The Owner, the Provider and the Subcontractors: How to Handle Accountability and Liability Management for 5G End to End Service

Chrystel Gaber, Ghada Arfaoui, Yannick Carlinet, Nancy Perrot, Laurent Valleyre, Marc Lacoste, Jean-Philippe Wary
firstname.name@orange.com
Orange Labs France
Châtillon, France

Yacine Anser
Orange
Châtillon, France
CNAM
Paris, France
yacine.anser@orange.com

Rafal Artych
Aleksandra Podlasek
Orange Polska
Warsaw, Poland
firstname.name@orange.com

Edgardo Montesdeoca
Vinh Hoa La
Montimage
Paris, France
edgardo.montesdeoca@montimage.com
vinh_hoa.la@montimage.com

Vincent Lefebvre
TAGES
Paris, France
vincent@solidshield.com

Gürkan Gür
Zurich University of Applied Sciences
Winterthur, Switzerland
gueu@zhaw.ch

ABSTRACT

The adoption of 5G services depends on the capacity to provide high-value services. In addition to enhanced performance, the capacity to deliver Security Service Level Agreements (SSLAs) and demonstrate their fulfillment would be a great incentive for the adoption of 5G services for critical 5G Verticals (e.g., service suppliers like Energy or Intelligent Transportation Systems) subject to specific industrial safety, security or service level rules and regulations (e.g., NIS or SEVESO Directives). Yet, responsibilities may be difficult to track and demonstrate because 5G infrastructures are interconnected and complex, which is a challenge anticipated to be exacerbated in future 6G networks. This paper describes a demonstrator and a use case that shows how 5G Service Providers can deliver SSLAs to their customers (Service Owners) by leveraging a set of network enablers developed in the INSPIRE-5Gplus project to manage their accountability, liability and trust placed in subcomponents of a service (subcontractors). The elaborated enablers are in particular a novel sTakeholder Responsibility, AccountabIity and Liability deScriptor (TRAILS), a Liability-Aware Service Management Referencing Service (LASM-RS), an anomaly detection tool (IoT-MMT), a Root Cause Analysis tool (IoT-RCA), two Remote Attestation mechanisms (Systemic and Deep Attestation), and two Security-by-Orchestration enablers (one for the 5G Core and one for the MEC).

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX

CCS CONCEPTS

• **Networks** → **Network manageability**.

KEYWORDS

Liability, management, 5G, service provider, verticals, security, supply chain

ACM Reference Format:
Chrystel Gaber, Ghada Arfaoui, Yannick Carlinet, Nancy Perrot, Laurent Valleyre, Marc Lacoste, Jean-Philippe Wary, Yacine Anser, Rafal Artych, Aleksandra Podlasek, Edgardo Montesdeoca, Vinh Hoa La, Vincent Lefebvre, and Gürkan Gür. 2018. The Owner, the Provider and the Subcontractors: How to Handle Accountability and Liability Management for 5G End to End Service . In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (ARES 2022).* ACM, New York, NY, USA, 7 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

5G networks play a fundamental role in the implementation of pervasive and digital services with anytime-anywhere connectivity. To this end, they are envisaged to be extremely flexible and dynamic to fulfill the myriad of use cases and verticals with very different requirements such as ultra-low latency or ultra-reliability. The Key Verticals expected to drive the wider adoption of 5G are the automotive industry, the smart city and public safety enablers, Industry 4.0, Healthcare, Energy and Entertainment.

Some of these Verticals must comply with stringent safety and cybersecurity legal obligations that can be translated into requirements for underlying 5G End to End (E2E) services, thereby creating additional stimulus to adopt such services. For example, healthcare, transport, energy and water supply services are considered as Operators of Essential Services (OES) by the European Network and Information Security (NIS) Directive because their interruption would have a significant impact on the functioning of the economy or society [5]. As such, they have to protect themselves against

Published version DOI: https://doi.org/10.1145/3538969.3544465

cyberattacks and can delegate or enrich some of these controls with services provided by 5G E2E Service Providers. Domain-specific regulation or standards like ISO 14971 for Health [12] or SEVESO [6] for industry also impose controls that can be translated into requirements for privacy, isolation of processing or network component certification levels.

However, the difficulty to track and demonstrate responsibilities in the multi-party and multi-layer 5G architecture hinders the adoption of 5G E2E Services. Indeed, given that zero-risk security cannot be achieved, the definition of liability and responsibilities when security breaches occur is essential to support confidence between parties and compliance with regulation.

