilities	Internal/External	• The consumer of the security management services

Invocation Service	This service allows the authorized service consumer to invoke a discovered security management service.	Invoke service	Internal/External	• The consumer of the security management services
Communication service	This service allows the communication between security management services via dedicated communication channels.	Create/Delete communication channel	Internal/External	• The security management services
		Subscribe to communication channel		
		Receive data from publisher		
		Publish data to subscriber		

Table 19 - Service Provided by the Integration Fabric.

4.4.13.3 Existing available platform analysis

There are two technologies involved in such a solution, a *service mesh* and *event-driven pub/sub services*. The proposal is a combination of both, covering most of the requirements.

A *service mesh* controls how different parts of an application share data with one another, covering the Registration Service, Discovery Service and Invocation Service, it also may provide a subset of the Communication Service. The missing service capabilities from the Communication Service are covered by the *pub/sub service*. It is an essential dedicated infrastructure when frameworks are broken down into parts to obtain the desired reachability between them but also to control the access to each element therefore extracting the communication logic from the services to the unified infrastructure. In particular within INSPIRE-5Gplus this mesh needs multi-domain support that simplifies and controls the inter-domain communications.

- Istio

is a service mesh technology that helps to connect new applications and it is able to better manage security, and to trace the communication between different services (gives a better idea of how applications are communicating with each other ”Metrics” and deliver better application robustness). It is built around the concept of a unified proxy-based service router. This is a TCP-based forwarding router that can actually distribute traffic and separate the resources in a much more efficient fashion, really understanding exactly where any one connection needs to go. In addition, it embedded TLS authentication mechanism as a part of that proxy.

- LinkerD v2

Is the last version of LinkerD, a service mesh for kubernetes, fully open source. It relies on the deployment of proxies next to each service instance, those proxies handle automatically the traffic while also monitoring/telemetry and receiving control commands. The proxies are written in Rust to be as small,

lightweight and safe as possible.

- Consul

Developed by hashicorp it is not completely open source but can be self-hosted with a certain degree of capabilities. It provides a full featured control plane with service discovery, configuration and segmentation. It has its own proxy but is usually employed with envoy as the proxy solution.

On the other hand, pub/sub services, event-driven or event streaming is oriented to capturing data in real-time and storing them for later usage with the particularity of being able to redirect such streams to the desired destinations. It is contrary to the pull approach.

- Kafka

Is an open-source distributed event streaming platform developed by the Apache Software Foundation. It is distributed consisting of servers and clients that communicate via a high-performance TCP network protocol. Servers run in a cluster, those dedicated to storage are known as brokers. It also provides with Connect which integrates non pub/sub enabled services.

- Pulsar

Is also opensource and also developed by the Apache Software Foundation. It is horizontally scalable guaranteeing ordering and consistency with a low latency and durable storage.

- RabbitMQ

Is opensource and one of the most popular message brokers, it supports multiple, messaging protocols and can be deployed distributed and federated at high-scale and high-availability. It is very lightweight.

Inspire's Characteristics	**Service Mesh**			**Event-Driven**			**Combined Alternatives**	
	Istio	LinkerD v2	Consul	Kafka	Pulsar	RabbitMQ	Istio + Kafka	Istio + Pulsar
Service Discovery	Yes	Yes	Yes				Yes	Yes
Traffic Management	Yes With load balancing and Rate Limiting	Yes Limited	Yes Rate Limit				Yes	Yes

Inspire's Characteristics	Service Mesh			Event-Driven			Combined Alternatives	
	Istio	LinkerD v2	Consul	Kafka	Pulsar	RabbitMQ	Istio + Kafka	Istio + Pulsar
Traffic Policy	Yes (complex)	Yes (simpler)	yes				Yes	Yes
Traffic Telemetry/ Observability	Prometheus	Prometheus (limited distribution)	Prometheus				Yes	Yes
Platform Agnostic (VM/k8s)	K8s	K8s only	K8s	VM, K8s optionally	K8s	VM, K8s optionally	K8s + VM	K8s + VM
Platform for Services	K8S/VM	K8s only	K8s				K8s + VM	K8S + VM
Integration of existing Services (Sidecar Proxy)	Envoy	Integrated	Envoy				Yes	Yes
Multi-Domain / Multi-Cluster	yes	hierarchical	yes				Yes	Yes
Access control	Yes	Yes	Yes				Yes	Yes
Rate Limiting	Yes	No	Yes				Yes	Yes
Service Mesh Interface (SMI)	Yes	Yes	Yes				Yes	Yes
Pub/Sub				yes	yes	Yes	Yes	Yes
Stream Processing				yes	yes	not natively	Yes	Yes
Storage				Broker based, Tiered	Broker, Tiered, BookKeeper (DLT), Chunk based	Mirrored Low throughput	Tiered	Tiered, DLT
Open Source	100	100	80	100	100	100	100	100

Inspire's Characteristics	Service Mesh			Event-Driven			Combined Alternatives	
	Istio	LinkerD v2	Consul	Kafka	Pulsar	RabbitMQ	Istio + Kafka	Istio + Pulsar
			(Enterprise edition for Scaling)					
Key Features	Complex Supports everything	Simpler Multi-Cluster v2 rather new	Medium complex Not fully FOSS	Well known and documented	Chunk storage, Stateless brokers	Mirrored, somehow limited	Already showcased	Not showcased

Table 20 - Existing platform, potentially to be used as Integration Fabric

INSPIRE-5Gplus proposes to instantiate Integration Fabric as a combination of Istio + Apache Kafka tools for taking advantage of event-driven and service mesh features. Istio provides a stable solution with multi-domain capabilities and access control to provide a service mesh, linkerd 2 is not yet sufficiently stable. Similarly the decision between Kafka and Pulsar is highly based on the simplicity to integrate with the selected service mesh even if some capabilities from Pulsar, such as the integration with DLT, would be highly appreciated in a production environment and for scalability.

4.4.14 Security Agent

4.4.14.1 Function

The Security Agent (SA) is a security asset for monitoring and managing security at a local point. It is able to capture data needed by other security functions and/or perform actionable behaviour decided locally but managed by other security functions. The SAs communicate with the INSPIRE-5Gplus management plane in their security domain based on configurable security policies. An SA may provide security data to the analysis and management functions from the traffic plane, acting for instance as an active or passive probe.

Preconfigured data for initial configuration is assumed to be injected or loaded at SA instantiation (e.g. by the NFV-MANO). An API for runtime configuration could also be available (e.g. NETCONF, REST). The SA's main function is to provide interoperability between the INSPIRE-5Gplus management plane and the security enablers in the **data and control planes** in an active or passive mode. Security enablers can vary in typology and nature. In some domains, they can be dedicated security network probes. In others, they can be existing VNFs or PNF with security capacity. In all cases, it is expected that the SA function helps translating security policies (e.g. MSPL) to specific or proprietary enabler configuration formats and collects the data required from the network to perform security analyses. This component will expand the interoperability between different vendors and solutions in the 5G domains.

4.4.14.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Security Policy Local Enforcement Service	This service receives a security rule, SSLA or security policy (e.g. MSPL) in a standard format and translates it to the security enablers' associated formats to be able to apply it.	Translate security policy Enforce security policy	Internal	• INSPIRE-5Gplus modules (essentially the Security Orchestrator)
Network Monitoring and Telemetry Service	This service is in charge of generating on-demand data (logs, alerts, network telemetry, statistics, trends).	Generate data	Internal	• SDC

Table 21 - Service provides by the Security Agent

4.4.15 Unified Security API

4.4.15.1 Function

The Unified Security API aims to be a set of commands/rules that will allow the exchange of information between the Management Functions elements (e.g. Network Slices, Network Service) and the HLA components, especially with the Security Orchestrator. This API must allow interactions to be in both directions “from and to” the HLA and the Management Functions elements. It may be deployed in both the E2E and the multiple management domains.

4.4.15.2 Provided Services

Service	Service Description	Service Capabilities	Service Visibility	Potential Consumers
Network Service Actions	This API defines the format/structure (i.e. syntax and semantics) of the requests or list of requests from the INSPIRE-5Gplus framework asking a Service Orchestrator to perform certain actions.	Services/Network deployment, re-configuration and termination actions (e.g., Channel Protection, Monitoring, Network slicing).	Internal	• INSPIRE-5Gplus modules (essentially the Security Orchestrator) • Different services managers (e.g., Network Slice Managers and Service Orchestrators)

Table 22 - Services provided by the Unified Security API

4.5 Automation & Closed Loop

4.5.1 INSPIRE-5Gplus Closed Loop Model

- The Orient-Observe-Decide-Act (OODA) [175] and Monitor-Analyse-Plan-Execute Knowledge (MAPE-K) [176] are the predominantly applied closed loops in self-management and autonomic networking [177]. The closed loop model supported by INSPIRE-5Gplus framework, shown in Figure 15, can be seen as a combination of the stages of OODA and MAPE-K models with integration of cognition capabilities leveraging AI/ML techniques:
- The Observe/Monitor stage is realized by the "Security Data Collector", where network assets/services are monitored, and security-relevant data are collected.
- The Orient/Analyse stage is realized by the "Security Analytics Engine", which analyses the collected data to detect/predict potential anomalies or perform root cause analysis.
- The Decision stage is accomplished by the "Decision Engine", which decides which mitigation plan to deploy based on the insights received from the "Security Analytics Engine" in order to resolve the detected security issue.
- The decisions made are governed by the established SSLA/security policies, which are managed by the "SSLA & Policy Management". The government also considers the trustworthiness of the system as well as the infrastructure. In fact, the "Trust Management" guarantees the trustworthiness of the closed loop, and oversees the life-cycle of trust, statically and dynamically, locally within a security domain, and end-to-end across domains.
- The Act/Execute stage is realized by the "Security Orchestration", which translates the inferred decisions into executable actions that can be enforced on the managed infrastructure through the deployed controllers and security agents.
- AI/ML techniques are leveraged for security analytics and decision making, which allows to incorporate cognition capabilities in the closed loop.
- The Knowledge base maintains the historical data and knowledge generated and used by the different stages of the closed loop.
- The definition of Trusted Data Services as part of the HLA implies the use of DLT with the Data generated, which can then in turn be used as input to calculate the trustworthiness of the actions performed and the infrastructure involved, therefore driving the Act/Execute stage.

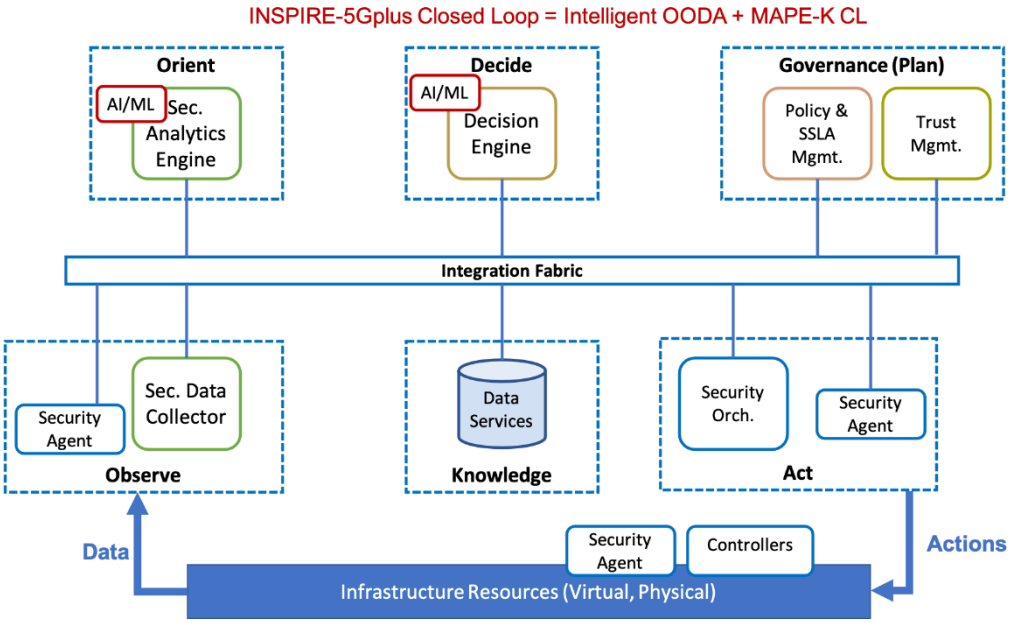


Figure 15 - INSPIRE-5Gplus Closed Loop Model

4.5.2 Typical Closed Loops

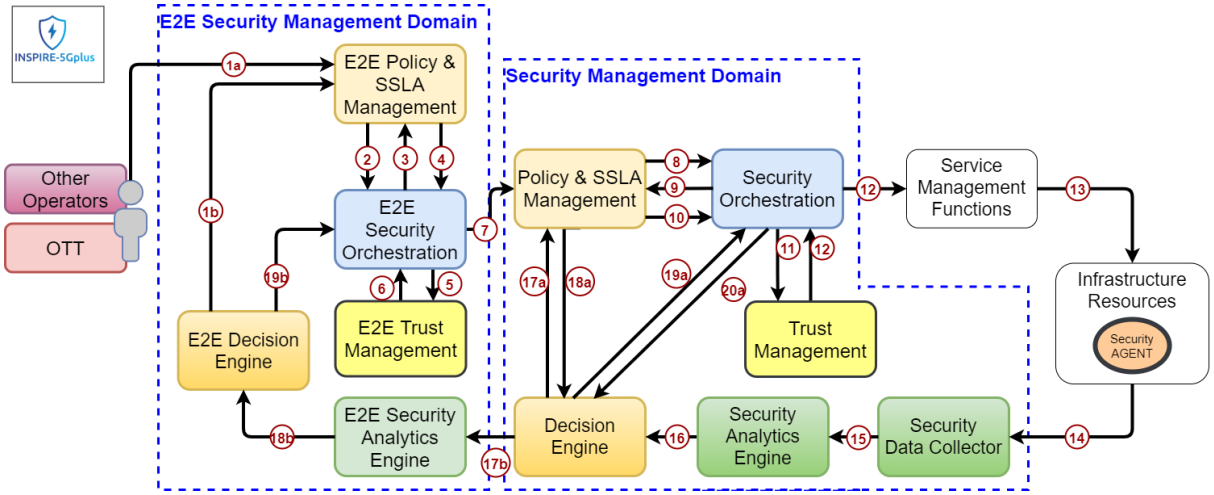


Figure 16 - Typical Security Management Closed Loops.

