ETSI TR 103 857 V1.1.1 (2026-07)

TECHNICAL REPORT

Core Network and Interoperability Testing (INT); Artificial Intelligence (AI); End-to-End Autonomic Security Management and Control in Multi-Domain 5G Networks

Reference
DTR/INT-00900

Keywords
5G, autonomic networking, cyber security, security,
security by default, self-management

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Core Network and Interoperability Testing (INT).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document introduces a Generic Autonomic Network Architecture (GANA) framework for achieving End-to-End Artificial Intelligence (AI)-powered Autonomic Security Management and Control (ASMC) across multi-domain 5G networks. It explains the role of AI models in the management and control operations of 5G networks, particularly in the context of Autonomic Management and Control (AMC) systems.

The present document presents an instantiation of he GANA reference model (framework), i.e. the application of the generic model (GANA) onto an implementation-oriented architecture and its use of AI algorithms to drive self-security operations in networks. It also highlights the need for E2E Autonomic (closed-loop) Service and Security Assurance through the federation of GANA Knowledge Plane (KP) platforms.

The present document references ETSI specifications and ongoing Proof-of-Concept (PoC) programs on "5G network slices creation, AMC and E2E Orchestration, with Closed-Loop (Autonomic)". It emphasizes the importance of a standardized GANA Framework for implementing AMC systems in the industry. The present document further elaborates on the capabilities and aspects covered in the 5G PoC White Paper No.6, including the use of AI models for AMC, security analytics, security functions placement/orchestration, and programmability requirements for self security management DE.

It encourages readers to refer to the complementary White Papers of the ETSI 5G PoC for more information and invites interested parties to join the PoC Consortium.

1 Scope

The present document provides a Framework that serves as an Implementation Guide for interoperable solutions that are aimed at addressing 5G security challenges. This is in reference to security challenges that should be addressed through the use of the following methods:

1) automated orchestration of security mechanisms and services that can be used for 5G network slices, network segments and services delivered by the End-to-End (E2E) network;

2) automated security policy computation and dynamic security policy enforcement in various points in the network infrastructure using GANA autonomics (closed control-loops) in response to new 5G slice and service instantiations, new intents and security SLAs supplied as inputs by the human network operator and/or in response to detected and predicted security attacks, threats and risks.

The Framework enables to implement solutions for "self-protection" and "self-defence" autonomic behaviours by 5G networks and their associated management and control systems without need for human operator involvement in the decisions and actions against detected and predicted security attacks, threats and risks - even across multiple 5G network operators by use of cross domain federated GANA KP platforms.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI White Paper No.16 GANA: "Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services".

[i.2] ETSI TS 103 195-2 (V1.1.1): "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management".

[i.3] White Paper No.1 of the ETSI 5G PoC: "C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA Knowledge Planes".

[i.4] ETSI TR 103 473 (V1.1.2): "Evolution of management towards Autonomic Future Internet (AFI); Autonomicity and Self-Management in the Broadband Forum (BBF) Architectures".

[i.5] ETSI TR 103 404: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in the Backhaul and Core network parts of the 3GPP Architecture".

[i.6] White Paper No.3 of the ETSI 5G PoC: "Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the ETSI GANA Knowledge Plane for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV/Clouds".

[i.7] White Paper No.2 of the ETSI 5G PoC: "ONAP Mappings to the ETSI GANA Model; Using ONAP Components to Implement GANA Knowledge Planes and Advancing ONAP for Implementing ETSI GANA Standard's Requirements; and C-SON - ONAP Architecture".

[i.8] ETSI TC INT AFI WG 5G POC: "Report on Specifications of Integration APIs for the ETSI GANA Knowledge Plane Platform with Other Types of Management and Control Systems, and with Info/Data/Event Sources in general".

[i.9] ETSI TS 128 533 (V15.0.0): "5G; Management and orchestration; Architecture framework (3GPP TS 28.533 version 15.0.0 Release 15)".