Moreover, the strategy to implement the highest level of security is unrealistic. For instance, some requirements may be incompatible. Most use cases do not need the strongest security level while verticals will be reluctant to pay for services that they do not need and do not use. And maintaining such an security level for all network and service components is a massive task that could increase the costs of some configurations in an inconsiderate manner.

Contributions. In this work, we combined eight INSPIRE-5Gplus enablers to form a management system which follows the principles of the Liability-Aware Management Service proposed by [9]. We demonstrate it in a use case where a 5G E2E Service Provider supports an industrial entity in demonstrating that its critical services are isolated, which is a legal obligation towards NIS Directive. We also show how the E2E Service Provider achieves this by committing to provide evidence of isolation at service level (also known as Service Level Isolation - SLI) to dynamically manage this constraint and to allow the customer to verify the status of the committed SSLA and Key Performance Indicators (KPIs) on the fly. To the best of our knowledge, there is very limited work on liability management systems for 5G E2E Service management as most existing management systems do not cover liability, target 5G use cases or aim to serve 5G E2E Service Providers.

Paper structure. The paper is structured as follows. Section 2 presents related works and demonstrates the novelty of our approach. The use case and the demonstrator developed in the INSPIRE-5Gplus project are detailed in Section 3. In Section 4, we describe the functional blocks of the Liability-Aware Management Service described in [9] and analyze how each enabler involved in the demonstrator contributes at its level to manage liabilities in one of the functional blocks described in Section 4.2. Finally, Section 5 concludes our work and presents future work.

2 RELATED WORKS

To the best of our knowledge, there is very limited work on liability management systems for 5G E2E service management as most existing management systems do not cover liability or do not target 5G use cases. At the cloud computing front, the Cloud Accountability project (A4Cloud) [1] has focused on accountability management tools to manage personal data in cloud services. For virtualized network services, the ETSI report on quality accountability framework [8] defines general principles for accountability management, roles and associated responsibilities in the NFV management system, but their work is limited to performance.

Guemkam et. al. [10] propose an Information System Security Risk Management meta-model including responsibility, accountability and commitment that was used to create a multi-agent system-based architecture for broadcasting forecasts and alerts in a power distribution infrastructure. Bonhomme et.al. [4] adapted this model to develop a decision mechanism for incident reaction in telecommunications network, but it is not adapted for the 5G Slicing context.

The closest approach to ours is the work by Hatzivasilis et al [11]. They describe a cyberinsurance tool which calculates insurance fees, alerts customers on potential violations and applies penalties to the entities at the origin of the violation. The main difference between their approach and ours is the separation of concerns. Our point of view is that of a 5G E2E Service Provider who aims at operating its E2E Service while minimizing its SLA violations, insurance fees and penalties. Their proposed tool targets the insurer who hedge risks.

Finally, there are Contract Management Systems such as ContractWorks [7], Juro [13] or Medius [14] to manage the creation, negotiation, signature, renewal, storage, reporting and data analysis of contracts. However, they are not designed to monitor and operate 5G E2E Services. Nonetheless, we can consider them as a blueprint for future research and extending our work.

3 USE CASE AND DEMONSTRATION DESCRIPTION

3.1 Use Case

In our use case, the E2E Service Provider (Orange) creates a multi-domain service for his industrial customer Acme Inc. (E2E Service Owner). The service spans from a local network in an IoT campus up to the Core Network and an Edge Network close to the customer's premises. It ensures the transport of the data collected from the IoT devices in the industrial campus and hosting of MEC applications processing these data. Based on anomaly detection and Root Cause Analysis, the E2E Service Provider also provides a surveillance service of the IoT Campus. Finally, depending on the nature of anomalies detected, the E2E Service Provider switches the service in a specific mode with enhanced security, which is named "critical mode". This critical mode ensures that the collected data is processed throughout the E2E Service by untampered functions which are co-located only with functions of the same criticality. The E2E Service Provider charges a fixed Monthly Recurring Charge (MRC) for the normal mode and a Pay-Per-Use (PPU) fee for the temporary activation of the critical mode. Both modes are defined in the contract between the E2E Service Provider and its customer.