(1a) – The initial E2E SSLA / Security Policy can be defined by the operator's security administrator or an external entity (e.g. OTT) requesting secure services to the operator;

(1b) – or received from the E2E decision engine;

Note that the E2E SSLA / Security Policy is described using a High-Level Abstraction Language.

(2) After checking for potential conflicts and/or impossibility of fulfilment, the E2E Policy & SSLA Management module communicates the requested E2E SSLA/Security Policy to E2E Security Orchestrator for enforcement;

(3 – 4) – The E2E Security Orchestrator relies on E2E Policy & SSLA Management services to refine the E2E SSLA /Security Policy, providing medium-level description of the E2E policy and its mapping to domain-level policies;

(5 - 6) - Trust scores are retrieved to prioritize deployment solutions that are enforced or going to be enforced.

(7 - 8) – Each domain receives its corresponding domain-level policy that will be first checked for potential conflicts and/or impossibility of fulfilment by the Policy & SSLA Management module before being transmitted to the Security Orchestrator for enforcement;

(9 - 10) – The Security Orchestrator relies on Policy & SSLA Management services to refine the domain-level policy into low-level actions that can be enforced on the domain infrastructure;

(11 - 12) - Trust scores are retrieved to prioritize deployment solutions that are enforced or going to be enforced.

(13 - 14) – Depending on the situation, the security policies can be enforced directly on the resources (e.g., configuration of new rules on a deployed vFirewall) or via the Unified Security API offered by the network/service orchestration services (e.g., instantiation of new security VNFs and their chaining);

(15) – Once the security policy is enforced, the data on the network performance and security are collected by the Security Data Collector from the Security Agents and analysed by the Security Analytics Engine to detect any potential violation of the policy; Data is also stored in Trustable Data Services from where the Trust score can be computed.

(16) – If an anomaly is detected, the Security Analytics Engine informs the Domain's Decision Engine; Trust scores from each Security Management Domain are used by E2E Security Management Domain Trust Management to provide with E2E trustiness score calculations.

(17a - 18a) – The Decision Engine generates a Domain-level mitigation decision (in the form of security policy) and asks for conflict detection.

(19a - 20a) The Decision Engine can provide the new policy to the Security Orchestrator.

(21a - 22a) - Trust scores are retrieved to prioritize deployment solutions.

(23a) Enforcement of the reactive decision is done.

(17b) – Alternatively (if the domain-level mitigation decision doesn't solve the problem or can have an impact on the E2E security policy), the E2E security management domain is informed;

(18b, 1b, 19b) – The data collected cross-domains are analysed for detecting E2E-level anomaly and producing the E2E-level mitigation decision in the form of security policy that will be enforced by the E2E Security Orchestrator after being checked for potential conflicts by the E2E Policy & SSLA Management module. This process may produce a new enforcement from the E2E Security Orchestrator to the Security Orchestrator.

5 Impact of Pandemic on 5G Security Threat Landscape

COVID-19 pandemic produced an unexpected challenge for society and to telecommunications infrastructure. That challenge has evolved with the phases of the pandemic, with a period of early response followed by a period of new normality after the acceptance of the situation by society.

During the early response, operators adapted quickly by activating their business continuity plans which implied changes to workspaces, reducing contact and off course, remote working among others. These business continuity plans allowed the operators to support emergency services and communications, such as broadcasting text messages (SMS), on top of which many countries relied their communications strategies. Call centres came under unprecedented strain and operators supported front-line workers by providing special support plans and the virtualization of customer care services to cope with the increase on the demand.

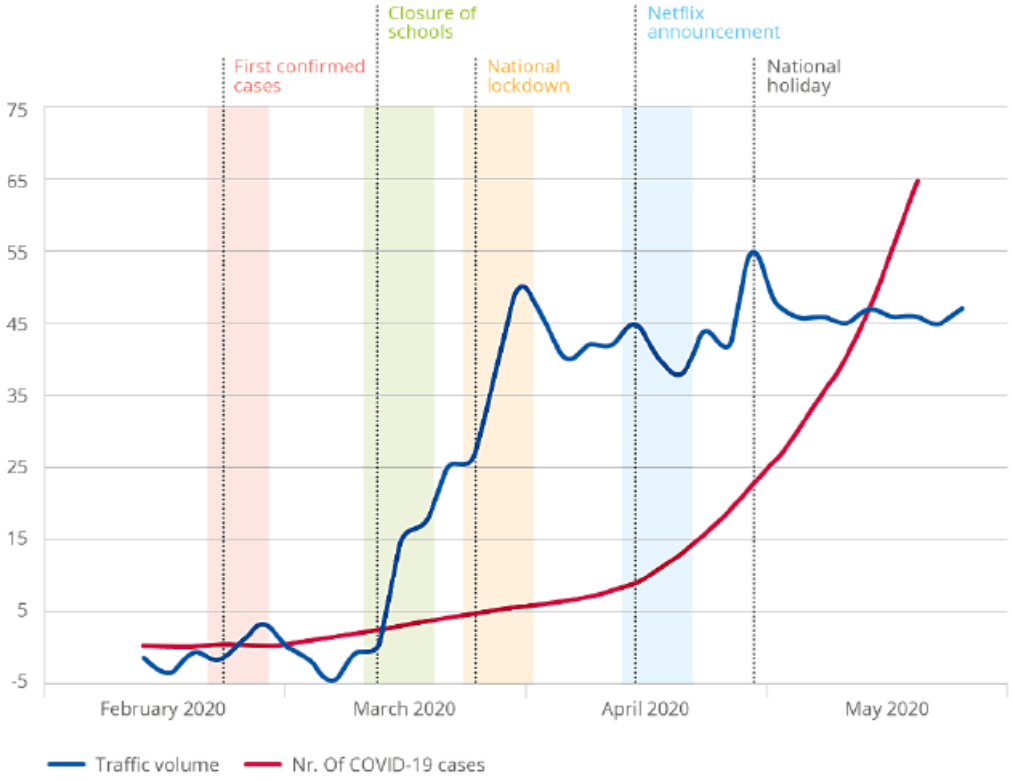


Figure 17 - Relation of COVID-19 case evolution with traffic volume [178]

After this initial strain, the new normality did not come with a restoration of pre-pandemic network usage and it is not even expected once the pandemic is completely under control. Changed consumption habits are consolidating and are thought to be providing permanent consumption habits of citizens. Those changes can be summarized in an initial spike in traffic volume as a consequence to the need to get new information and communicate with now forced distant acquaintances due to lockdown. That communication implied a higher usage of voice and online collaboration services and also a relocation of the source of traffic from business centres to residential areas with a high increase in upload. There has been also an increase in traffic peak hours in the morning and afternoons outside the traditional evening peak. That increase produced an increase in backbone network up to 40% but demonstrated to have sufficient capacities. On the contrary, GPRS roaming exchange (GRX) traffic volume saw a significant drop in traffic because of travel being banned.

Apart from network reconfigurations which partly alleviated the increase in traffic peaks as well as in traffic changes, spectrum resources were also increased. Requests for unallocated spectrum bands and spectrum sharing, ensured licenses for the deployment of 5G as well as providing spectrum for

backhaul were needed. “During COVID-19, fast and flexible changes to regulations proved to be essential”[178].

Video transmission is one of the more bandwidth hungry applications and the increase of streaming service consumption during the lockdown was one of the reasons of traffic increase which was partly mitigated, by the collaboration of the users by making them aware of the effects of such behaviour and asking for responsibility, as well as by the industry which reacted by reducing the quality of streamed content. Without that, increase in some networks may have risen to a 70% increase which would have severely affected many networks during peak hours.

Network operators have seen during the pandemic an increase in DDoS attacks and ransom demands against healthcare organisations. In addition, the need of equipment purchase for remote work introduced the possibility of malware infection plus connection from home networks which may have already been compromised may lead to business cybersecurity flaws. Similarly, attackers have focused in VPN concentrators on which companies needed to rely to enable remote work for their workforces.

Also there has been a trend in physical attacks to operator staff members during equipment upgrades and empty offices, even base stating attacks, while conspiracy theories around 5G and health have been circulating around Europe to the extent of involving 5G as motivation if the disease. [180]

5G commercialization in China has changed the way the pandemic has been fought by providing better assistance and enhanced virus tracking, remote patient monitoring and data access and analysis. In particular, in the field of Telemedicine, adopting 5G is a requirement since previous networks lack the bandwidth capacity for real-time video conferencing, not to say the enablement of virtual and augmented reality technologies (VR/AR). In addition, ULLC is a requirement for wearables that can be used to monitor patients. Another field in which 5G is being taken profit is the use in Robots to reduce the burden of first-line officials in monitoring and ensuring social distancing and patrol streets.

What the pandemic has demonstrated is the capacity of 5G but mainly in collaboration with other emerging technologies such as robotics or IoT, while a speed up in 5G deployment is needed to also reduce the cost.[181]

Even if 5G promises fully anonymised authentication techniques, such techniques need to be explicitly activated in the network equipment by network operators. The lack of anonymised authentication, or techniques to bypass it, in addition to the fact that 5G network cells are smaller, implies precise location of the user by the operator. This Location-tracking data can be deceitful usage for simply advertising or more alarming political prosecution among others, therefore the operators need to bring this technology in line with the current European laws, in particular the GDPR and ePrivacy Directive. This need is even magnified by the facilities that 5G brings to IoT and the fact that users need to know where their data is processed which in turn is complicated by the fact that some device vendors are locate in third party countries. This is why the European Commission recognises the importance of 5G as a fundamental block of the necessary digital transformations and has therefore taken further steps to strengthen Europe's digital sovereignty, calling Member States to boost investments in high-capacity broadband connectivity infrastructures, including 5G [179].

6 Conclusions

In this deliverable we presented the key architectural requirements and emerging enabling technologies and the associated risks to provide liability-aware trustable and smart 5G security. That security has been put into context by providing a set of illustrative use cases that has serve as the seed to the definition of the INSPIRE-5GPlus High Level Architecture and the requirement analysis and service definition carried out. Finally, because of the unfortunate pandemic suffered all over the globe during year 2020 an initial analysis of its effects in the telecommunication industry and in relation with security has been carried out.

Section 1 described the objective of this deliverable and its role for other work packages in the INSPIRE-5Gplus project.

Section 2 provides a beyond the state-of-the-art analysis of the emerging enabling technologies for security in 5G and beyond, from academia as well as from previous research projects, analysing also the risks of their adoption, the challenges and finally the future usage.

Section 3 introduces a set of illustrative use cases identified by INSPIRE-5GPlus partners, their relations with the already introduced emerging enabling technologies and how the technologies are valuable for the different proposals.

Section 4 describes the High-Level Architecture from INSPIRE-5GPlus, the requirements identified, and the framework proposed with a detailed description of the different functional blocks and the proposed services. This section also introduces the Automation and closed loop approach that INSPIRE-5GPlus is adopting.

Section 5 provides an overview of the COVID-19 pandemic on 5G security threat landscape.

The work that has been carried out in the scope of Work Package 2 during the first 18 months of the INSPIRE-5Gplusproject, covering the identified enabling technologies and the definition of the High-Level Architecture leveraging on such technologies with a set of Illustrative Use Cases to demonstrate the potential of the proposal as a collaborative work of the partners involved, serving as the foundation to the deeper analysis of Use Cases already on-going and the development of INSPIRE-5Gplus enablers.