[i.10] NGMN: "5G End-to-End Architecture Framework v3.0.8".

[i.11] White Paper No.4 of the ETSI 5G PoC: "ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Autonomic Management and Control (AMC) of Networks and Services; and Intent-Based Networking (IBN) via GANA Knowledge Planes (KPs)".

[i.12] White Paper No.6 of the ETSI 5G PoC: "Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management and Control for 5G Slices, Networks/Services".

[i.13] 5G security recommendations: "Package #2: Network Slicing", by NGMN Alliance, 27 April 2016.

[i.14] ODA TM Forum's Open Digital Architecture (ODA): "IG1167 ODA Functional Architecture Vision R18.0.0 (Intelligence Management Function Block)".

[i.15] 5G security - Package 3: "Mobile Edge Computing / Low Latency / Consistent User Experience", NGMN Alliance: 20 February 2018, by NGMN 5G security group.

[i.16] ODA TM Forum's Open Digital Architecture (ODA): "IG1177 ODA Intelligence Management Implementation Guide R18.5.0", IG1177 Release 18.5, December 2018.

[i.17] James Crawshaw: "Network Automation Roadmap: Where to Start and What to Aim for, A Heavy Reading white paper produced for Juniper Networks Inc".

[i.18] Cabaj K., Szczypiorski K., Becker S. (2010): "Towards Self-defending Mechanisms Using Data Mining in the EFIPSANS Framework", In: Nguyen N.T., Zgrzywa A., Czyżewski A. (eds) Advances in Multimedia and Network Information System Technologies. Advances in Intelligent and Soft Computing, vol 80. Springer, Berlin, Heidelberg: DOI: 10.1007/978-3-642-14989-4_14.

[i.19] Alberto Huertas, Manuel Gil Pérez, Félix J. García Clemente, Gregorio Martinez Perez: "Towards the autonomous provision of self-protection capabilities in 5G networks", December 2019, Journal of Ambient Intelligence and Humanized Computing 10(12):4707-4720: DOI: 10.1007/s12652-018-0848-6.

[i.20] Manuel Gil Perez, et al: "Self-Organizing Capabilities in 5G Networks: NFV and SDN Coordination in a Complex Use Case", EuCNC 2018-3rd Network Management Workshop for 5G Networks, June 2018.

[i.21] Ashutosh Dutta, Ph.D.: "Conference Slides: Security in SDN/NFV and 5G Networks Opportunities and Challenges", Chair, IEEE™ Future Network Initiative, 05/06/2019.

[i.22] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov: "5G Security: Analysis of Threats and Solutions", In 2017 IEEE™ Conference on Standards for Communications and Networking (CSCN): DOI: 10.1109/CSCN.2017.8088621.

[i.23] Palo Alto Networks White Paper: "5G SECURITY: Establishing a Holistic Approach to Paving the 5G Evolution", 2018.

[i.24] Falko Dressler, Gerhard Münz, Georg Carle: "Attack detection using cooperating autonomous detection systems (CATS)", Proceedings of 1st IFIP International Workshop on Autonomic Communication, Poster Session, Berlin, Germany, October 2004.

[i.25] Anastasios Zafeiropoulos, Athanassios Liakopoulos, Alan Davy, Ranganai Chaparadza: "Monitoring within an Autonomic Network: A GANA Based Network Monitoring Framework: Conference: Service-Oriented Computing", ICSOC/ServiceWave 2009 Workshops - International Workshops, ICSOC/ServiceWave 2009, Stockholm, Sweden, November 23-27, 2009, Revised Selected Papers: DOI: 10.1007/978-3-642-16132-2_29.

[i.26] On Using sFlow for Security Attacks detection.

[i.27] Flowmon® White Paper: "Whitepaper - Flow for Security: IP flow based detection of cyber threats", and online article: "Network Anomaly Detection and Network Behavior Analysis".