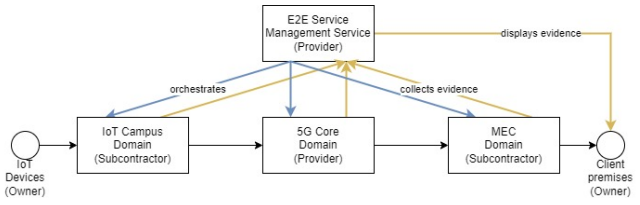

Figure 1: Overview of the demonstrator set up

Published version DOI: https://doi.org/10.1145/3538969.3544465

3.2 Demonstrator set-up

Based on this use case, we built a demonstrator in the scope of the INSPIRE-5Gplus project. Figure 1 provides a overview of the demonstrator. It involves three actors (Orange, Montimage, TAGES) and three roles (E2E Service Provider, Domain Service Provider and Component Providers). Orange plays the role of E2E Service Provider, Domain Service provider for 5G Core and the Multi-Access Edge (MEC) Domains. Orange also plays the roles of Component Provider by providing orchestrators, deep attestation mechanisms and infrastructure. Montimage plays the role of a Domain Service Provider which ensures the collection of events, monitoring of network-related data, and detection anomalies in the IoT Campus Domain. Montimage also plays the role of Component Provider by using its own software and infrastructure to realise these tasks. It relies on the Systemic Component provided by TAGES to get its software protected against various forms of attacks. TAGES therefore plays the role of Component Provider.

The demonstrator integrates eight network enablers developed in the INSPIRE-5Gplus project. In the IoT Campus Domain, the enabler IoT-MMT monitors network events and detects anomalies. The IoT-RCA enabler analyses the anomalies and determines a root cause for an incident. The Systemic enabler detects specific attacks on the software and reports them. The 5G Core Domain contains a Security Orchestrator which takes decisions based on risk assessment and vulnerability scores as well as a Deep Attestation - Remote Attestation Agent and Server [3]. The MEC domain also contains an orchestrator which takes the decision of MEC application placement using Security by Orchestration for MEC enabler. A Liability-Aware Service Manager is used in order to create the sTakeholder Responsibility, AccountabIility and Liability deScriptor (TRAILS) of the service as defined by Gaber *et. al* [9].

3.3 Demonstration scenario

The first demonstration scenario shows how the LASM-Referencing Service and TRAILS help the Service Provider build a service. The E2E Service Provider selects components among the catalog of available TRAILS which comply with customer requirements. When it combines them, the LASM generates the TRAILS for the composed service and assists the Service Provider to generate the SSLA for the resulting composition.

The second scenario highlights how the 5G Core and MEC orchestrators deploy and manage dynamically on-demand service level isolation. Based on the alert provided by the IoT Campus, the critical mode is activated. This triggers the placement of the virtual functions and MEC applications by the orchestrators so that they are colocated only with functions of the same criticality level.

Finally, in the third scenario, we show how different forms of evidence (the Systemic remote attestation, the deep attestation remote attestation and the logs recorded by the MEC orchestrator) are collected and aggregated to demonstrate isolation at service level for the E2E Service.

4 ACHIEVING ACCOUNTABILITY AND LIABILITY MANAGEMENT

This section analyses how the combination of INSPIRE-5Gplus enablers achieves liability-aware management of services.

4.1 Background on accountability, liability and trust

As defined in [2], accountability corresponds to the expectation for an *accountor* to provide elements of proof in order to demonstrate to an *accountee* that a task was performed as expected on a technical, design or policy level. Liability on the other hand corresponds to accountability towards the law. In this case, the accountor is an actor subject to legal or contractual requirements and the accountee is the judiciary system.

As in [2], we differentiate the notions of responsibility and liability. While responsibility reflects that one has a duty to perform a task as defined in a set of pre-agreed objectives, liability reflects that one is required to do so by a law or a contract and may have to justify the realisation of this task in court.

Trust on the other corresponds to a *trustor*'s belief that the *trustee* will perform a task while complying with a set of pre-agreed objectives. Möllering [15] shows that trust and control are two dual concepts in the sense that they are inevitably connected and have a reflexive influence on one another. By combining several elements of trust and control, an actor reaches positive expectations of other actors and, as a result, remaining uncertainty becomes acceptable for him.

Given that liability towards contractual commitment or legal requirements influence the scope of controls and that trust is a foundation to negotiate legally binding agreements or contracts, we believe that liability and trust are also dual concepts.

4.2 Liability-Aware Service Management functional blocks

Based on [9], we identify that a liability management service requires three functional blocks, as depicted in figure 2.

The first functional Block FB.1 consists of identifying the governance required to set up the E2E or Domain service, the evidence required to demonstrate compliance to regulation and contractual agreements and the liability relationships among actors (customers, E2E or domain service providers and subcontractors).