References

[1] C. Benzaid and T. Taleb, "ZSM Security: Threat Surface and Best Practices," in IEEE Network, vol. 34, no. 3, pp. 124-133, May/June 2020, doi: 10.1109/MNET.001.1900273.

http://www.mosaic-lab.org/uploads/papers/8be6454f-8c50-4f6b-9ba9-9b80f7c5761b.pdf

[2] D2.1: 5G Security: Current Status and Future Trends - https://www.inspire-5gplus.eu/wp-content/uploads/2020/05/i5-d2.1_5g-security-current-status-and-future-trends_v1.0.pdf

[3] ETSI GS ZSM 002, "Zero-touch network and Service Management (ZSM); Reference Architecture," Aug. 2019.

https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf

[4] eCPRI Specification V2.0 (2019-05-10) http://www.cpri.info/downloads/eCPRI_v_2.0_2019_05_10c.pdf

[5] NG-RAN; F1 general aspects and principles https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3257

[6] ETSI GS NFV 002 v1.2.1 (2014-12); Network Functions Virtualisation (NFV); Architectural Framework ttps://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf

[7] ITU-T Y.3300: Framework of software-defined networking https://www.itu.int/rec/T-REC-Y.3300-201406-I/en

[8] C. Benzaid and T. Taleb, "AI-driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions," in IEEE Network Magazine, Vol. 34, No. 2, Mar. 2020, pp. 186-194

http://www.mosaic-lab.org/uploads/papers/20edfc7e-02db-4fad-9b63-d584342130d2.pdf

[9] C. Benzaid and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defence or Offense Enabler?" in IEEE Network Magazine. https://ieeexplore.ieee.org/document/9186438

http://www.mosaic-lab.org/uploads/papers/be3137de-432f-43d6-bcf8-0e801dc62cc6.pdf

[10] SelfNet D5.3. Report and Prototypical Implementation of the Integration of the Algorithms and Techniques used to Provide Intelligence to the Decision-Making Framework.

[11] SliceNet D2.2. Overall Architecture and Interfaces Definition.

[12] D. Lorenz, V. Perelman, E. Raichstein, K. Barabash, A. Shribman. SliceNet – Cognitive Slice Management Framework for Virtual Multi-Domain 5G Networks. In Proc. of the 11th ACM International Systems and Storage Conference, pp. 129, June 2018.

[13] SliceNet D6.6. Single-Domain Slice FCAPS Management. May 2020

[14] J. Ali-Tolppa, S. Kocsis, B. Schultz, L. Bodrog, and M. Kajo, "Self- healing and Resilience in Future 5G Cognitive Autonomous Networks," in 10th ITU Academic Conf., Machine Learning for a 5G Future, Nov. 2018, pp. 35 – 42.

[15] M.Qin,Q.Yang,N.Cheng,H.Zhou,R.R.Rao,andX.Shen,"Machine Learning Aided Context-Aware Self-Healing Management for Ultra Dense Networks with QoS Provisions," IEEE Transactions on Vehicular Technology, vol. 67, no. 12, pp. 12 339 – 12 351, Dec. 2018.

[16] P. Salva-Garcia, E. Chirevella-Perez, J. B. Bernabe, J. M. Alcaraz-Calero and Q. Wang, "Towards Automatic Deployment of Virtual Firewalls to Support Secure mMTC in 5G Networks," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 2019, pp. 385-390, doi: 10.1109/INFCOMW.2019.8845183.

[17] L. Fernández Maimó, Á. L. Perales Gómez, F. J. García Clemente, M. Gil Pérez and G. Martínez Pérez, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," in IEEE Access, vol. 6, pp. 7700-7712, 2018, doi: 10.1109/ACCESS.2018.2803446.

[18] Ana Serrano Mamolar, Pablo Salvá-García, Enrique Chirivella-Perez, Zeeshan Pervez, Jose M. Alcaraz Calero, Qi Wang, "Autonomic protection of multi-tenant 5G mobile networks against UDP flooding DDoS attacks", Journal of Network and Computer Applications, Volume 145, 2019, 102416, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2019.102416

[19] MonB5G D2.1. 1st Release of the MonB5G Zero Touch Slice Management and Orchestration Architecture. Feb. 2021.

[20] G. Carrozzo et al., "AI-driven Zero-touch Operations, Security and Trust in Multi-operator 5G Networks: a Conceptual Architecture," 2020 European Conference on Networks and Communications (EuCNC), 2020, pp. 254-258, doi: 10.1109/EuCNC48522.2020.9200928.

[21] C. Benzaid and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defence or Offense Enabler?" in IEEE Network Magazine, Vol. 34, No. 6, Nov. 2020, pp. 140 - 147.

[22] Intel developer website: How to Properly Use SGX PCL to Guarantee the Confidentiality of Code? -https://community.intel.com/t5/Intel-Software-Guard-Extensions/How-to-Properly-Use-SGX-PCL-to-Guarantee-the-Confidentiality-of/td-p/1155448

[23] AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More January, 2020 - https://www.amd.com/system/files/TechDocs/SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more.pdf

[24] Yuanzhong Xu, Weidong Cui, Marcus Peinado, IEEE Symposium on Security and Privacy. Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems. (2015).

[25] Jo Van Bulck, *imec-DistriNet, KU Leuven;* Nico Weichbrodt and Rüdiger Kapitza, *IBR DS, TU Braunschweig;* Frank Piessens and Raoul Strackx, *imec-DistriNet, KU Leuven. USENIX.* Telling Your Secrets Without Page Faults: Stealthy Page Table-based Attacks on Enclaved Execution. (2017).

[26] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado Inferring fine grain control flow inside SGX (6th USENIX Security Symposium (Security), Vancouver, Canada, August 2017

[27] Johannes Götzfried, Moritz Eckert, Sebastian Schinzel, Tilo Müller. Cache Attacks on Intel SGX. EuroSec'17: Proceedings of the 10th European Workshop on Systems Security. April 2017

[28] Ferdinand Brasser, *Technische Universität Darmstadt;* Urs Müller, Alexandra Dmitrienko, Kari Kostiainen, and Srdjan Capkun, *ETH Zurich;* Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*. USENIX 2017. Software Grandd Exposure,

[29] Daniel Moghimi, Gorka Irazoqui, Thomas Eisenbarth. Conference: International Conference on Cryptographic Hardware and Embedded Systems ; CacheZoom: How SGX Amplifies the Power of Cache Attacks (2017)

[30] Michael Schwarz et al, International Conference on Detection of Intrusions and Malware, Malware Guard Extension: abusing Intel SGX to conceal cache attacks (Feb 2017)

[31] Moritz Lipp et al. Meltdown: Reading Kernel Memory from User Space. 2017; https://meltdownattack.com/meltdown.pdf

[32] Paul Kocher et al. Spectre Attacks: Exploiting Speculative Execution ; 2017. https://meltdownattack.com/meltdown.pdf

[33] Jo Van Bulck et al. FORESHADOW: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution. 2017

[34] *Esmaeil Mohammadian Koruyeh et al.*Spectre Returns! Speculation Attacks using the Return Stack Buffer ; 2017

[35] SGXSPECTRE; https://github.com/lsds/spectre-attack-sgx

[36] Guoxing Chen et al; 2019 IEEE European Symposium on Security and Privacy (EuroS&P). SGXPECTRE: Stealing Intel Secrets from SGX Enclaves via Speculative Execution

[37] Stephan van Schaik et al. RIDL: Rogue In-Flight Data Load. Nov 2019

[38] https://zombieloadattack.com; Michael Schwarz. 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019 ZombieLoad: Cross-Privilege-Boundary Data Sampling.

[39] Stephan van Schaik. CacheOut: Leaking Data on Intel CPUs via Cache Evictions (June 2020)

[40] Stephan van Schaik. SGAxe: How SGX Fails in Practice (October 2020): Using RIDL to break the whole SGX system (Intel enclaves and remote attestation)

[41] Stephan van Schaik et al Transactional Abort Attack (TAA), Addendum 1 to RIDL: Rogue In-flight Data Load

[42] Jo Van Bulck et al. **LVI**: Hijacking Transient Execution through Microarchitectural Load Value Injection ; https://lviattack.eu/

[43] Ragab et al. CROSSTALK: Speculative Data Leaks Across Cores Are Real

[44] Coppens et al 2009, Practical mitigations for timing-based side channel attacks

[45] Rane et al 2015. 2017. Shih et al: T-SGX Eradicating Controlled-Channel Attacks Against Enclave Programs

[46] Shinde et al. 2016. Preventing Page Faults from Telling Your Secrets:

[47] *Shih et al. 2017.* T-SGX Eradicating Controlled-Channel Attacks Against Enclave Programs.

[48] Strackx et al**,** 2017 The Heisenberg Defence: Proactively Defending SGX enclaves against Page-Table-Based Side Channel Attacks

[49] S. M. Hand et al, 1999 Self-paging in the Nemesis operating system

[50] Costan et al. 2016 Sanctum:: Minimal hardware extensions for strong software isolation

[51] Molnar et al. 2005 The program counter security model: Automatic detection and removal of control-flow side channel attacks. In International Conference on Information Security and Cryptology, pages 156–168. Springer, 2005.

[52] Johan Agat et al, 2000 Transforming out timing leaks. In ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages, pages 40–53.

[53] Ye et al. 2014 A Dynamic Cache Partitioning System Using Page Coloring, published in 2014 23rd International Conference on Parallel Architecture and Compilation Techniques (PACT)

[54] Jicheng Shi et al. 2011. Limiting Cache-based Side-Channel in Multi-Tenant Cloud using Dynamic Page Coloring.

[55] Brasser et al. 2019; DR.SGX: Automated and Adjustable Side-Channel Protection for SGX using Data Location Randomization

[56] Meng Wu et al 2018 Eliminating Timing Side-Channel Leaks using Program Repair (2018) and previous works.

[57] Jin et al, 2009. A Simple Cache Partitioning Approach in Virtualized Environment. (Jin et al). Statically defined split.

[58] Ahmad et al, 2019. A Commodity Obfuscation Engine on Intel SGX

[59] Chiapetta et al, 2016. Real time detection of cache-based side-channel attacks using Hardware

Performance Counters.

[60] Felicitas Hetzelt and Robert Buhren. Security analy- sis of encrypted virtual machines. In *ACM SIGPLAN Notices*. ACM, 2017.

[61] Mathias Morbitzer, Manuel Huber, Julian Horsch, and Sascha Wessel. SEVered: Subverting AMD's virtual machine encryption. In *11th European Workshop on Systems Security*. ACM, 2018.

[62] Robert Buhren, Shay Gueron, Jan Nordholz, Jean-Pierre Seifert, and Julian Vetter. Fault attacks on encrypted general purpose compute platforms. In *7th ACM on Con- ference on Data and Application Security and Privacy*. ACM, 2017.

[63] Zhao-Hui Du, Zhiwei Ying, Zhenke Ma, Yufei Mai, Phoebe Wang, Jesse Liu, and Jesse Fang. Secure encrypted virtualization is unsecure. *arXiv preprint arXiv:1712.05090*, 2017.

[64] Lipp et al. 2016. Usenix conference. technical sessions. Armageddon: Cache Attacks on Mobile Devices

[65] Lapid et al, 2018. Cache-Attacks on the ARM TrustZone implementations of AES-256 and AES-256-GCM via GPU-based analysis

[66] Qualcomm Trustzone - http://bits-please.blogspot.com/2015/08/exploring-qualcomms-trustzone.html

[67] ARM white paper Whitepaper Straight-line Speculation June 2020 Version 1.0

[68] ARM straight line speculation - https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability/downloads/straight-line-speculation

[69] Intel® Advanced Encryption Standard Instructions (AES-NI) - https://software.intel.com/content/www/us/en/develop/articles/intel-advanced-encryption-standard-instructions-aes-ni.html

[70] Introduction to Cache Allocation Technology in the Intel® Xeon® Processor E5 v4 Family https://software.intel.com/content/www/us/en/develop/articles/introduction-to-cache-allocation-technology.html

[71] ETSI NFV SEC - https://docbox.etsi.org/ISG/NFV/Open/Publications_pdf/Specs-Reports/NFV-SEC%20022v2.8.1%20-%20GS%20-%20API%20Access%20Token%20Spec.pdf

[72] Gottel et al. 2018. Security, Performance and Energy Trade-offs of Hardware-assisted Memory Protection Mechanisms

[73] Ali Shafiee, and Rajeev Balasubramonian. 2018. VAULT: Reducing Paging Overheads in SGX with Efficient Integrity Verification Structures. In Proc. of ACM ASPLOS.

[74] Hongliang Tian, Qiong Zhang, Shoumeng Yan, Alex Rudnitsky, Liron Shacham, Ron Yariv, and Noam Milshten. 2018. Switchless Calls Made Practical in Intel SGX. In Proc. of ACM SysTEX.

[75] Duan et al. CSS 2019. London. LightBox: Full-stack Protected Stateful Middlebox at Lightning Speed

[76] Shih et al. S-NFV: Securing NFV states by using SGX. ACM International Workshop 2016. S NFV

[77] *SDN-NFV Sec'17, March 22-24 2017, Scottsdale, AZ, USA* Coughlin et al. TRUSTED CLICK. Trusted Click: Overcoming Security issues of NFV in the Cloud

[78] Youssef et al. International journal of Advanced Computer Science and Applications. Nov 2020. Secure Software Defined Networks Controller Storage using Intel Software Guard Extensions

[79] Wand et al. IEEE Transactions on Cloud Computing. April 2020. S-Blocks: Lightweight and Trusted Virtual Security Function with SGX

[80] 2016 Towards Management of trust for Multi clouds with SGX

[81] 5G CITY, https://www.5gcity.eu

[82] DIVE SHIELD: https://www.shield-h2020.eu

[83] ENSURE/ https://www.5gensure.eu

[84] Lefebvre et al. ARES 2018. Universal trusted / Universal Trusted Execution Environments for Securing SDN/NFV Operations

[85] Youssef et al. International journal of Advanced Computer Science and Applications. Nov 2020. Secure Software Defined Networks Controller Storage using Intel Software Guard Extensions

[86] Wand et al. IEEE Transactions on Cloud Computing. April 2020**.** S-Blocks: Lightweight and Trusted Virtual Security Function with SGX

[87] Duan et al. CSS 2019. London. LightBox: Full-stack Protected Stateful Middlebox at Lightning Speed

[88] *SDN-NFV Sec'17, March 22-24 2017, Scottsdale, AZ, USA* Coughlin et al. TRUSTED CLICK. Trusted Click: Overcoming Security issues of NFV in the Cloud

[89] Shih et al. S-NFV: Securing NFV states by using SGX. ACM International Workshop 2016. S NFV

[90] C. Benzaid and T. Tarik. AI for Beyond 5G Networks: A Cyber-Security Defence or Offense Enabler? IEEE Network, 34(6): 140 – 147, Nov./Dec. 2020.

