ETSI ZSM Driven Security Management in Future Networks

Geoffrey Chollon, Dhouha Ayed
THALES
Paris, France
{geoffroy.chollon,dhouha}@thalesgroup.com

Rodrigo Asensio Garriga, Alejandro Molina Zarca, Antonio Skarmeta
Dept. of Information and Communications Eng.
University of Murcia (UMU)
Murcia, Spain
{rodrigo.asensio, alejandro.mzarca, skarmeta}@umu.es

Maria Christopoulou
Institute of Informatics and Telecommunications
NCSR Demokritos
Athens, Greece
maria.christopoulou@iit.demokritos.gr

Wissem Soussi, Gürkan Gür
Zurich Uni. of Applied Sciences (ZHAW)
Winterthur, CH
{sous, gueu}@zhaw.ch

Uwe Herzog
EURESCOM
Heidelberg, Germany
herzog@eurescom.eu

***Abstract*—This paper presents a security management framework driven by Zero-Touch Network and Service Management (ZSM) paradigm and embedded in the High-Level Architecture (HLA) developed in the INSPIRE-5Gplus project. This project work also included design and implementation of different smart 5G security methods and techniques that are essential for achieving security management in future networks. Moreover, the paper provides a summary of lessons learned and guidelines gathered during the practical validation activities for bringing closed loop and smart security management into Beyond 5G systems. Finally, we discuss the key challenges and future work needed to enable integrating closed-loop security management in future networks.**

***Index Terms*—Security management, ETSI ZSM, closed-loop management, 5G networks, 6G networks**

I. Introduction

6G will be a highly distributed computing and connectivity architecture. With the advances in softwarisation, the expectation that most of the software of a 6G system will be cloud-based. With the increased automation of management functionalities, more capable devices and integration of different potential technologies such as Distributed Ledger Technology (DLT), Native Artificial Intelligence (AI), THz communications and quantum computing, an attack surface will be exposed that will be more complex and challenging to defend compared to current 5G networks [1], [2]. The expected complexity will require to advance or complement traditional management security with AI/ML-driven and automated closed-loop mechanisms [3]. These developments should be based on widely accepted standards. In that regard, the ETSI Zero-touch Network and Service Management (ZSM) specifications have been key contributions [4].

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The EC is not responsible for any use that may be made of the information it contains.

This paper describes a smart security management framework that is compliant with the ETSI Zero-touch Network and Service Management (ZSM) reference architecture and the High-Level Architecture (HLA) developed in the INSPIRE-5Gplus project, namely *INS-HLA*. The framework integrates various software-defined and cognitive enablers in order to enable end-to-end (E2E) management in a closed-loop and smart way [5]. As a case study, we present practical experience from the design and implementation work and discuss some key aspects such as closed loop establishment, conflict resolution and policy management in such an automated management architecture.

This paper is organized as follows. Section II describes the main aspects of the ETSI ZSM concept and several key aspects for provisioning security in future networks. Section III describes a "small-scale" ZSM closed loop built around Moving Target Defense (MTD) enabler developed in the INSPIRE-5Gplus project to illustrate how ETSI ZSM is implemented in the INS-HLA. Section IV elaborates on how conflicts and priorities are managed when the closed loops are deployed in a multi-domain context. In Section V, we present how ZSM closed concept concept is realized in the INS-HLA. Finally, the conclusion provides a parallel with the ETSI ZSM vision.

II. ETSI ZSM and Key Aspects for Security Management

ZSM is a revolutionary architecture that employs the benefits of contemporary technologies and paradigms, e.g., AI, Network Function Virtualization (NFV), Software Defined Networking (SDN), and network slicing, to enable intelligent, autonomous, and agile management of cellular network architectures. ZSM separates the cellular network in distinct management domains, namely the Radio Access, Edge, Transport, Core and Cloud networks, following a "separation of concerns" approach. It uses policy languages as the primary communication tool between the provided services of its

This is the submitted manuscript version of a paper published by IEEE. The Version of Record is available at https://doi.org/10.1109/FNWF55208.2022.00065