FB.2 consists of monitoring for accountability evidences. Security agents collect the evidences from the infrastructure as identified by the first functional block. The first objective is to demonstrate compliance with legal obligations or contractual agreements by using Remote Attestations, Path Proof Protocol or by collecting logs. The second objective is to identify and trace events or incidents.

Finally, FB.3 objective is to analyse the evidences of events/incidents collected by FB.2. Based on the liability relationships identified by FB.1, FB.3 can qualify compliance or potential violations and resolve responsibilities. FB.3 then provides reports to administrators or jurists to support further forensic investigations or negotiations to settle disputes. The output of FB.3 can also be used by billing systems in order to calculate penalties or remediation expected by

Published version DOI: https://doi.org/10.1145/3538969.3544465

the customer from the E2E Service Provider or by the E2E Service Provider from his subcontractors.

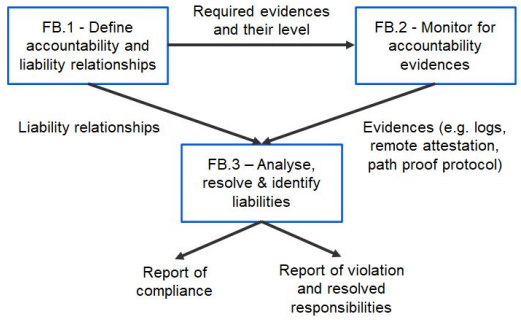

Figure 2: Functional blocks of a liability-aware management system

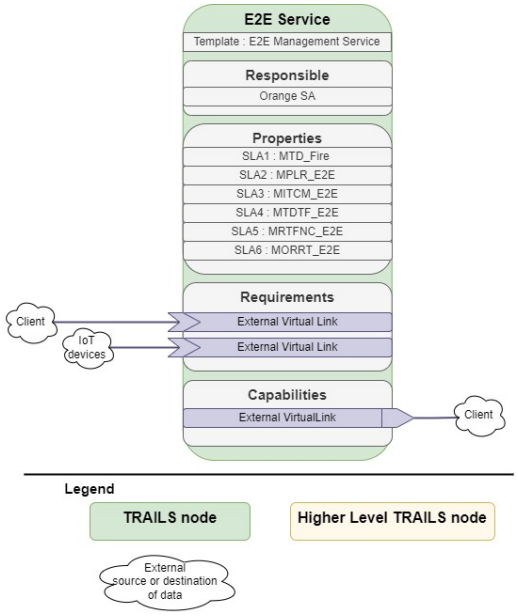

Figure 3: E2E Service Topology Layer 0

4.3 Identification of liability relationships

The responsible party of a Component is mandated to provide the TRAILS manifest which corresponds to the Component. As described in [2], the TRAILS manifest keeps tracks of the contractual agreements taken by the Component's responsible entity and translates them into technical SLAs that can be read and interpreted by a machine. TRAILS manifests can also be used to express Operational Limitations, additional constraints on the Component in order to make it comply with the context where the Component can be deployed. Usage Conditions, on the other side, allows the supplier to define recommendations for the Users so that the Component behaves as expected.

Figure 3, 4 and 5 are examples of the topology view that the LASM-RS displays when a TRAILS manifest is imported in the system. For the sake of brevity, we do not display here the views generated for the layer 1 5G Core and MEC domains. With these views, the administrator can explore layer by layer the architecture of the E2E service, the relationships between its components, the responsible entity of the component as well as the SLA committed by the responsible entity / integrator of the component.

Figure 3 shows the overall view of the service and the SLA committed by Orange as the E2E Service Provider. The first SLA is the Mean Time To Detect a Fire (MTD_Fire) which corresponds to the event which triggers the critical mode. The second SLA is the Mean Packet Loss Ratio (MPLR) calculated between the entrance in the E2E Service and the reception by the dashboard in the MEC. The third SLA is the Mean Initial Time for Critical Mode (MITCM) which corresponds to the time between the moment the E2E Service Manager activates the critical mode and the moment the critical mode is actually activated in all three domains. The fourth SLA is the Mean Time To Detect Tampering or incorrect location of Function (MTDTF), Mean Ratio of Time Functions are Not isolated In Critical mode (MRTFNC) which corresponds to the average time required to detect an issue with the isolation at service level in one of the three domains. Finally, the sixth SLA corresponds to the Mean Observation Report Response Time (MORRT) which corresponds to the average time between the client's request to receive evidence of Service-Level Isolation property and the response provided by the E2E Service Manager with the aggregated responses from the IoT Campus, 5G Core and MEC domains.