[91] C. M. Moreira, G. Kaddoum, and E. Bou-Harb, "Cross-Layer Authentication Protocol Design for Ultra-Dense 5G HetNets," in Proc. of the IEEE International Conf. on Communications (ICC), Kansas City, MO, USA, July 2018.

[92] X. Qiu, T. Jiang, S. Wu, and M. Hayes, "Physical Layer Authentication Enhancement Using a Gaussian Mixture Model," IEEE Access, vol. 6, pp. 53 583 – 53 592, Sept. 2018.

[93] R. Liao, H. Wen, F. Pan, H. Song, A. Xu and Y. Jiang, "A Novel Physical Layer Authentication Method with Convolutional Neural Network," 2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, 2019, pp. 231-235, doi: 10.1109/ICAICA.2019.8873460.

[94] T. M. Hoang, T. Q. Duong and S. Lambotharan, "Secure Wireless Communication Using Support Vector Machines," 2019 IEEE Conference on Communications and Network Security (CNS), Washington DC, DC, USA, 2019, pp. 1-5, doi: 10.1109/CNS.2019.8802716.

[95] H. Fang, X. Wang, and S. Tomasin, "Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks," IEEE Wireless Communications, vol. 26, no. 5, pp. 55 – 61, Oct. 2019.

[96] H. Fang, A. Qi and X. Wang, "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement," in IEEE Network, vol. 34, no. 3, pp. 24-29, May/June 2020, doi: 10.1109/MNET.011.1900276.

[97] ETSI GS ENI 002, "Experential Networked Intelligence (ENI); ENI Requirements," Sept. 2019.

[98] M. Husák, J. Komárková, E. Bou-Harb and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 640-660, Firstquarter 2019, doi: 10.1109/COMST.2018.2871866.

[99] A. Krayani, M. Farrukh, M. Baydoun, L. Marcenaro, Y. Gao, and C. S. Regazzoni, "Jammer Detection in M-QAM-OFDM by Learning a Dynamic Bayesian Model for the Cognitive Radio," in Proc. of the 27th European Signal Processing Conference (EUSIPCO), Sept. 2019.

[100] J. A. Herrera and J. E. Camargo, "A Survey on Machine Learning Applications for Software Defined Network Security," In Zhou J. et al. (eds) Applied Cryptography and Network Security Workshops (ACNS 2019), Lecture Notes in Computer Science, vol. 11605, pp. 70 – 93, June 2019.

[101] T. A. Tang et al., "Deep Learning Approach for Network Intrusion Detection in Software Defined

Networking," in Proc. of the 7th Int. Conf. on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, Oct. 2016.

[102] T. Tang et al., "Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks," in Proc. of the 4th IEEE Conf. on Network Softwarization and Workshops (NetSoft), Montreal, QC, Canada, June 2018.

[103] S. S. Mohammed et al., "A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Net- work," in Proc. of the 14th Int. Conf. on Wireless and Mobile Computing, Networking and Commun. (WiMob), Limassol, Cyprus, Oct. 2018.

[104] A. R. Narayanadoss, T. Truong-Huu, P. M. Mohan, and M. Gu- rusamy, "Crossfire Attack Detection using Deep Learning in Software Defined ITS Networks," in Proc. of the 89th IEEE Ve- hicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, Apr./May 2019.

[105] M. Siracusano, S. Shiaeles, and B. V. Ghita, "Detection of LDDoS Attacks based on TCP Connection Parameters," in Proc. of the Global Information Infrastructure and Networking Symposium (GIIS), Thessaloniki, Greece, Oct. 2018.

[106] C. M. Mathas et al., "Evaluation of Apache Spot's Machine Learning Capabilities in an SDN/NFV enabled Environment," in Proc. of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, Aug. 2018.

[107] F. T. Liu, K. M. Ting, and Z. H. Zhou, "Isolation Forest," in Proc. of the 8th IEEE international Conference on Data Mining (ICDM'08), Pisa, Italy, Dec. 2008.

[108] Al-Turjman, Fadi. "Intelligence and security in big 5G-oriented IoNT: An overview." Future Generation Computer Systems 102 (2020): 357-368.

[109] Youness Arjoune*, Saleh Faruque: Artificial Intelligence for 5G Wireless Systems: Opportunities, Challenges, and Future Research Direction. CCWC 2020: 1023-1028*

[110] Rajesh Gupta, Aparna Kumari, Sudeep Tanwar: Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. Trans. Emerg. Telecommun. Technol. 32(1) (2021)

[111] Yalin E. Sagduyu*, Tugba Erpek, Yi Shi: Adversarial Machine Learning for 5G Communications Security. CoRR abs/2101.02656 (2021)*

[112] Jani Suomalainen, Arto Juhola, Shahriar Shahabuddin, Aarne Mämmelä, Ijaz Ahmad: Machine Learning Threatens 5G Security. IEEE Access 8: 190822-190842 (2020)

[113] Chih-Fong Tsai,Yu-Feng Hsu,Chia-Ying Lin,Wei-Yang Lin: "Intrusion detection by machine learning: A review". Expert Syst. Appl. 36(10): 11994-12000 (2009)

[114] Slavica V. Bostjancic Rakas, Mirjana D. Stojanovic, Jasna D. Markovic-Petrovic: "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems". IEEE Access 8: 93083-93108 (2020)

[115] Mbugua, Joseph & Thiga, Moses & Siror, Joseph. "A Comparative Analysis of Standard and Ensemble Classifiers on Intrusion Detection System". International Journal of Computer Applications Technology and Research. 8. 107-115. 10.7753/IJCATR0804.1005. (2019)

[116] M. Panda, A. Abraham, and M. R. Patra, "A hybrid intelligent approach for network intrusion detection". Procedia Eng., vol. 30, no. 2011, pp. 1–9, (2012)

[117] C. Benzaid and T. Taleb, "AI-Driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions," IEEE Network, vol. 34, no. 2, Mar.- Apr. 2020, pp. 186–94.

[118] L. Haung et al., "Adversarial Machine Leaning," Proc. 4th ACM Workshop on Artificial Intelligence and Security, Oct. 2011, pp. 43–58.

[119] R. A. Maronna et al., Robust Statistics: Theory and Methods (with R), 2nd Ed., Wiley Series in

Probability and Statistics, 2019.

[120] Q. Song et al., “Moving Target Defence for Embedded Deep Visual Sensing against Adversarial Examples,” Proc. 17th Conf. Embedded Networked Sensor Systems (Sen- Sys’19), Nov. 2019, pp. 124–37.

[121] Reznik, Alex, et al. "Developing software for multi-access edge computing." ETSI White Paper 20 (2017).

[122] Elias Bou-Harb, Nataliia Neshenko: Cyber Threat Intelligence for the Internet of Things. Springer 2020, ISBN 978-3-030-45857-7, pp. 1-89

[123]] Lili Du, Yaqin Fan, Lvyang Zhang, Lianying Wang, Tianhang Sun: A Summary of the Development of Cyber Security Threat Intelligence Sharing. Int. J. Digit. Crime Forensics 12(4): 54-67 (2020)

[124] http://www.opentaxii.org/en/stable/

[125] https://github.com/csirtgadgets/massive-octo-spice/wiki/The-CIF-Book

[126] https://opentpx.org/

[127] https://yeti-platform.github.io/

[128] http://gosint.readthedocs.io/en/latest/

[129] https://github.com/MISP/MISP

[130] https://cybersecurity.att.com/products/ossim

[131] Thanh Thi Nguyen and Vijay Janapa Reddi, Deep Reinforcement Learning for Cyber Security, arXiv:1906.05799, cs.CR, 2020.

[132] Radanliev, P., De Roure, D., Page, K. et al. Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. Cybersecurity 3, 13 (2020). https://doi.org/10.1186/s42400-020-00052-8

[133] C. Kalalas, J. Alonso-Zarate, Sensor Data Reconstruction in Industrial Environments with Cellular Connectivity, in Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications 2020 (IEEE PIMRC ’20), August 2020.

[134] Zanzi, L., Albanese, A., Sciancalepore, V. and Costa-Pérez, X., 2020. NSBchain: A Secure Blockchain Framework for Network Slicing Brokerage. arXiv preprint arXiv:2003.07748.

[135] Kapassa, E., Touloupos, M., Kyriazis, D. and Themistocleous, M., 2019, December. A Smart Distributed Marketplace. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 458-468). Springer, Cham.

[136] Matheu, S.N., Robles Enciso, A., Molina Zarca, A., Garcia-Carrillo, D., Hernández-Ramos, J.L., Bernal Bernabe, J. and Skarmeta, A.F., 2020. Security architecture for defining and enforcing security profiles in dlt/sdn-based iot systems. Sensors, 20(7), p.1882.

[137] T. N. Dinh and M. T. Thai, "AI and Blockchain: A Disruptive Integration," in Computer, vol. 51, no. 9, pp. 48-53, September 2018, doi: 10.1109/MC.2018.3620971.

[138] K. D. Pandl, S. Thiebes, M. Schmidt-Kraepelin and A. Sunyaev, "On the Convergence of Artificial Intelligence and Distributed Ledger Technology: A Scoping Review and Future Research Agenda," in IEEE Access, vol. 8, pp. 57075-57095, 2020

[139] E. O. Kiktenkoet al., ‘‘Quantum-secured blockchain,’’Quantum Sci.Technol., vol. 3, no. 3, p. 035004, 2018.

[140] K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," in IEEE Access, vol. 7, pp. 10127-10149, 2019

[141] H. Kakavand, N. K. De Sevres, and B. Chilton. (Jan. 2017).TheBlockchain Revolution: An Analysis

of Regulation and Technol-ogy Related to Distributed Ledger Technologies. [Online]. Available:https://ssrn.com/abstract=2849251

[142] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken and M. Liyanage, "The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions," 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 2020, pp. 1-5.

[143] P. Alemany, R.Vilalta, R.Muñoz, R.Casellas, R.Martínez, "End-to-End Network Slice Stitching using Blockchain-based Peer-to-Peer Network Slice Managers and Transport SDN Controllers," accepted in The Optical Networking and Communication Conference & Exhibition (OFC), 6-11 June 2021, virtual event.

[144] P. Alemany, R. Vilalta, R. Muñoz, R. Casellas and R. Maríinez, "Peer-to-Peer Blockchain-based NFV Service Platform for End-to-End Network Slice Orchestration Across Multiple NFVI Domains," 2020 IEEE 3rd 5G World Forum (5GWF), 2020, pp. 151-156, doi: 10.1109/5GWF49715.2020.9221311.

[145] P. Alemany, R. Vilalta, R. Muñoz, R. Martínez and R. Casellas, "Managing Network Slicing Resources Using Blockchain in a Multi-Domain Software Defined Optical Network Scenario," 2020 European Conference on Optical Communications (ECOC), 2020, pp. 1-4, doi: 10.1109/ECOC48923.2020.9333352.

[146] ETICS Final publishable summary report, May 2013, [online] Available: https://www.laquadrature.net/files/ETICS_final_publishable_summary.pdf.

[147] C. Gaber et al., "Liability-Aware Security Management for 5G," 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 133-138, doi: 10.1109/5GWF49715.2020.9221407

[148] G. Guemkam, C. Feltus, P. Schmitt, C. Bonhomme, D. Khadraoui and Z. Guessoum, "Reputation Based Dynamic Responsibility to Agent Assignement for Critical Infrastructure", 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, vol. 2, pp. 272-275, 2011.

[149] 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, pp. 1-2, 2010.

[150] C. Gaber, J.-L. Grimault, C. Loiseaux, M. Hajj, L. Coureau and J.-P. Wary, How increasing the confidence in the eSIM ecosystem is essential for its adoption, [online] Available: https://hellofuture.orange.com/en/how-increasing-the-confidence-in-the-esim-ecosystem-is-essential-for-its-adoption/.

[151] A. Giaretta, N. Dragoni and F. Massacci, "IoT Security Configurability with Security-by-Contract", Sensors, vol. 19, no. 19, pp. 4121, 2019.

[152] G. Costa, N. Dragoni, L. Aliaksandr, F. Martinelli, F. Massacci and M. Ilaria, "Extending Security-by-Contract with Quantitative Trust on Mobile Devices", International Conference on Complex Intelligent and Software Intensive Systems, 2010.