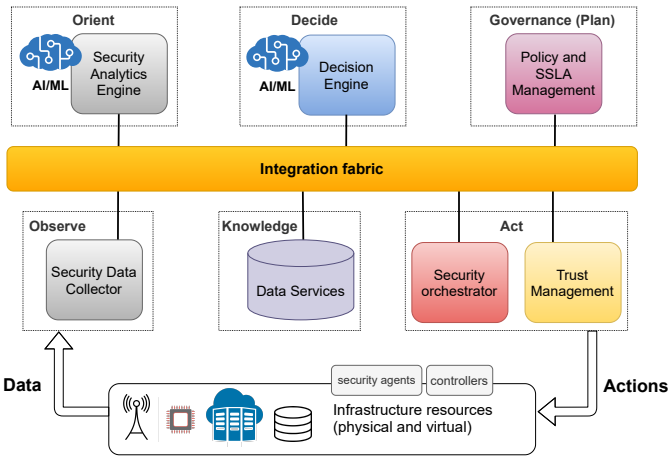


Fig. 1. INSPIRE-5Gplus closed-loop reference architecture and OODA stages.

architecture and includes an intelligent orchestrator as the primary engine to execute actions across the infrastructure. ZSM presents a single End-to-End (E2E) management domain with a global perspective of the underlying management domains, coordinating the overall workflow and decisions simultaneously. All management domains include a data service for storing information that are used for decision-making both on E2E and local management level, achieving the overall coordination of the network towards zero-touch network automation. All ZSM services communicate via an Integration Fabric,i.e., a common message interface.

ZSM has been designed to govern the NFV Infrastructure (NFVI) through closed loops that can be found in the different levels of the architecture. Closed loops are instrumental in realizing zero-touch network automation, because they define sets of recurring logical steps -from data collection to decision execution- for managing the services constituting a ZSM-based framework. There are intra- and inter-closed loops for the dynamic and autonomous management of the various domains locally or globally, allowing the decision-making to be escalated to the E2E domain, in case an action must be executed across the local management domains. This way, ZSM transforms network management into an autonomous, efficient and agile operation, simplifies the lifecycle management of the services and network, and reduces the Operating Expenses (OpEx) through self-managing capabilities (e.g., self-configuration, self-optimization, self-healing, and self-protection) [4].

In the INSPIRE-5Gplus project, we use ZSM to provide autonomous and intelligent security capabilities to the system. To do so however, we take into consideration that ZSM is composed of a wide set of technologies (e.g., virtualization, programmability, automation, AI/ML), where each one introduces a set of threats that must be studied and covered. We classified the potential security threats into five categories: (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

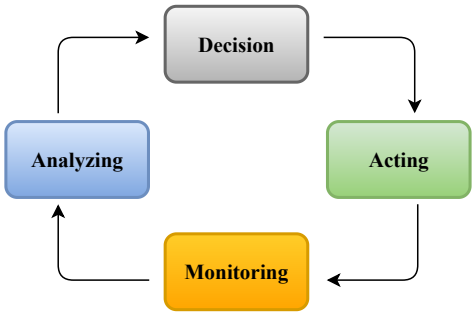


Fig. 2. ETSI Closed Loop.

adoption of programmable network technologies (i.e., NFV and SDN) [6] and mitigate them with appropriate controls, including adversarial AI/ML training and Trusted Execution Environments (TEEs).

III. Smart Closed Loops for Security Management

There are different models that describe closed loop mechanisms, such as the Orient-Observe-Decide-Act (OODA) and Monitor-Analyze-Plan-Execute (MAPE-K) [4]. Regardless of the steps definitions, such models follow a similar high-level workflow: Data Collection-Analytics-Decision-Execution, as shown in Fig. 2. Fig. 1 is a depiction of the OODA and MAPE-K principles adapted and applied to the INS-HLA, where a control loop runs on top of the infrastructure [7]. In the first *Observe* phase, the Security Data Collector gathers infrastructure data. In the second *Orient* phase, the Security Analytics Engine augments the data with extra information or correlations. Then in the third *Decide* phase, the Decision Engine finds the mitigation from the relevant event and the current infrastructure state. In the next fourth *Governance* phase, the Policy and SSLA Manager adapts the security mitigation relative to the security policies rules. Then in fifth *Act* phase, the Security Orchestrator enforces the mitigation inside the infrastructure.