Figure 4 shows that the E2E Service Manager is responsible for activating the critical mode in each domain (IOT Campus, 5G Core and MEC) and aggregating the evidence collected from each domain before providing it to the client. It also shows that the E2E Service Management Service is responsible for delivering the KPIs committed in the SLA. This view also illustrates how the first level of subcomponents interact with each other and their individual SLAs.

Figure 5 depicts the IoT Campus Domain. In particular, we can see that the logs produced by the IoT-ML and IoT-RCA components and the remote attestations produced by the Systemic Agent are transferred to the E2E Service Management Service for aggregation with the metrics collected from the other domains. The 5G Core and the MEC Domain are organized similarly.

Figure 6 shows the responsibility view that the LASM-RS displays when a TRAILS manifest is imported in the system. With this view, the administrator can visualize the perimeter of each component or service provider as well as the responsibility relationships which are distributed among entities.

4.4 Monitoring of compliance or collection of violation evidences

Both orchestrators provided by Orange ensure the Service-Level Isolation of the services in the 5G Core and MEC Domains. Then, the Systemic Component, Deep Attestation Server and agents create evidences that can be used to demonstrate that the Domain or E2E Services comply with the contract clauses agreed between Supplier

Published version DOI: https://doi.org/10.1145/3538969.3544465

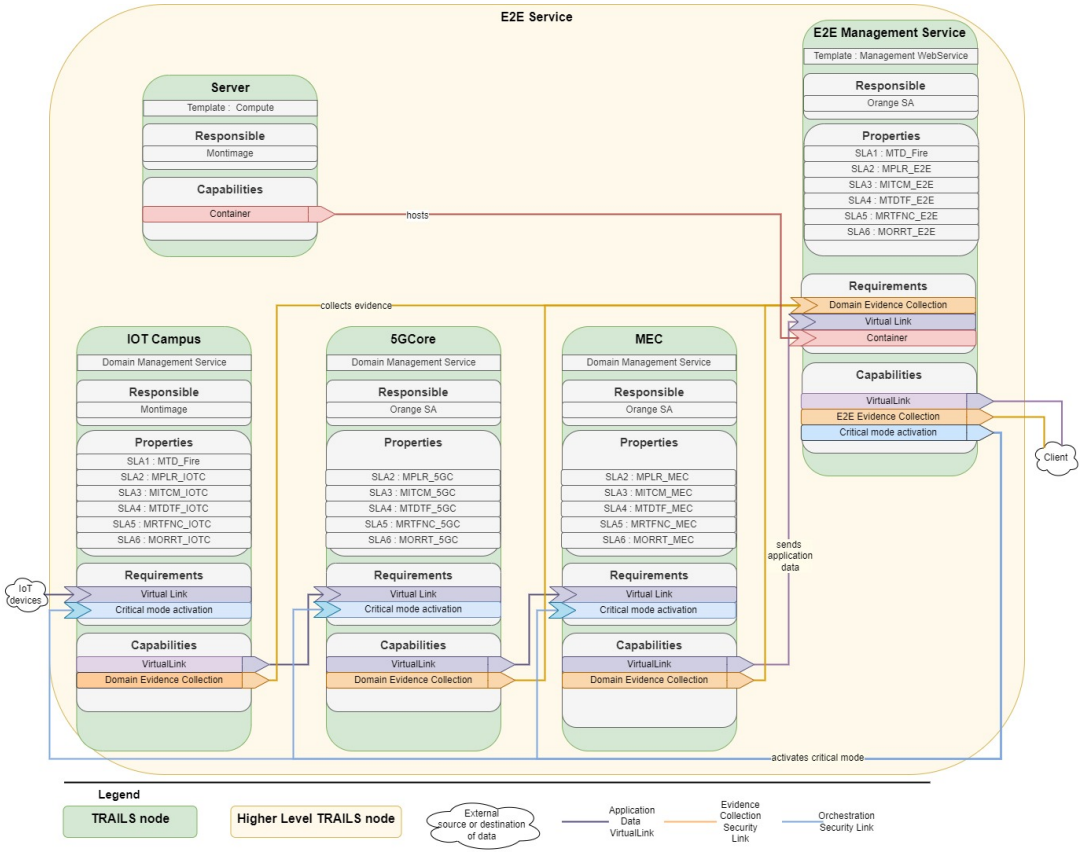

Figure 4: E2E Service Topology Layer 1

and E2E Service Provider or between the Customer and the E2E Service Provider.