[i.28] Anna Sperotto: "PhD Thesis: Flow-Based Intrusion Detection", 2010.

[i.29] Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller: "An Overview of IP Flow-Based Intrusion Detection", IEEE™ Communications Surveys and Tutorials, Vol. 12, No. 3, Third Quarter 2010.

[i.30] Jordan Lam, Robert Abbas: "Machine Learning based Anomaly Detection for 5G Networks", March 2020.

[i.31] Jiaqi Li, Zhao Zhifeng, Rongpeng Li: "A Machine Learning Based Intrusion Detection System for Software Defined 5G Network", DOI: 10.1049/iet-net.2017.0212.

[i.32] European Union Agency for Network and Information Security (ENISA): "ENISA Threat Landscape for 5G Networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G)", November 2019.

[i.33] White Paper by Huawei: "Partnering with the Industry for 5G Security Assurance".

[i.34] GSMA™: "AI in Network Use Cases in China", October 2019.

[i.35] Andrea Peiro, CUJO AI: "Securing 5G Networks With Deep Learning-Based Threat Detection Systems", by Blogs and Opinions 6/10/2019.

[i.36] ETSI TS 129 520 (V15.0.0): "5G; 5G System; Network Data Analytics Services; Stage 3 (3GPP TS 29.520 version 15.0.0 Release 15)".

[i.37] White Paper by Huawei: "AI Security White Paper", 2018.

[i.38] Kelsey Ziser, Jim Hodges, Gordon Mansfield, Christina Ashraf: "5G Exchange", eBook: Innovation at the Speed of 5G.

[i.39] Jim Hodges: "Implementing 5G Security: Priorities and Preferences: A Heavy Reading white paper produced for F5 Networks", Heavy Reading White Paper, 2019, Fortinet, NetNumber, and Palo Alto Networks.

[i.40] Verizon White Paper: "Network Threat Advanced Analytics", 2016.

[i.41] ETSI TS 123 288: "5G; Architecture enhancements for 5G System (5GS) to support network data analytics services (3GPP TS 23.288 version 19.6.0 Release 19)".

[i.42] RCR Wireless News: "How to develop 5G security standards at a global scale", online article.

[i.43] Emmanouil Pateromichelakis, et al: "End-to-End Data Analytics Framework for 5G Architecture", In IEEE™ Access Online Special Section on Roadmap to 5G: Rising to the Challenge, Volume 7, 2019.

[i.44] White Paper No.5 of the ETSI 5G PoC: "Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs) via a Generic Test Framework for Testing GANA Multi-Layer Autonomics and their AI Algorithms for Closed-Loop Network Automation".

[i.45] 3GPP SA3 - Security.

[i.46] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

[i.47] ETSI GS NFV-REL 004: "Network Functions Virtualisation (NFV); Assurance; Report on Active Monitoring and Failure Detection".

[i.48] ETSI TC INT / AFI WG 5G PoC BrightTalk Webinar: "End-to-End Autonomic Closed-Loop Security Management and Control for 5G Networks".

[i.49] NGMN: "ODiN -Operating Disaggregated Networks", Project V 2.0, 20.09.2022.

[i.50] TM Forum Telco Data Space Initiative: "Promoting a trusted telco data space to drive new opportunities", supported by Catalysts Projects.

[i.51] Gaia-X European Association for Data and Cloud: "Gaia-X Architecture Document".

[i.52] IEEE™ Industry Newsletter: "The Road to European Digital Sovereignty with GAIA-X and IDSA", Arnaud Braud, Gaël Fromentoux, Benoit Radier and Olivier Le Grand, Orange Labs, France - March issue.

[i.53] Fraunhofer: "Reference architecture model for the Industrial Data Space". IDSA International Data Spaces Association.

[i.54] IDSA: "Reference Architecture Model", Version 3.0, April 2019.

[i.55] ENISA Threat Landscape for 5G Networks: "Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)", December 2020.