A. MTD in ZSM-Oriented Closed Loop Mode

As a concrete realization of smart closed loop concept for security, we briefly elaborate on MTD operation integrated into our architecture in this section. Please refer to [8] for further information on how MTD is integrated to the developed security architecture. Moreover, you can find how other INS-HLA enablers are integrated in [7].

1) Observe: As MTD components evaluate and enforce proactive and reactive MTD strategies, they collect various data for the evaluation of the attack surface and attack success probability of possible attacks (proactive case), and attack detection alerts from security agents and anomaly detection systems (reactive case).

For the proactive case, MTD collects network performance measurements, consumption of computing resources, and vulnerability scans of the VNFs used in the infrastructure. Network measurements come from monitoring probes that can be installed directly in the VNFs or in the Virtual Infrastructure

Managers (VIMs), via port mirroring (or port forwarding). The consumption of computing resources comes from the VIMs, such as Openstack, observing CPU cores, RAM, and storage consumption, and keeping count of the remaining available resources. The vulnerability scans are triggered by MTD and are implemented using the Open Vulnerability Assessment Scanner (OpenVAS) vulnerability scanner.

For the reactive case, MTD collects attack alerts from the security agents which can detect security incidents and anomalies that vary from the normal behaviour of the VNFs. Such anomalies can be generated by Advanced Persistent Threats (APTs), such as installed malware (e.g. spyware), C&C, or backdoors. Attack alerts are received together with information on the VNF target and the attack type.

2) Orient: In the proactive case, MTD evaluates the attack surface of each resource in the network by finding related vulnerabilities, listed as Common Vulnerability Enumeration (CVE) entries. CVEs found by the vulnerability scans are classified as vectors of different types of attacks, such as APTs, data leaks, and DoS attacks. This classification is done based on their mapping with Common Weakness Enumeration (CWE) entries and on keyword matching. The CVSS base scores and exploitability scores of such CVEs are then aggregated based on this classification. Finally, we estimate the reduction of the attack success probability (ASP) on the resources based on their attack surface and the estimated effect of each MTD action on each attack type (considering the frequency of the MTD action as a parameter).

3) Decide: In the proactive case, this data and its augmented evaluations are used for the multi-objective deep Reinforcement Learning (RL) training, which identifies three objectives: operational cost of MTD operations using a cost formula, security improvement by reducing the ASP and increasing the attack surface shifts, and the network overhead by keeping network performances stable. The RL agent is implemented in a continuous learning setup as it updates the ML model periodically based on the MTD operations that have been decided and the measurements received from the environment.

In the reactive case, MTD can rely on two mitigation policies: learned mitigation policy based on the specific attack detected, and manually defined mitigation policy by the network administrator. The learned mitigation policy is part of the autonomous RL optimization policy, where the agent learns the optimal mitigation policy based on whether the attack stopped its effect or not, which will lead the security agents to stop sending attack alerts. The manually defined mitigation policy can be used when the best mitigation to an attack is known by the network administrator who forces MTD to use it instead.

4) Governance and Act: After the decision of on the MTD action, MTD enforces the action coordinating operations imparted to the network slice manager and the OSM NFVO.

IV. Closed loop and E2E coordination

One of the main challenges that the INSPIRE-5Gplus project targets is the support of E2E security management in a multi-domain context. Handling separate Security Management Domains (SMDs) raises a set of issues since the closed loops need to deal with the enforcement of security policies in multiple domains that provide various capabilities. Conflicts may then arise when applying a policy or a decision. This section describes the coordination that happens at the core of the INSPIRE-5Gplus smart closed-loops to illustrate how the closed loop concept can be integrated into security management. We elaborate on the conflict and policy management as key requirements of closed loop implementation. A closed loop hierarchical organisation is then detailed.