The security properties derived from the use case and which are extracted by the Systemic Component's and Deep Attestation agent's built-in security are the execution status, the location status and the integrity status of the software to be protected. The use case applies novel software security techniques to extract these security properties, as well as their trustworthy and convention-based sharing between stakeholders. These basic software properties are the foundation for establishing liability-aware and accountability methods, as reflecting that the normal execution of the software, at the correct place and in its genuine form. Time tags and the software identification are appended to the property validation messaging, hence providing an enriched execution context data for the elaboration of liability and accountability methods.

Last, the security properties are delivered to several SLA stakeholders, either checking the good functioning state during the service execution or for post-mortem, incident root cause analysis. In both cases, the security properties shall be considered with certainty as being lost if any associated check fails. As a matter of fact, on a technical point of view, any test failure brings certainty whereas any test success reversely does not carry the same certainty, because of the lack of completeness of the test, which may fail to detect a specific scenario. For liability and dependability purposes, it is however of major interest to collect any information attesting that the software was not operating in normal conditions or not executing at all. As a consequence, collecting such information is very relevant.

4.5 Analysis and resolution of liabilities

The IoT-RCA is a component that investigates an event or an anomaly in order to determine its origin. As described in Section 4.3, the Systemic Component and the Deep Attestation module both provide evidences of SLA compliance or violation. Given that they are bound with a physical infrastructure, Systemic and Deep Attestation can also be used to pinpoint the origin of an event of incident or SLA violations.

Based on the aggregation of evidences collected at the IoT Campus, 5G Core and MEC Domains, the E2E Service Provider can generate a compliance report which demonstrates that the E2E Service behaves as expected. It can also generate an SLA violation report which document an incident or event, its Root Cause as well as the evidences that support this analysis.

These reports can be used by legal actors to settle negociations. They can also serve for billing purpose, for example to determine potential penalties or remediation to be provided by the E2E Service Provider to the Customer or by a Supplier to the E2E Service Provider.