[153] Ahmad Terra, Rafia Inam, Sandhya Baskaran, Pedro Batista, Ian Burdick, Elena Fersman: Explainability Methods for Identifying Root-Cause of SLA Violation Prediction in 5G Network. GLOBECOM 2020: 1-7

[154] Pablo Muñoz Luengo, Isabel de la Bandera, Emil J. Khatib, Ana Gómez-Andrades, Inmaculada Serrano, Raquel Barco: Root Cause Analysis Based on Temporal Analysis of Metrics Toward Self-Organizing 5G Networks. IEEE Trans. Veh. Technol. 66(3): 2811-2824 (2017)

[155] Sergio Fortes Rodriguez, Raquel Barco, Alejandro Aguilar-García: Location-based distributed sleeping cell detection and root cause analysis for 5G ultra-dense networks. EURASIP J. Wirel. Commun. Netw. 2016: 149 (2016)

[156] Harrison Mfula, Jukka K. Nurminen: Adaptive Root Cause Analysis for Self-Healing in 5G

Networks. HPCS 2017: 136-143 2016

[157] Ana Gómez-Andrades, Pablo Muñoz Luengo, Inmaculada Serrano, Raquel Barco: Automatic Root Cause Analysis for LTE Networks Based on Unsupervised Techniques. IEEE Trans. Veh. Technol. 65(4): 2369-2386 (2016)

[158] Hedi Bouattour,Yosra Ben Slimen, Marouane Mechteri, Hanane Biallach: Root Cause Analysis of Noisy Neighbors in a Virtualized Infrastructure. WCNC 2020: 1-6

[159] Reshmi, T.R., Azath, M. Improved self-healing technique for 5G networks using predictive analysis. Peer-to-Peer Netw. Appl.14, 375–391 (2021). https://doi.org/10.1007/s12083-020-00926-1

[160] Yan Z., Li X., Kantola R. (2017) Heterogeneous Data Access Control Based on Trust and Reputation in Mobile Cloud Computing. In: Mavromoustakis C., Mastorakis G., Dobre C. (eds) Advances in Mobile Cloud Computing and Big Data in the 5G Era. Studies in Big Data, vol 22. Springer, Cham. https://doi.org/10.1007/978-3-319-45145-9_4

[161] Yan, Z., Li, X.Y., Kantola, R.: Personal data access based on trust assessment in mobile social networking. In: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, p. 989. IEEE, Beijing, Sept 2014. doi: 10.1109/TrustCom.2014.131

[162] Yan, Z., Li, X.Y., Kantola, R.: Controlling cloud data access based on reputation. Mob. Netw. Appl. March 2015. Springer, ISSN 1572-8153

[163] F. Valenza, T. Su, S. Spinoso, A. Lioy, R. Sisto, and M. Vallini, “A formal approach for network security policy validation,” JoWUA, vol. 8, pp. 79–100, 2017.

[164] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini, “Security policy enforcement for networked smart objects,” Computer Networks, vol. 108, pp. 133 – 147, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128616302663

[165] Jordi Ortiz Murillo, Ramon Sanchez-Iborra, Jorge Bernal Bernabé, Antonio F. Skarmeta, Chafika Benzaid, Tarik Taleb, Pol Alemany, Raul Muñoz, Ricard Vilalta, Chrystel Gaber, Jean-Philippe Wary, Dhouha Ayed, Pascal Bisson, Maria Christopoulou, George Xilouris, Edgardo Montes de Oca, Gürkan Gür, Gianni Santinelli, Vincent Lefebvre, Antonio Pastor, Diego López: INSPIRE-5Gplus: intelligent security and pervasive trust for 5G and beyond networks. ARES 2020: 105:1-105:10

[166] Gregory Blanc, Nizar Kheir, Dhouha Ayed, Vincent Lefebvre, Edgardo Montes de Oca, Pascal Bisson: Towards a 5G Security Architecture: Articulating Software-Defined Security and Security as a Service. ARES 2018: 47:1-47:8

[167] Ricard Vilalta, Pol Alemany, Roshan Sedar, Charalampos Kalalas, Ramon Casellas, Ricardo Martínez, Francisco Vazquez Gallego, Jordi Ortiz Murillo, Antonio F. Skarmeta, Jesús Alonso-Zárate, Raul Muñoz: Applying Security Service Level Agreements in V2X Network Slices. NFV-SDN 2020: 114-115

[168] ENISA Procure Secure: A guide to monitoring of security service levels in cloud contracts https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

[169] https://cordis.europa.eu/project/id/610795

[170] https://cordis.europa.eu/project/id/644429

[171] https://www.sendate.eu/

[172] Van Lamsweerde, Axel. *Requirements engineering: From system goals to UML models to software*. Vol. 10. Chichester, UK: John Wiley & Sons, 2009

[173] INSPIRE-5GPlus D5.1: 5G Security Test Cases v1.6 https://zenodo.org/record/4569524/files/i5-

D5.1_5G%20security%20test%20cases_v1.6.pdf?download=1

[174] White Paper on Intelligent Security Architecture for 5G and Beyond Networks https://www.inspire-5gplus.eu/white-paper-on-intelligent-security-architecture-for-5g-and-beyond-networks/

[175]. Boyd. The Essence of Winning and Losing. June 1995.

[176] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," in Computer, vol. 36, no. 1, pp. 41-50, Jan. 2003, doi: 10.1109/MC.2003.1160055.

[177] I. Vaishnavi, L. Ciavaglia. Challenges Towards Automation of Live Telco Network Management: Closed Control Loops.

[178] ENISA Telecom - Security During A Pandemic https://www.enisa.europa.eu/publications/telecom-security-during-a-pandemic

[179] European Cybersecurity Month 2020: Time for clarity on 5G, security and privacy in the “new normal” | European Data Protection Supervisor (europa.eu) https://edps.europa.eu/press-publications/press-news/blog/european-cybersecurity-month-2020-time-clarity-5g-security-and_en

[180] FASG COVID-19 Situation Report April 2020 https://www.gsma.com/newsroom/wp-content/uploads//FASG-COVID-19-Situation-Report-April-2020.pdf

[181] V. Chamola, V. Hassija, V. Gupta and M. Guizani, "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact," in IEEE Access, vol. 8, pp. 90225-90265, 2020, doi: 10.1109/ACCESS.2020.2992341

[182] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. Nguyen, F. Liu, T. Hewa, M. Liyanage, A. Ijaz, J. Partala, R. Abbas, A. Hecker, S. Jayousi, A. Martinelli, S. Caputo, J. Bechtold, I. Morales, A. Stoica, G. Abreu, S. Shahabuddin, E. Panayirci, H. Haas, T. Kumar, B.O. Ozparlak and J. Roning. 6G White paper: Research challenges for Trust, Security and Privacy. ArXiv abs/2004.11665, 2020.

[183] F. A. Alvares de Oliveira Jr., R. Sharrock and T. Ledoux, "Synchronization of Multiple Autonomic Control Loops: Application to Cloud Computing," in 14th International Conference on Co-ordination Models and Languages (COORDINATION), 2012, pp. 29-43.

[184] R. Cammarota, M. Schunter, A. Rajan, F. Boemer, F., A. Kiss, A. Treiber, C. Weinert, T. Schneider, E. Stapf, A.-R. Sadeghi, D. Demmler, H. Chen, S.U. Hussain, S. Riazi, F. Koushanfar, S. Gupta, T. Rosing, K. Chaudhuri, H. Nejatollahi, N. Dutt, M. Imani, K. Laine, A. Dubey, A. Aysu, F.S. Hosseini, C. Yang, E. Wallace and P. Norton. Trustworthy AI Inference Systems: An Industry Research View. ArXiv abs/2008.04449, 2020.

[185] S.M.K. Gueye, N. de Palma and E. Rutten, "Component-Based Autonomic Managers for Coordination Control", in 15th International Conference on Coordination Models and Languages (COORDINATION), 2013, pp. 75-89.

Appendix A Business and Organizational Requirements Questionnaire

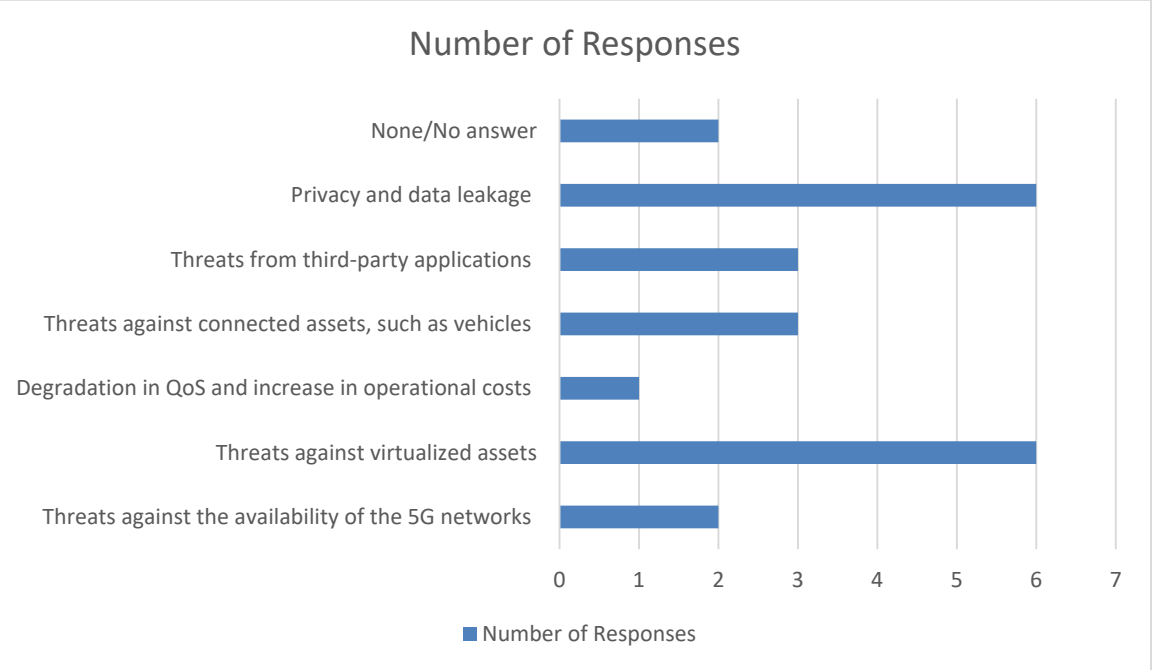
The questionnaire is comprised by 12 questions in total. It was divided into three categories: 1) Business and Organizational Requirements; 2) Regulatory compliance and reputation requirements; and 3) Background information.

The survey has been disseminated into stakeholders with expertise into 5G services. These stakeholders will highlight some key requirements and needs that 5G security enablers need to fulfil. In total the questionnaire received 23 responses from key stakeholders in the 5G security domain.

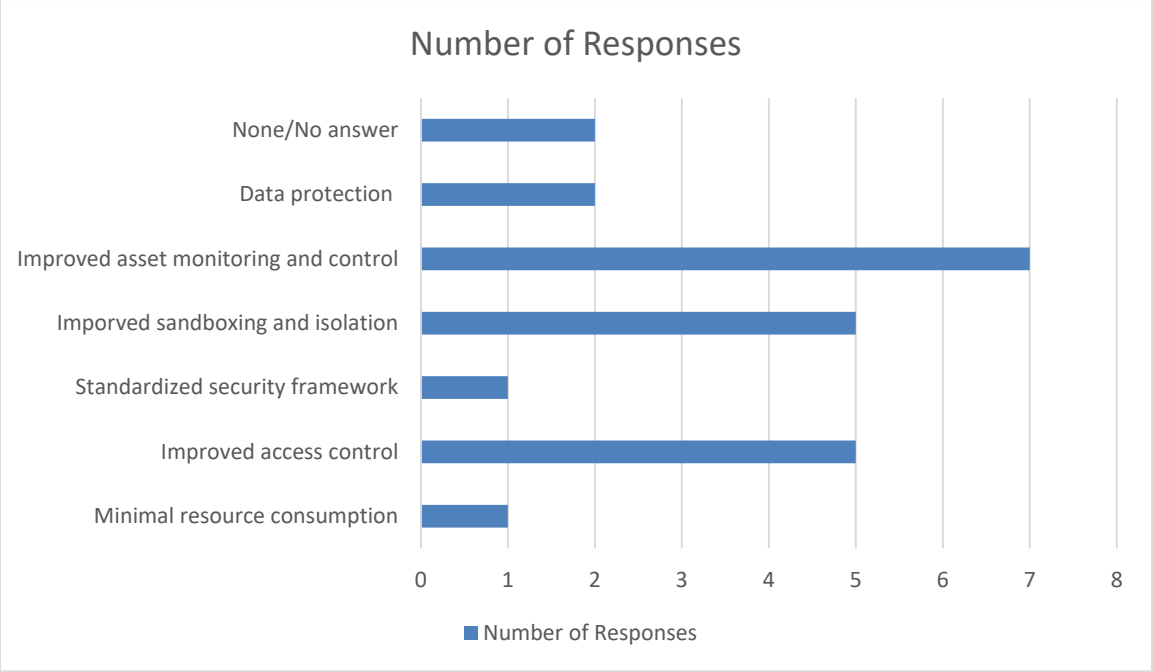
A.1 Results of the Business and Organizational Requirements