A. E2E Security Policies Management

Policy management at the E2E level is part of the closed management loop. It maintains the objective of ensuring compliance with the SSLAs on network services contracted with a vertical through the security management of network slices. The closed policy management loop has two possible entry points on the E2E Security Orchestrator (SO). The first entry point, the proactive one, deploys the network service and security services that ensure compliance with the security requirements set forth in the SSLAs, while the other entry point, the reactive one, generates countermeasures that maintain SSLA compliance when a change in context (e.g., an attack) compromises them. The proactive part receives the policy from the E2E Slice Manager. This policy is an Orchestration Policy that contains in MSPL-OP language [9] the translation of the SSLA: a network service that must be deployed and some security requirements that must be associated to that service, all this as part of an E2E Network Security Slice. When the E2E SO, receives this policy, it first examines it to detect that it is a security slice, this makes the E2E SO build a policy per domain, where each policy is considered a sub-slice, this sub-slice contains: the service in case this domain is the target of the service, and the security requirements to be deployed in the domain. In other words, for each domain, the E2E SO builds an orchestration policy that accumulates the necessary requirements to be deployed so that the security requirements established in the SSLA are fully met.

The construction of each orchestration policy per domain is called “enforcement plan”. Each policy has an associated priority level that allows the orchestrator to dictate in which order the policies should be applied. As each orchestration policy of the enforcement plan may contain multiple policies, the highest priority of the set of policies belonging to that orchestration policy will be applied, so the enforcement plan is sorted by domain priority. The reactive part refers to the entry point from the E2E Decision Engine (DE), triggered as part of a reactive process given from the Security Analytics Engine (SAE) when an anomaly is detected. The main difference of the reactive orchestration policies generated by the E2E DE is that they do not have to contain inside as a capability the 5g_security_slice, in which case the flow varies since the enforcement plan does not generate a single orchestration policy per domain but generates several orchestration policies

per domain and they are applied (i.e. sent to the SMD SO) depending on their individual priority.

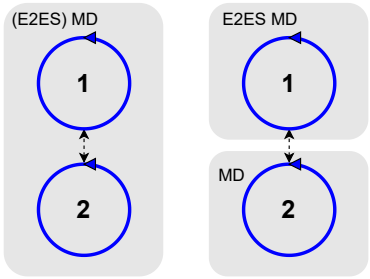
B. Conflict Management

The conflict detector module belongs to the Policy Framework. This module is in charge of maintaining policy consistency during the closed management loop through a system of rules provided by Pyke engine [10]. Specifically, the conflict detection is a step during the orchestration process, prior to policy enforcement. The module receives a security policy for orchestration expressed in MSPL-OP language (e.g., Filtering, Channel Protection, etc.), evaluates all the parameters included in the policy and try to match them with the corresponding rules defined in the rule engine. This process takes as the input the MSPL-OP and check that the parameters can be applied to the specific policy type, but it also verifies that the new policy does not conflict with any already enforced policies. The policies maintain a status, the new ones are incorporated as "pending" and those that are retrieved from the policy repository, if they are still applied, their status will also indicate it. First those that were already applied are added to the rules system, and then the policies belonging to the MSPL-OP will be added. Thus, each "pending" policy will be passed through the rule engine and matched against already enforced policies and against the other policies of the MSPL-OP. During this process, it is for example checked that the policy has not already been applied or that an action does not contradict another already applied (e.g., ALLOW and DENY). After this process called Inference, new conclusions can be added to the knowledge base, and can be further used to detect new conflicts.

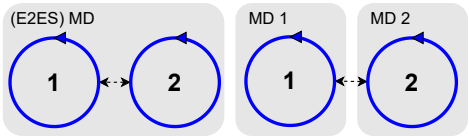
Through the knowledge base facts, we can add objects with different characteristics necessary to correctly perform the conflict detection. For example, we add to the fact base the different capabilities that a given domain has, focusing on the E2E perspective, the conflict detector performs a search for inter-domain conflicts, e.g., the possibility that between two domains that are going to establish a channel protection using the same key and protocol parameters (IPsec/DTLS). To do this, the capabilities of each domain are added to the fact base, and when the Channel Protection policy is received, it is verified that each domain involved in the MSPL has the necessary capabilities to apply the policy. In case the Conflict Detector detects a conflict, an alert is triggered indicating a risk and the orchestration process is stopped so that the Decision Engine can take appropriate action. The rules to perform the E2E Channel Protection conflict detection can be found below:

```
MSPL(?m1)^(hasnot(m1.dest.domain1, m1.capability) ||
hasnot(m1.dest.domain, m1.capability))
→ ``Capability in Domain Missing(?m1)"
```

The Conflict Detection module allows to ensure the robustness of the system while maintaining and benefiting from the flexibility of the policies since it can be extended to cover new security assets or domains, or even adapt it to new conflicts discovered.