Published version DOI: https://doi.org/10.1145/3538969.3544465

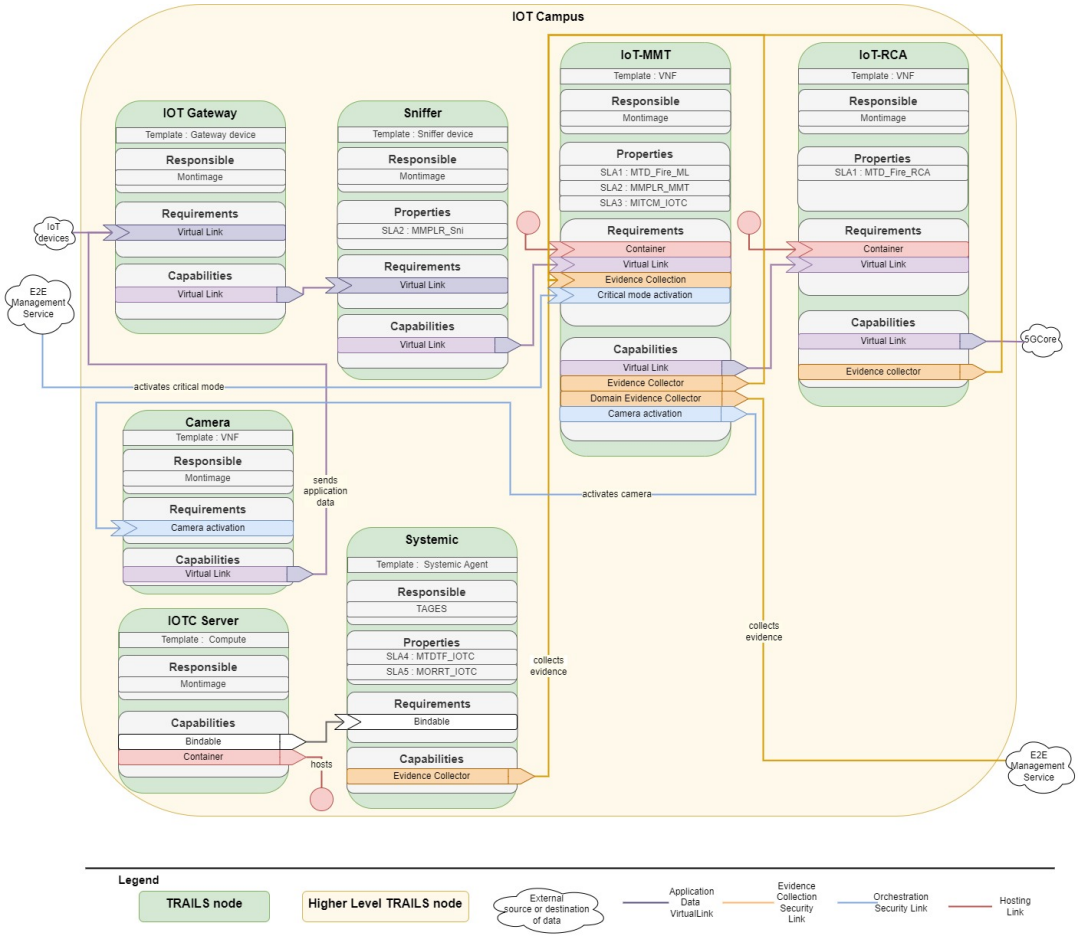

Figure 5: E2E Service Topology Layer 2 - IoT Campus

5 CONCLUSION

In this paper, we presented a use case which corresponds to a multi-domain service which spans from an IoT Campus Domain to the 5G Core Network Domain. Then, we described how the network enablers developed in the INSPIRE-5Gplus project can be combined to manage dynamically a Service Level Isolation SSLA along with evidence collection and liability management for an industrial entity which has a legal obligation to ensure and demonstrate that its critical services are isolated.

In future work, we plan to further enrich the framework in order to include SLA deviation metrics or responsibility metrics as well as SSLA composition rules.

ACKNOWLEDGMENTS

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 Commission is not responsible for any use that may be made of the information it contains.

REFERENCES

[1] A4Cloud. 2022. A4Cloud website. Retrieved May, 05 2022 from http://www.cloudaccountability.eu/

[2] Y. Anser, C. Gaber, J.P. Wary, S.N. Mattheu, and S. Bouzefrane. 2022. TRAILS: Extending TOSCA NFV profiles for liability management in the Cloud-to-IoT continuum. In *IEEE International Conference on Network Softwarization - NETSOFT 2022*. IEEE, 3, Park ave, NY, USA, 1–6.

[3] Ghada Arfaoui, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Adina Nedelcu, Cristina Onete, and Léo Robert. 2021. A Cryptographic View of Deep-Attestation, or how to do Provably-Secure Layer-Linking. *IACR Cryptol. ePrint Arch.* 2021 (2021), 1487.

[4] C. Bonhomme, C. Feltus, and D. Khadraoui. 2010. A multi-agent based decision mechanism for incident reaction in telecommunication network. In *ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010*. IEEE, 3, Park ave, NY, USA, 1–2.

[5] European Commission. 2016. EU Network and Information Security (NIS) Directive (EU 2016/1148). Retrieved May, 15 2022 from http://data.europa.eu/eli/dir/2016/1148/oj

[6] European Commission. 2016. SEVESO III Directive (2012/18/EU). Retrieved May, 15 2022 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0018

[7] ContractWorks. 2022. ContractWorks website. Retrieved May, 15 2022 from https://www.contractworks.com/

[8] ETSI. 2019. ETSI GR NFV-SEC018 Report on NFV Remote Attestation Architecture.

[9] Chrystel Gaber, José Sánchez Vilchez, Gürkan Gür, Morgan Chopin, Nancy Perrot, Jean-Luc Grimault, and Jean-Philippe Wary. 2020. Liability-Aware Security Management for 5G. In *2020 IEEE 3rd 5G World Forum (5GWF)*. IEEE, 3, Park ave, NY, USA, 133–138. https://doi.org/10.1109/5GWF49715.2020.9221407