[i.56] Allan Edgard Silva Freitas: "On Design Autonomic Behavior for Blockchain platforms", LADC '23, Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing, October 2023, pp. 166-167.

[i.57] Fariba Ghaffari, Komal Gilani, Emmanuel Bertin, Noel Crespi: "Identity and access management using distributed ledger technology: a survey", International Journal of Network Management, 2022, 32(2), pp.e 2180. DOI: 10.1002/nem.2180.hal-03315497.

[i.58] NIS Cooperation Group: "Report on the cybersecurity of Open RAN", 11 May 2022, Report produced jointly by EU Member States, with the support of the European Commission and the EU Agency for Cybersecurity (ENISA) on a concerted approach to the cybersecurity of 5G networks.

[i.59] National Telecommunications and Information Administration (NTIA): "Open RAN Security Report", Outcome from Quad Critical and Emerging Technology Working Group, May 2023.

[i.60] Madhusanka Liyanage, An Braeken, Shahriar Shahabuddin, Pasika Ranaweera: "Open RAN security: Challenges and opportunities", Journal of Network and Computer Applications, Volume 214, 2023, 103621, ISSN 1084-8045.

[i.61] R. B. Bohn et al.: "NIST Multi-Domain Knowledge Planes for Service Federation for 5G & Beyond Public Working Group: Applications to Federated Autonomic/Autonomous Networking", 2023 IEEE™ Future Networks World Forum (FNWF), Baltimore, MD, USA, 2023, pp. 1-6, doi: 10.1109/FNWF58287.2023.10520595.

[i.62] Pastor-Galindo J., López-Millán G., Marín-López R., et al.: "A Framework for Dynamic Configuration of TLS Connections Based on Standards", J Netw Syst Manage 30, 24 (2022).

[i.63] ENISA: "Security in 5G Specifications: Controls in 3GPP Security Specifications (5G SA)", February 2021.

[i.64] NIST Special Publication 800-207: "Zero Trust Architecture".

[i.65] H. A. Kholidy et al.: "Toward Zero Trust Security in 5G Open Architecture Network Slices", MILCOM 2022 - 2022 IEEE™ Military Communications Conference (MILCOM), Rockville, MD, USA, 2022, pp. 577-582, doi: 10.1109/MILCOM55135.2022.10017474.

[i.66] H. A. Kholidy, A. Karam, J. L. Sidoran and M. A. Rahman: "5G Core Security in Edge Networks: A Vulnerability Assessment Approach", 2021 IEEE™ Symposium on Computers and Communications (ISCC), Athens, Greece, 2021, pp. 1-6, doi: 10.1109/ISCC53001.2021.9631531.

[i.67] H. A. Kholidy and R. Kamaludeen: "An Innovative Hashgraph-based Federated Learning Approach for Multi Domain 5G Network Protection", 2022 IEEE™ Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 139-146, doi: 10.1109/FNWF55208.2022.00033.

[i.68] H. A. Kholidy, A. Karam, J. H. Reed and Y. Elazzazi: "An Experimental 5G Testbed for Secure Network Slicing Evaluation", 2022 IEEE™ Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 131-138, doi: 10.1109/FNWF55208.2022.00032.

[i.69] Suriya M.: "Machine learning and quantum computing for 5G/6G communication networks - A survey", International Journal of Intelligent Networks, Volume 3, 2022, pp. 197-203, ISSN 2666-6030, DOI: 10.1016/j.ijin.2022.11.004.

[i.70] Draft new Recommendation ITU-T Y.3819: "Quantum key distribution network - Requirements and architectural model for autonomic management and control".

[i.71] ETSI TS 103 744 (V1.2.1): "CYBER; Quantum-Safe Cryptography (QSC); Quantum-safe Hybrid Key Establishment".

[i.72] ETSI TS 104 015 (V1.1.1): "Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies".

[i.73] ETSI TR 103 616 (V1.1.1): "CYBER; Quantum-Safe Signatures".