A.1.1 Questions and results

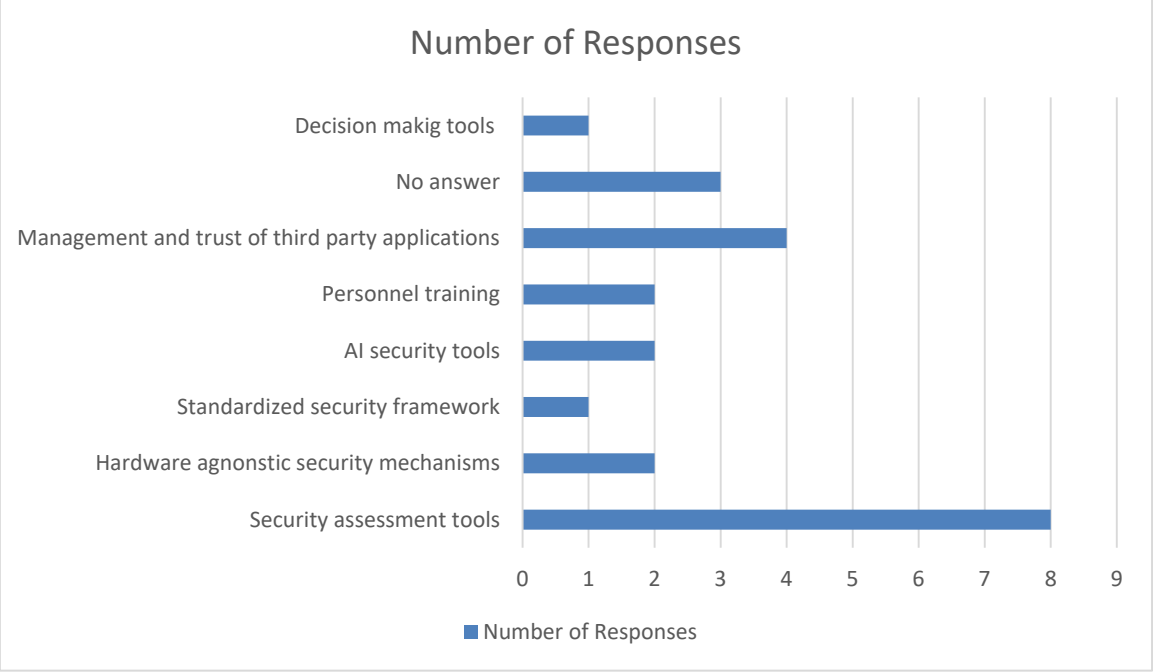
What are the major threats you would like 5G services and applications to be protected? (21 responses)



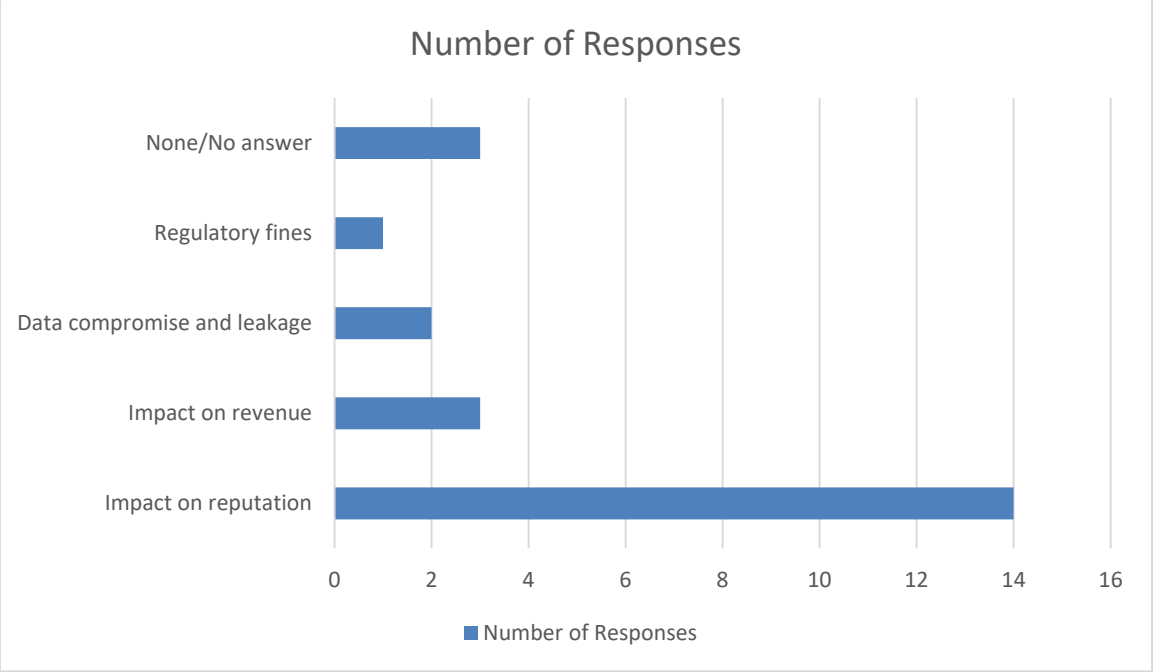
What critical features in terms of security of 5G infrastructure would you require to be improved?



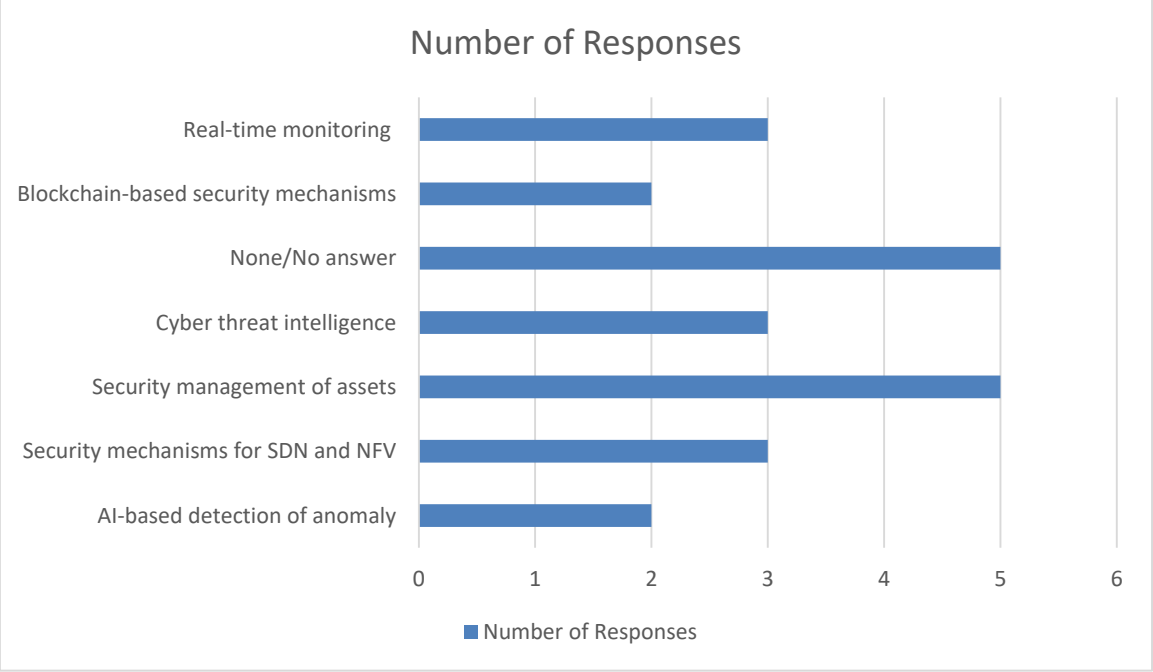
What key security design improvements would you consider as a plus compared to your business activities? How would you like your personnel to be assisted in this regard?



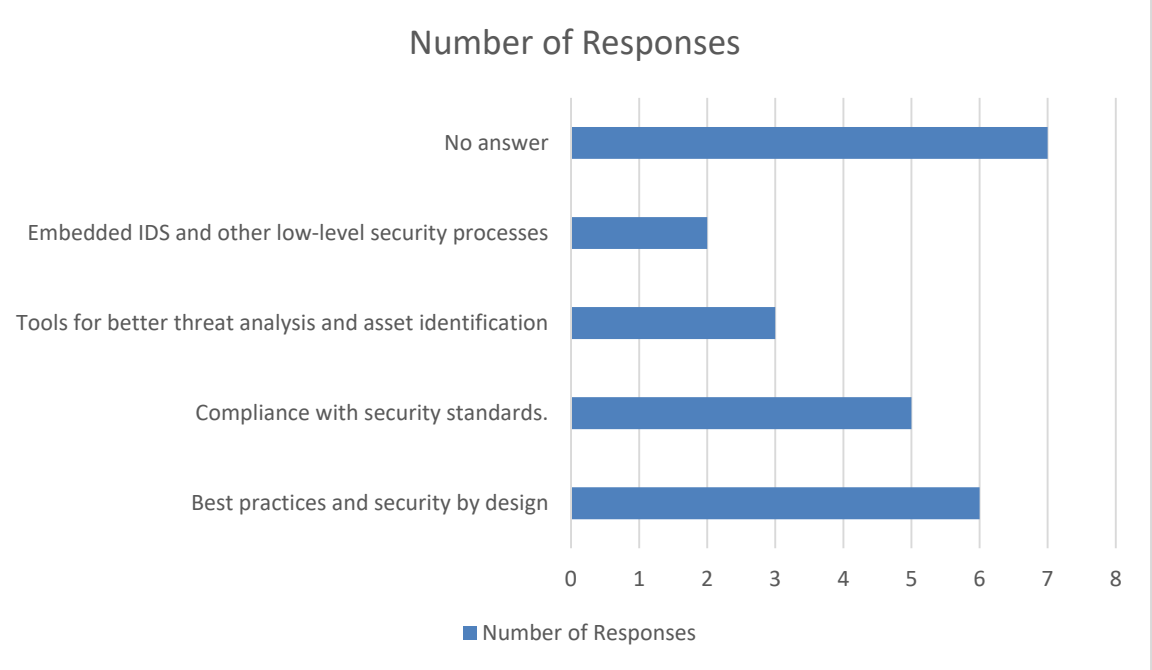
What would be the business impact of a security incident for your organization?



What type of technologies of INSPIRE-5Gplus you consider are more likely to improve your security? Explain briefly why?



What key processes, policies, best practices on privacy and security in your organisation do you consider key for the use of the proposed INSPIRE-5Gplus?



A.1.2 Summary of results

The first part of the questionnaire elicited the business and organizational requirements of key stakeholders of the 5G security domain. The questionnaire revealed several patterns in terms of security that affect more than one of the responders.

Several responders want to protect against threats targeting virtualized assets (6) and threats that impact the confidentiality and integrity of data (6). A smaller number of responders want to protect against threats coming from external assets, such as vehicles (3) and third-party applications (3).

Responders wanted improvements on their existing security infrastructure in the area of asset monitoring (7), sandboxing (5) and access control (5). The majority of the responders wanted better tools to assess their security (8) and manage their applications and trust (4).

The majority of the responders are not comfortable with the virtualization and fluid functionality of 5G infrastructure, where malicious actors can leverage third-party application access to compromise systems. The assets and resources of 5G networks are dynamic, require having more holistic security mechanisms that can adapt and facilitate decision support.

On the business impact of a security incident, the majority of responders answered that the main concern would be the impact and the loss on the reputation (14). A lesser number responded with the impact on revenue (3) and regulatory fines (1).

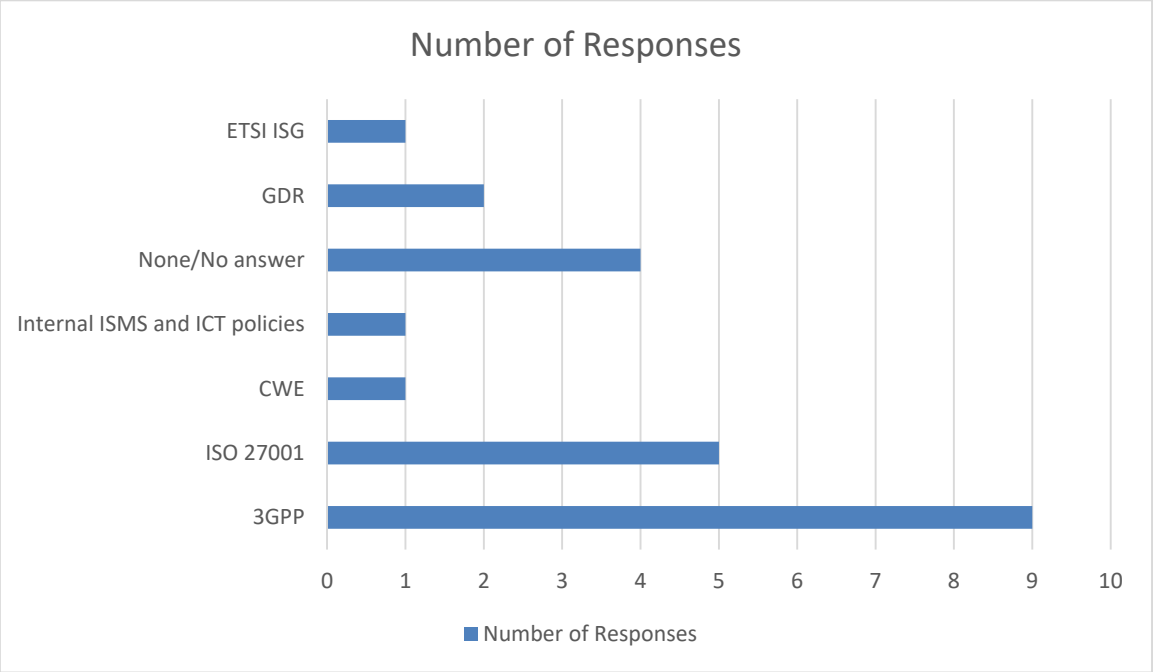
On the technologies of INSPIRE-5Gplus that could improve the security, the responses were divided equally among several answers. Security management of assets (5), real-time monitoring (3), cyber-threat intelligence (3), security mechanisms for SDN and NFV (3), were the most popular. Blockchain-based security mechanisms (2), and AI-based anomaly detection (2), were proposed as well. However, 5 responders answered that they could not identify any security mechanisms of INSPIRE-5Gplus at the moment.