(a) ETSI Hierarchical Closed Loops.



(b) ETSI Peer Closed Loops.

Fig. 3. ETSI closed loops [11].

C. Hierarchical organization

1) Decision delegation/escalation: While running a local closed loop, the local SMD Decision Engine may forward the alerts to the E2E level. It provides an autonomous local ZSM closed loop in the domain that enforces fast reactions. In an escalation context, the forwarded event can trigger more mitigations at the E2E Decision Engine level. For example, a local mitigation stopping a brute force attack can be broadcasted to the others domains. Sometimes, the local SMD closed loop is unnable to react due, for example, to missing capabilities in the local domain. In this context, SMD Decision Engine cannot take any mitigation and by forwarding the event to the E2E level, it delegates the decision.

2) Policies hierarchical enforcement for E2E security: The E2E Decision Engine delegates the global enforcement to the global Security Orchestrator residing at the top level. The E2E SO manages the technical details on how to split and forward the global policies downward. The E2E Security Orchestrator verifies the capabilities of a subordinate domain before translating the policies to the required format.

V. ETSI ZSM CLOSED LOOPS SUPPORT IN THE INS-HLA

The ETSI, in the "Closed-Loop Automation; Part 1: Enablers" document, defines two types of closed loops [11]:

- Made-to-order closed loops (M2O-CL) which are built and deployed on demand by the ZSM framework.
- Ready-made closed loops (RM-CL) which are created by the ZSM vendors without any further dynamism.

In such context, the ZSM loops presented in the INS-HLA are inside the Ready-made loop, as each component was selected and assembled around a main enabler. A subset of the M2O-CL is also supported as some components of a closed loop are dynamically deployed (for example the monitoring probes). The commissioning phase is prepared statically and the operational phase is static. Moreover, in terms of governance, the INS-HLA does not integrate a global

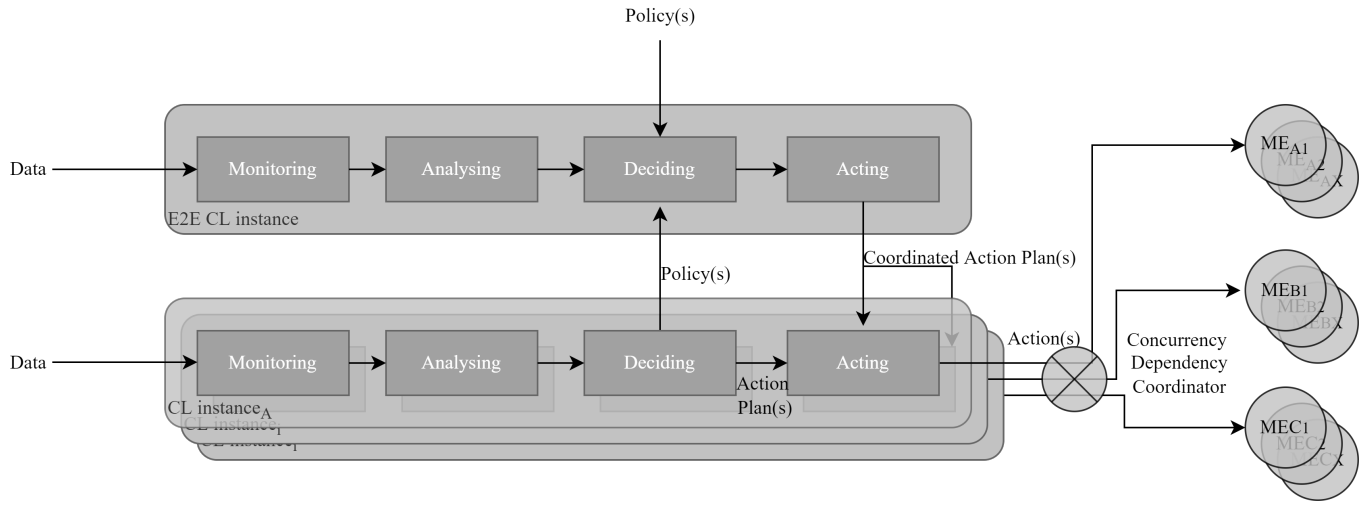


Fig. 4. ETSI exemplary Closed Loop Coordination timeline [11].