Published version DOI: https://doi.org/10.1145/3538969.3544465

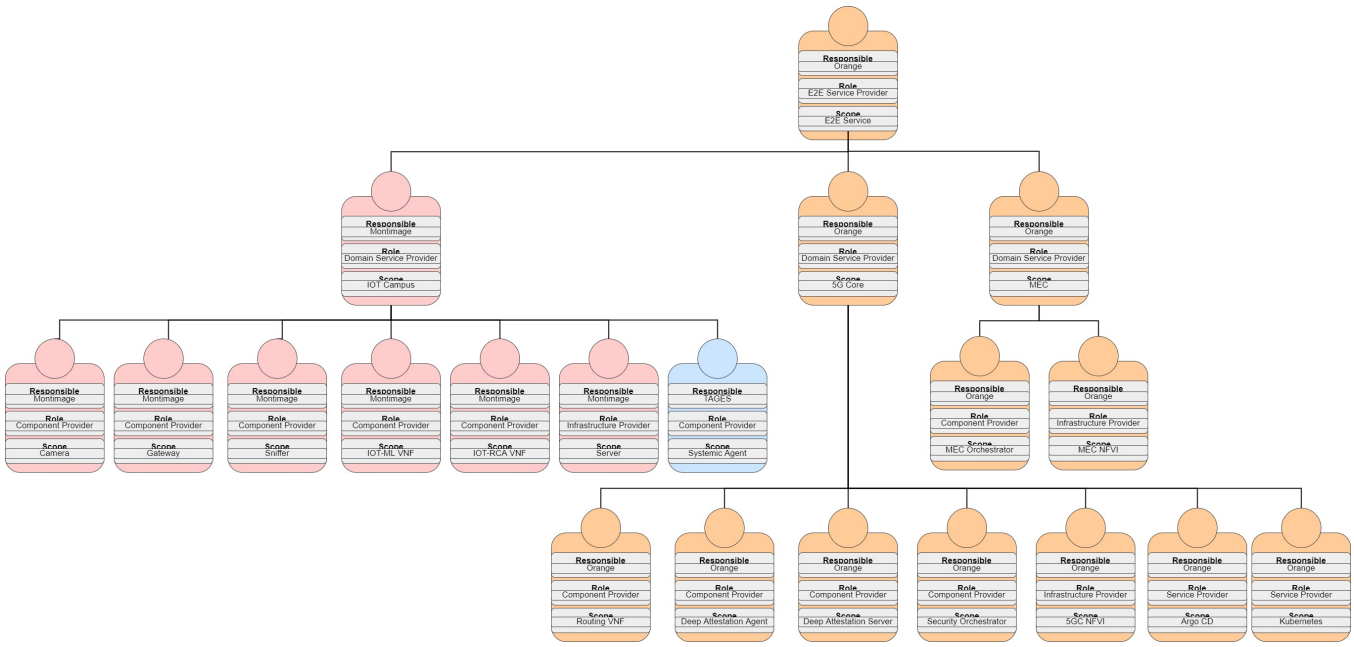

Figure 6: E2E Service Responsibilities

[10] G. Guemkam, C. Feltus, P. Schmitt, C. Bonhomme, D. Khadraoui, and Z. Guessoum. 2011. Reputation Based Dynamic Responsibility to Agent Assignment for Critical Infrastructure. In *2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*, Vol. 2. IEEE, 3, Park ave, NY, USA, 272–275.

[11] George Hatzivasilis, Panos Chatziadam, Nikos Petroulakis, Sotiris Ioannidis, Matteo Mangini, Christos Kloukinas, Artsiom Yautsiukhin, Michalis Antoniou, Dimitrios G. Katehakis, and Marios Panayiotou. 2019. Cyber Insurance of Information Systems: Security and Privacy Cyber Insurance Contracts for ICT and Helathcare Organizations. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 3, Park ave, NY, USA, 1–6. https://doi.org/10.1109/CAMAD.2019.8858165

[12] ISO. 2019. ISO 14971:2019 Medical devices — Application of risk management to medical devices. Retrieved May, 15 2022 from https://www.iso.org/standard/72704.html

[13] Juro. 2022. Juro website. Retrieved May, 15 2022 from https://juro.com/

[14] Medius. 2022. Mediuswebsite. Retrieved May, 15 2022 from https://www.medius.com/solutions/medius-contract-management/

[15] Guido Möllering. 2005. The Trust/Control Duality: An Integrative Perspective on Positive Expectations of Others. *International Sociology* 20, 3 (2005), 283–305. https://doi.org/10.1177/0268580905055478

A ABBREVIATIONS

E2E service	End-to-End Service
IoT-MMT	Anomaly detection tool
IoT-RCA	Root Cause Analysis tool
KPI	Key Performance Indicator
LASM-RS	Liability-Aware Service Management Referencing Service
MEC	Multi-access Edge Computing
MITCM	Mean Initial Time for Critical Mode
MTD_Fire	Mean Time To Detect a Fire
MPLR	Mean Packet Loss Ratio
MORRT	Mean Observation Report Request Response Time
MRC	Monthly Recurring Charge
MRTFNC	Mean Ratio of Time Functions are Not isolated In Critical mode
MTDTF	Mean Time To Detect Tampering or incorrect location of Function
NIS	Network and Information Security
NFV	Network Function Virtualisation
OES	Operator of Essential Services
PPU	Pay-Per-Use
SLA	Service Level Agreement
SSLA	Security Service Level Agreement
TRAIL	sTakeholder Responsibility, AccountabIity and Liability deScriptor

Table 1: Abbreviations

Published version DOI: https://doi.org/10.1145/3538969.3544465