As for the key policies and processes, the majority of the responders had to be compliant with standards (5), and best security practises (6).

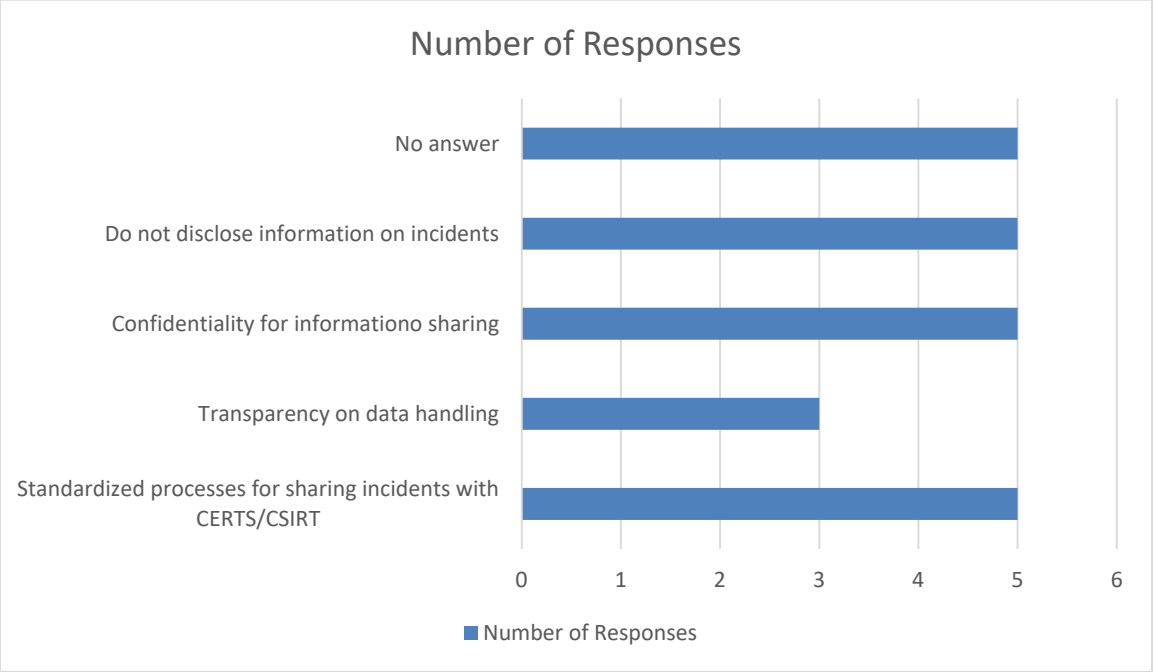
A.2 Results of the Regulatory compliance and reputation requirements

A.2.1 Questions and results

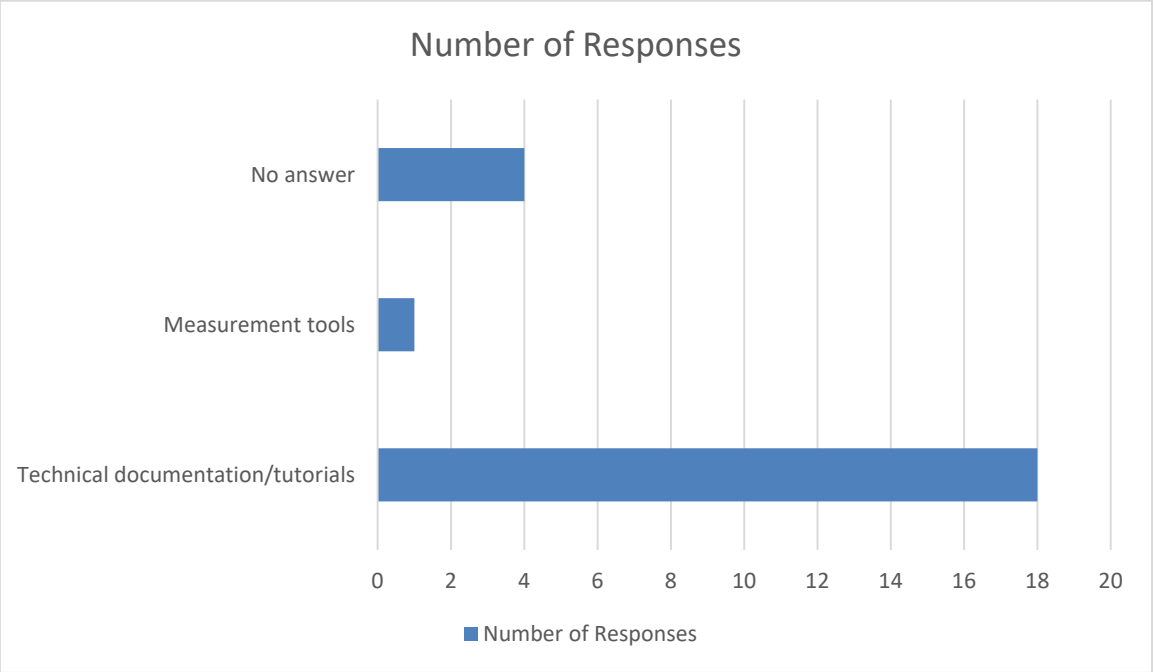
What are the key standards and regulations your infrastructure has to comply with for security and privacy? How do you see INSPIRE-5Gplus can help to achieve this compliance?



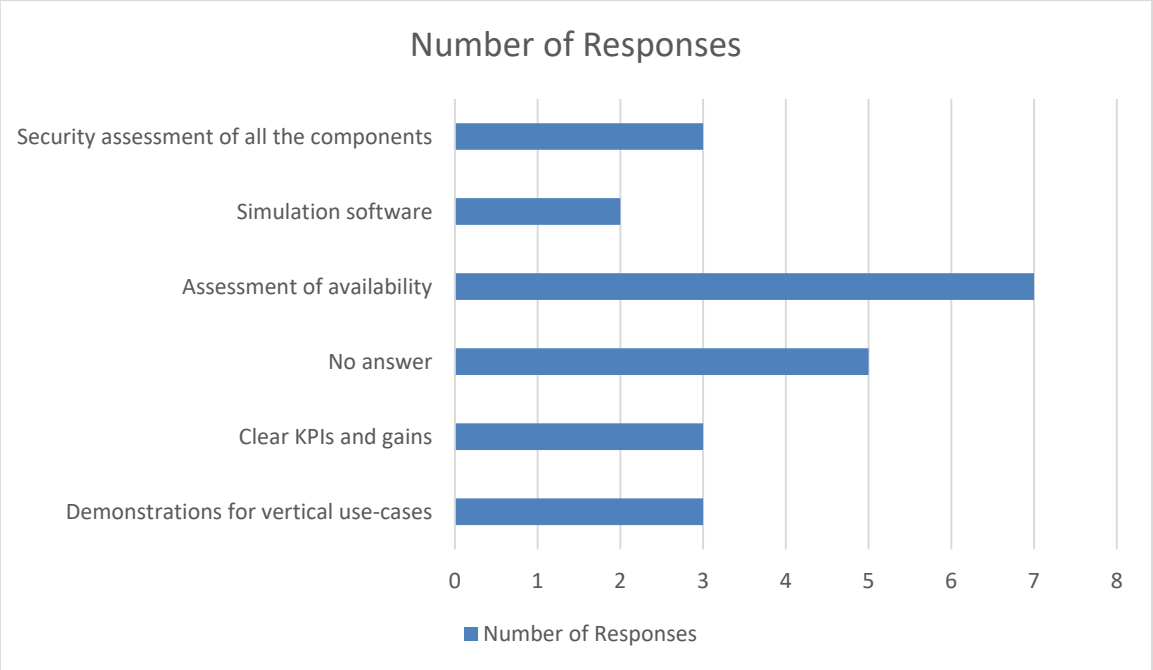
What feature would increase your trust in relation to exchanging anonymous information about incidents within a closed group of 5G operators and providers?



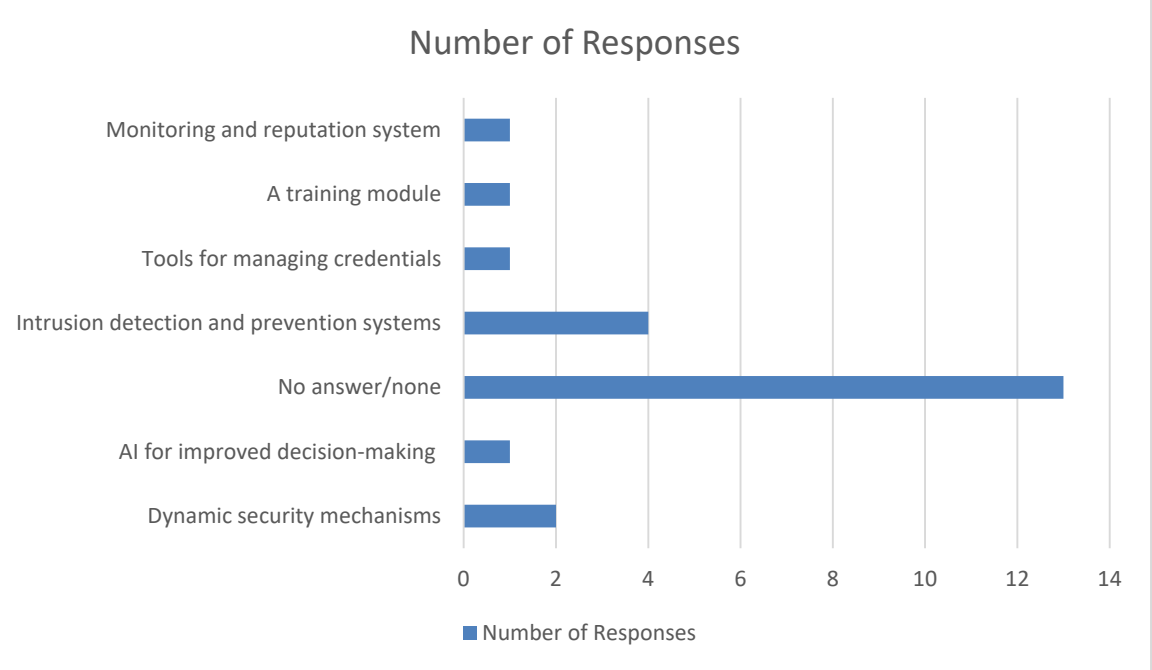
Please describe possible usability requirements regarding the utilisation and deployment of INSPIRE-5Gplus which will be developed during the project (e.g., the tutorial of each components/processes should be available in different languages).



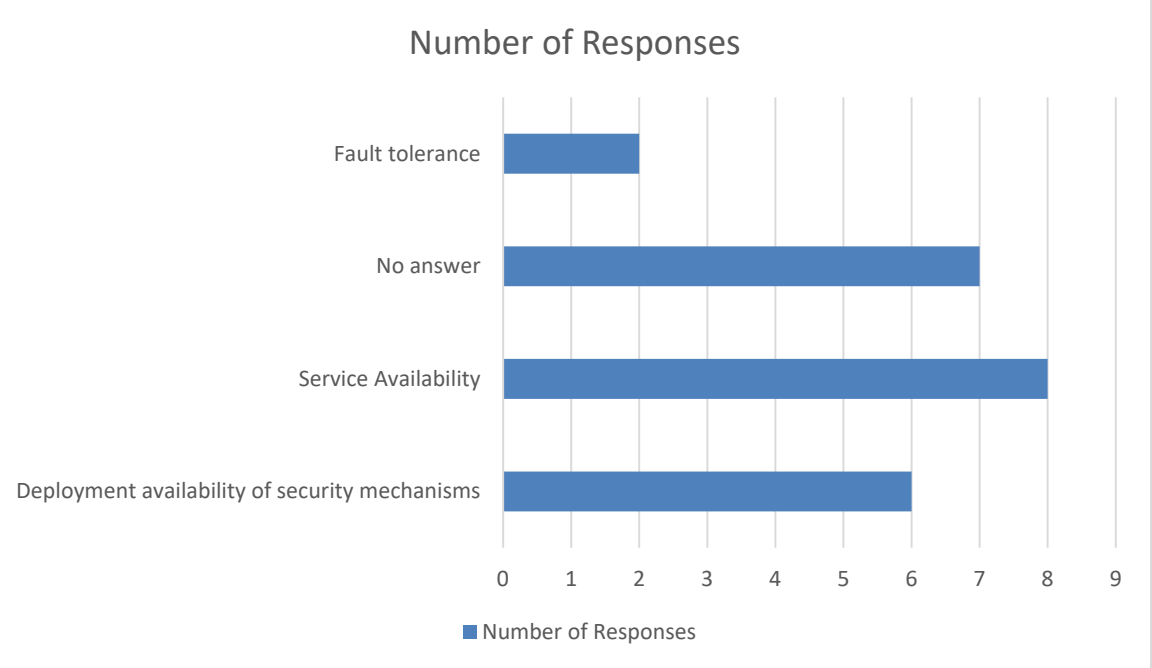
What availability tests do you consider necessary for testing the availability/efficiency of INSPIRE-5Gplus technologies you are waiting? Could you please specify what type of security KPIs are you expecting?