management life cycle of the closed loops or their models. The closed-loops of the INS-HLA focus on the lifecycle of the managed entities (network slices, security policies, etc.). ETSI defines the ability of the ZSM framework to monitor KPIs and adapt the closed loops and their models to optimise the closed-loops set goals. In this regard, on the two basic type of policies, the INS-HLA uses the service policy type to control the security around a running service based on the externally observable behaviour: attack pattern or security warning. The resource policy type optimizing the delivery of constraints around a service is used during on-boarding with the refinement of SSLAs into lower level MSPL manifests.

ETSI introduces two types of coordination between multiple concurrent running closed-loops that defines the delegation and escalation between them. Moreover, these types can also be classified based on the domain where the closed-loops are deployed. The hierarchical model, shown in the Fig. 3(a), where a top-level closed-loop manages a set of underlying closed-loop, running either in the same domain or in a separate domain. In the peer model in Fig. 3(b), each closed-loop is independent but can influence each other's behaviour with a flexibility in their domain deployment. ETSI refines the hierarchical model as a mode where the subordinate closed-loops are managing the local domain targeting a self-healing goal and local optimum, whereas the top-level domain focuses on a global or end-to-end optimum. In this scenario, the subordinate might take conflicting decision, which the top-level can coordinate and orchestrate. The coordination can involve:

- Delegation: where the top-level pushes global order down to the subordinates closed-loop.
- Escalation; where the subordinate close-loops inform the top-level loop of local events.

In the INS-HLA, the employed ZSM closed-loop framework is of a hierarchical type. Each local Security Management Domain (SMD) contains a closed-loop. This loop manages the local security deployment. Then it escalates the local decision to the top-level End-to-End (E2E) domain for further interactions. Yet the final coordination is hybrid since in the E2E level the side-effect is managed by a global Security Orchestrator which crafts and delegates the policies down to each SMD Security Orchestrator.

Fig. 4 displays an example timeline of some coordination between two closed-loops where multiples Managed Entities (ME) are manipulated by concurrent closed-loops. Each closed-loop has its computing model ingesting data from monitoring probes, analysing it, taking a decision based on it and executing it. With that, some conflicts might appear in the executed actions. The INSPIRES-5Gplus ZSM framework follows the same pattern with equivalent OODA loops as exemplified in Section III. As for the conflicts, the hierarchical model has some priority level parameters and the Security Orchestrator has a conflict detection component for the security policies. As for the impact assessment, as the project focuses on security, the goal is achieved when the originating probe acknowledges the disappearance of the threat.

ETSI also introduces some services for the ZSM closed-loop governance. The INSPIRE-5Gplus framework covers a subset. For example, in the Closed Loop Governance (CLG) service, the "Escalate issue" capability is covered by the local Decision Engine to the E2E level. The "Manage Closed Loop goal" is covered by the local Security Orchestrator which handles the local security goal achievement. In the Pre-execution coordination service, the "Provide notifications of conflicting action plans" capability is also performed by the local Security Orchestrator within the scope of the security policies manifests.

Finally, the ETSI "Means of Automation" document introduces the concept of entities governance trough policies [12]. While in ETSI those policies can cover multiple aspects from QoS to energy, the INS-HLA targets the management of security. In the ETSI approach the Policy Continuum

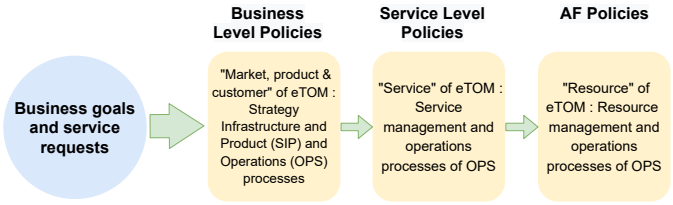


Fig. 5. ETSI policy levels defined in [12].

preserves the policy relationships in each level of abstraction. The policies are translated between each level with a set of potential dependencies between them.

Fig. 5 shows those the possible policy levels from the ETSI point of view.

- The `Business Level` Policies: correspond to the "Market, product & customer" layer with global and generic constraints. This level is represented by the HSPL (High Level Security Policy) layer in the INS-HLA [13] that allows modeling high-level security requirements, priorities and dependencies independently from underlying technologies.
- The `Service level` and `AF level`: is the intermediate level where generic resources are configured. This level is represented by the MSPLs (Medium Security Policies) and SSLAs layer in the INS-HLA [13].
- The `AF policies` level: is where the entities are manipulated and the policies enforced. In the INS-HLA, MSPLs are translated to lower level rules that are enforced by security and network controllers.

With that work, the INS-HLA approach was successful to build several "specialized" ZSM closed-loops. For more information on these closed loops based on developed security enablers, please refer to [7]. The pay-off was a local management of a security aspect (relative to each enabler).

VI. Conclusion

This paper describes how the INSPIRE-5Gplus smart security management framework follows the ETSI ZSM paradigm. The enablers in this framework implement the most important HLA capabilities starting from intelligent data collection and analysis and accurate runtime monitoring of virtualized 5G environments to cognitive and efficient prevention, detection and mitigation of security in multi-tenant, multi-domain network infrastructures. The paper details the establishment of ZSM closed loops based on those enablers for security and provides solutions to manage policies, conflicts and priorities when closed loops are deployed in a multi-domain context. An important future work is for that framework to be tested in the demonstration related work where a subset of enablers will be combined to create an overall ZSM framework across multiple domains.

References

[1] C. J. Bernardos and M. A. Uusitalo, "European vision for the 6G network ecosystem," Jun. 2021. [Online]. Available: https://doi.org/10.5281/zenodo.5007671

[2] P. Porambage, G. Gür, D. P. Moya Osorio, M. Livanage, and M. Yliantila, "6g security challenges and potential solutions," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, pp. 622–627.

[3] B. M. Khorsandi *et al.*, "Hexa-X deliverable D1.3: Targets and requirements for 6G - initial E2E architecture," Mar. 2022. [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D1.3.pdf

[4] ETSI, "Zero-touch network and service management (ZSM); reference architecture," https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf, Group Specification ZSM 002 V1.1.1, Aug. 2019.

[5] J. Ortiz *et al.*, "INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3407023.3409219

[6] C. Benzaid and T. Taleb, "ZSM Security: Threat Surface and Best Practices," *IEEE Network*, vol. 34, no. 3, pp. 124–133, May 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8994962/

[7] INSPIRE-5Gplus Project, "INSPIRE-5Gplus - D3.4 smart 5G security," https://www.inspire-5gplus.eu/wp-content/uploads/2022/07/i5-d3.4_smart-5g-security_v1.0.pdf, Accessed on 17.08.2022.

[8] W. Soussi, M. Christopoulou, G. Xilouris, and G. Gür, "Moving target defense as a proactive defense element for beyond 5G," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 72–79, 2021.

[9] A. M. Zarca, J. B. Bernabé, J. Ortíz, and A. Skarmeta, "Policy-based definition and policy for orchestration final report." [Online]. Available: http://www.anastacia-h2020.eu/deliverables/ANASTACIA-WP2-T2.1-UMU-D2.5-PolicyBasedDefinitionAndPolicyForOrchestrationFinalReport-v1.0.pdf

[10] B. Frederiksen, "Applying expert system technology to code reuse with pyke," *PyCon: Chicago*, 2008.

[11] ETSI, "Zero-touch network and service management (ZSM); closed loop automation; part 1: Enablers," https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/00901/01.01.01_60/gs_ZSM00901v010101p.pdf, Group Specification ETSI GS ZSM 009-1, June 2021.

[12] ——, "Zero-touch network and service management (zsm); means of automation," https://www.etsi.org/deliver/etsi_gr/ZSM/001_099/005/01.01.01_60/gr_zsm005v010101p.pdf, Group Specification ETSI GR ZSM 005-1, May 2020.

[13] INSPIRE-5Gplus Project, "INSPIRE-5Gplus - D3.2 security drivers and associated software-defined models," https://www.inspire-5gplus.eu/wp-content/uploads/2021/11/i5-d3.2_5g-security-drivers-and-associated-software-defined-models_v1.3.pdf, Accessed on 20.08.2022.