What are your availability concerns or issues? How do you think INSPIRE-5Gplus technology may assist you?



What kind of other improvements and/or technologies would like INSPIRE-5Gplus to implement and what are the expected value you would hope to derive from them?



A.2.2 Summary of results

The second part of the questionnaire focussed on the regulatory compliance and reputation aspects of 5G security.

The key standards and regulations that the majority of the responders had to be compliant with was the 3GPP (9), and the ISO 27001 (5). This is to be expected since most of the responders are involved in the telecommunications sector. A large number of responders do not share any information on security incidents (5). Other responders wanted better transparency (4), data confidentiality (5), and standardized processes to share information with CERT/CIRTs (5). Almost all the responders

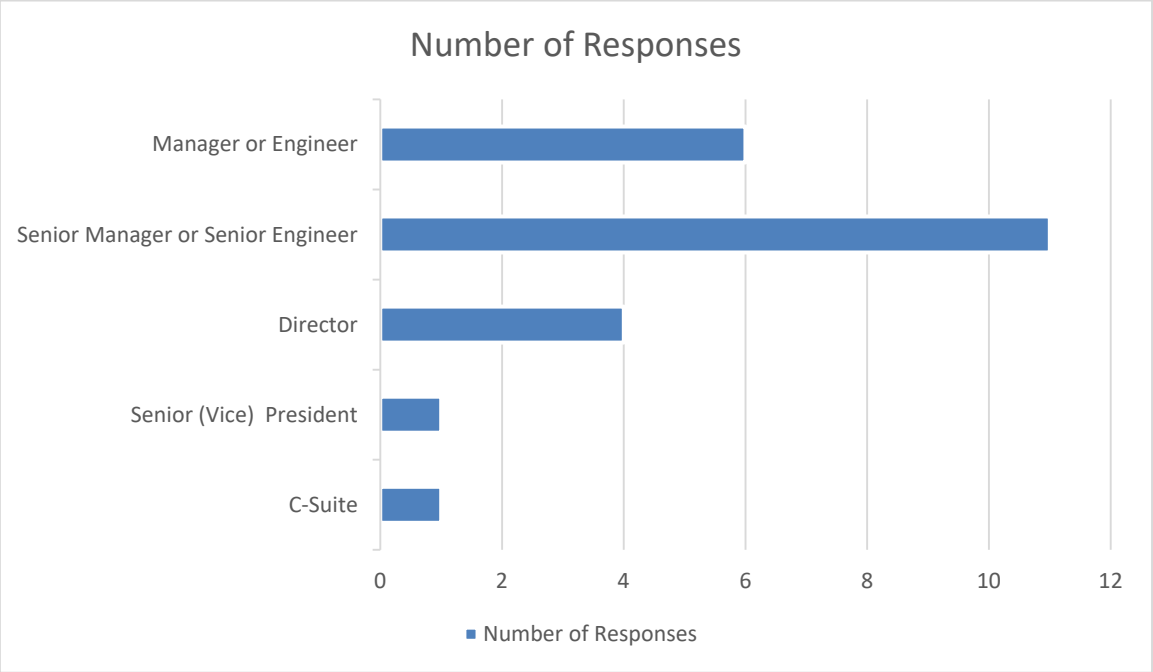
requested to have access to technical documentation, and tutorials (18) for the outputs that will be developed throughout the INSPIRE-5Gplus project.

To demonstrate the availability of the INSPIRE-5Gplus technologies, responders wanted assessments of availability (7), clear KPIs and benefits of the technology, vertical use case demonstration (3) and simulation software (2). The majority of the responders that they have no availability issues that technologies of INSPIRE-5Gplus can assist them (13). Other responders propose intrusion detection and prevention systems (2), or dynamic security mechanisms (2). The other improvements and technologies that would like INSPIRE-5Gplus to implement were service availability (8), improved deployment availability of security mechanisms (6) and fault tolerance (2).

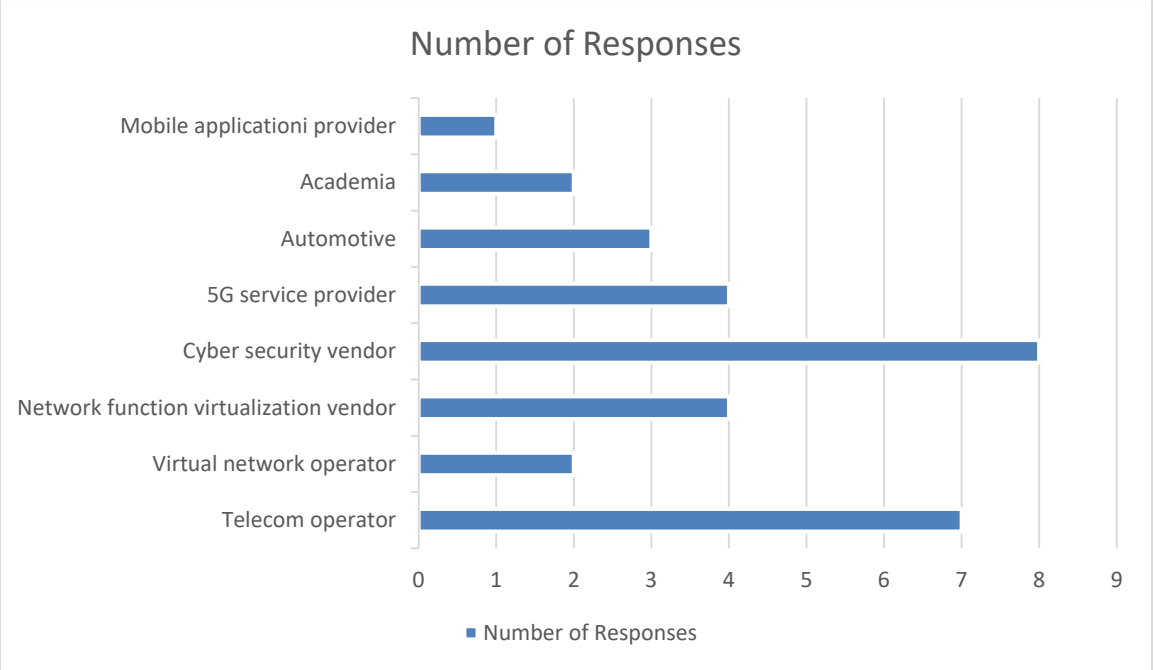
A.3 Results of the Background Information

A.3.1 Questions and results

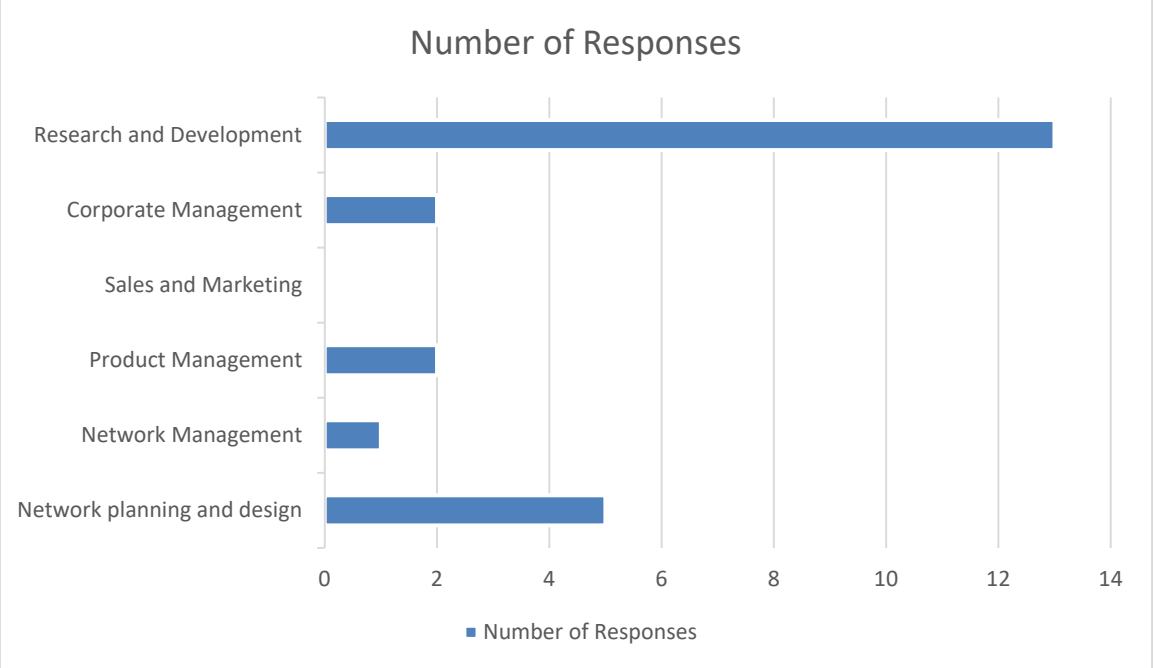
What is your level of responsibility at your company?



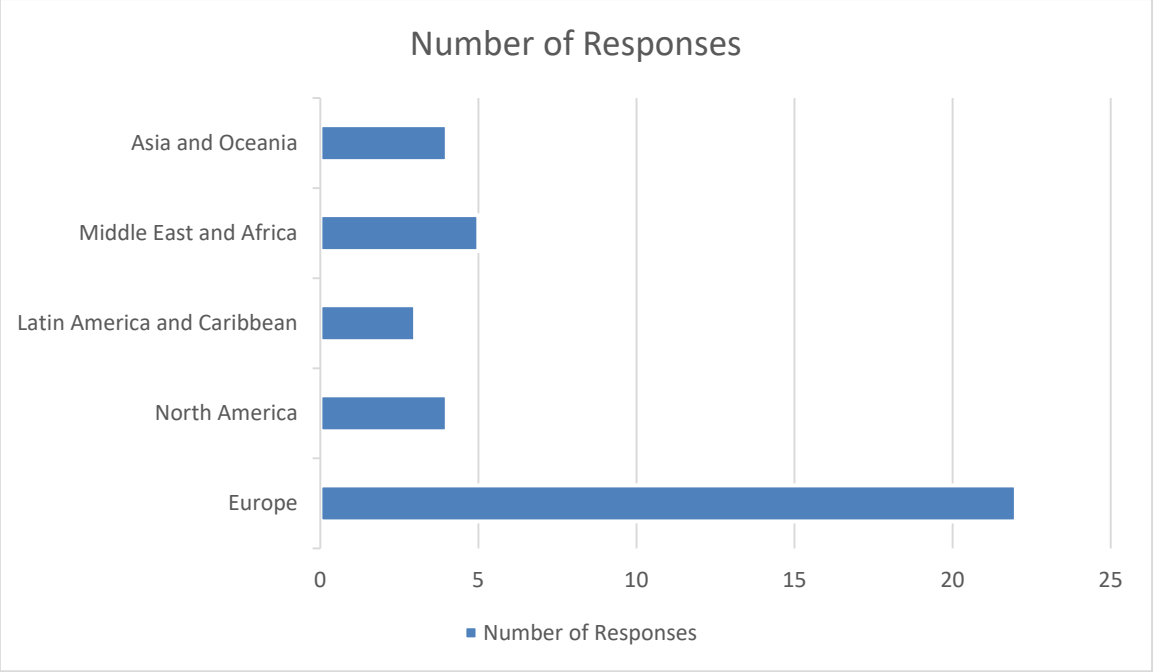
What is industrial domain is your company involved?



What is your main job function?



In which world region(s) does your company offer services/products?



A.3.2 Summary of results

The last part of the questionnaire gathered information related to the background of the responders, such their position in their company or their main job function.

The majority of the responders were either senior engineers/managers (11) or engineer/managers (6). The directors (4) and executives (2) were a smaller percentage of the responders. The main sectors of the responders were the cybersecurity (8) and the telecommunications (7). From the vertical domains, we received responses from the automotive (4), 5G service providers (4), network function virtualization vendors (4), and virtual network operators (2). Additionally, we received 2 responses from the academia. The main job function of the responders was research and development (13), network planning and design (5), and to lesser extend corporate management (2), and network management (1). All of the responders primarily offer their services to Europe (23), and to a significantly lesser extend to other parts of the world, such as middle east and Africa (5), north America (4), and Asia and Oceania (4).