[i.74] ETSI TR 103 617 (V1.1.1): "Quantum-Safe Virtual Private Networks".

[i.75] ETSI TR 103 618 (V1.1.1): "CYBER; Quantum-Safe Identity-Based Encryption".

[i.76] ETSI TR 103 619 (V1.1.1): "CYBER; Migration strategies and recommendations to Quantum Safe schemes".

[i.77] ETSI TR 103 692 (V1.1.1): "CYBER; State management for stateful authentication mechanisms".

[i.78] ETSI TR 103 747 (V1.1.1): "Core Network and Interoperability Testing (INT/ WG AFI); Federated GANA Knowledge Planes (KPs) for Multi-Domain Autonomic Management and Control (AMC) of Slices in the NGMN(R) 5G End-to-End Architecture Framework".

[i.79] ETSI TR 103 823: "CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation".

[i.80] ETSI TR 103 949: "Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study".

[i.81] ETSI TR 103 966: "CYBER Security (CYBER); Quantum-Safe Cryptography (QSC); Deployment Considerations for Hybrid Schemes".

[i.82] ETSI TR 103 965: "CYBER; Quantum-Safe Cryptography (QSC); Impact of Quantum Computing on Cryptographic Security Proofs".

[i.83] ETSI TR 103 967: "Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Impact of Quantum Computing on Symmetric Cryptography".

[i.84] ETSI TR 103 195-1: "Core Network and Interoperability Testing (INT/ WG AFI); Generic Autonomic Network Architecture; Part 1: Business drivers for autonomic networking".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
6G	6th Generation
AF	Application Function
AFI	Autonomic Future Internet
AI	Artificial Intelligence
AMC	Autonomic cognitive Management and Control
AMF	Access and Mobility Management Function
AN	Autonomous Network
API	Application Programming Interface
AS	Application Server
ASMC	Autonomic Security Management and Control
BB	Building Block
CEP	Complex Event Processing
C-SON	Centralized Self Organizing Network
CSP	Communications Service Provider
CUPS	Control and User Plane Separation
CYBER	Cyber Security
DC	Data Center
dDE	distributed DE
DDoS	Distributed Denial of Service
DE	Decision making Element
DL	Deep Learning
DoS	Denial of Service
D-SON	Distributed SON
DT	Domain Type
E2E	End-to-End
eMBB	enhanced Mobile Broadband
EMM	EPS Mobility Management
ENISA	European Union Agency for Network and Information Security
EPS	Edge Packet Service
ESM	EPS Session Management
FM	Fault-Management
F-MBTS	Federation - "Model Based Translation Service"
FW	Firewall
GANA	Generic Autonomic Network Architecture
gNB	next generation Node Base station
GS	Group Specification
H-SON	Hybrid SON
HSS	Home Subscriber Server
IAM	Identity and Access Management
IBN	Intent-Based Networking
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IDSA	International Data Spaces Association
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISG	Industry Specification Group
ISV	Independent Software Vendor
IT	Information Technology
ITS	Intelligent Transport Systems
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector

KP	Knowledge Plane
KP DE	Knowledge Plane Decision-making Element
KPI	Key Performance Indicator
LCM	Lifecycle Management
MANO	Management and Orchestration
MAPE-K	Monitor-Analyse-Plan-Execute over a shared Knowledge
MBTS	Model-Based Translation Service
MDAS	Management Data Analytics Service
MDKP	Multi-Domain Knowledge Plane
ME	Managed Entity
MEC	Mobile Edge Computing
ML	Machine Learning
MNO	Mobile Network Operator
NAS	Non Access Stratum
NE	Network Element
NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
NFVO	NFV Orchestrator
NGMN	Next Generation Mobile Networks
NIST	National Institute of Standards and Technology (US)
NRF	Network Repository Function
NWDAF	Network Data Analytics Function
OBB	Out-Of-Band
O-CU	Open RAN-Centralized Unit
ODA	Open Digital Architecture
ODiN	Operating Disaggregated Networks
O-DU	Open RAN-Distributed Unit
ONAP	Open Network Automation Platform
ONIX	Overlay Network for Information eXchange
OOB	Out-Of-Band
O-RAN	Open Radio Access Network
O-RU	Open RAN-Radio Unit
OS	Operating System
OSS	Operations Support Systems
OTT	Over The Top
PCF	Policy Control Function
PM	Performance Management
PNF	Physical Network Function
PRINS	Protocol for (roaming security reference point) N32 Interconnect Security
PWG	Public Working Group
QF	QoS Function
QKD	Quantum Key Distribution
QoS	Quality of Service
QSC	Quantum Safe Cryptography
R&D	Research and development
RAN	Radio Access Network
REL	Reliability
RIC	RAN Intelligence Controller
SBA	Service Based Architecture
SDN	Software Defined Networks
SDO	Standards Development Organizations
SEC	Security
SECaaS	SECurity-as-a-Service
SF	Security Function
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMF	Session Management Function
SON	Self Organizing Networks
SPAN	Switched Port Analyser
SSL	Secure Sockets Layer

TAP	Test Access Point
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TM	TeleManagement
TR	Technical Report
TS	Technical Specification
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
VNF	Virtual Network Function
VPN	Virtual Private Network
WG	Working Group
ZTP	Zero Trust Principle

4 GANA 5G self-adaptive security management and control

4.1 Autonomic Security Management and Control (ASMC)

ETSI TS 103 195-2 [i.2], described the autonomics principles and enablers for Autonomic cognitive Management and Control (AMC) and Autonomous Networks (AN) paradigm instantiated in the 5G architectures in ETSI TR 103 747 [i.78]. AMC paradigm helps to achieve End-to-End (E2E) Closed-Loop (Autonomic) Security Management and Control (ASMC) in 5G E2E Architectures.

Generic Autonomic Network Architecture (GANA) Model defines an autonomic (closed-loop) manager for realizing security closed-loop that can be instrumented (implemented) as a software module. The autonomic manager component is referred to in the ETSI GANA Model as "**Security management Decision-making Element (DE)**".

In addition, such module could be powered by Artificial Intelligence (AI) such as Machine Learning (ML) or Deep Learning (DL) models that enable it to intelligently achieve security assurance targets at the level of its operations scope. A Cognitive Security-Management-DE is one that has a capability of learning and reasoning, and so it is considered as a deployable AI Model that needs to be tested before it is on boarded to run in a production environment.

A Security management-DE is responsible for autonomically managing any security issues. It does so by adaptively employing and managing "Managed Entities" (MEs) that pertain to the use of Certificates/Passwords Algorithms, Hash Algorithms, Encryption Algorithms, Access Control Mechanisms, Trust Mechanisms, Denial of Service (DoS) Detection/Prevention mechanisms, signature based intrusion detection mechanisms, and other security enforcement mechanisms.

Figure 1 illustrates the two levels at which "Security management DEs" can be designed to operate. The higher "Network-level Security management-DE" in the KP is responsible for controlling the lower "Node-level Security Management DEs" in Networks Elements (NEs) with Networks Functions (NFs) belonging to the network segment. The Security management DEs is a sub-part of the what is called the "Node-main-DE" in a GANA Node, along with other sub-DEs of the Node-main-DE such as Autoconfiguration and discovery management DE, resilience management DE, and Fault Management DE.

NOTE 1: Some MEs of an NE, such as Protocols of the Stack, may have own intelligence for security enforcement or may intrinsically embed security features. However, the MEs communications with the outside world may need to be constrained or policy-controlled by the global security enforcement policies of the Security Management-DE. And so the two GANA levels-DE to give particular in designing and implementing ASMC are the Node level-DE (GANA Level 3) and Network Level-DE (GANA Level 4).

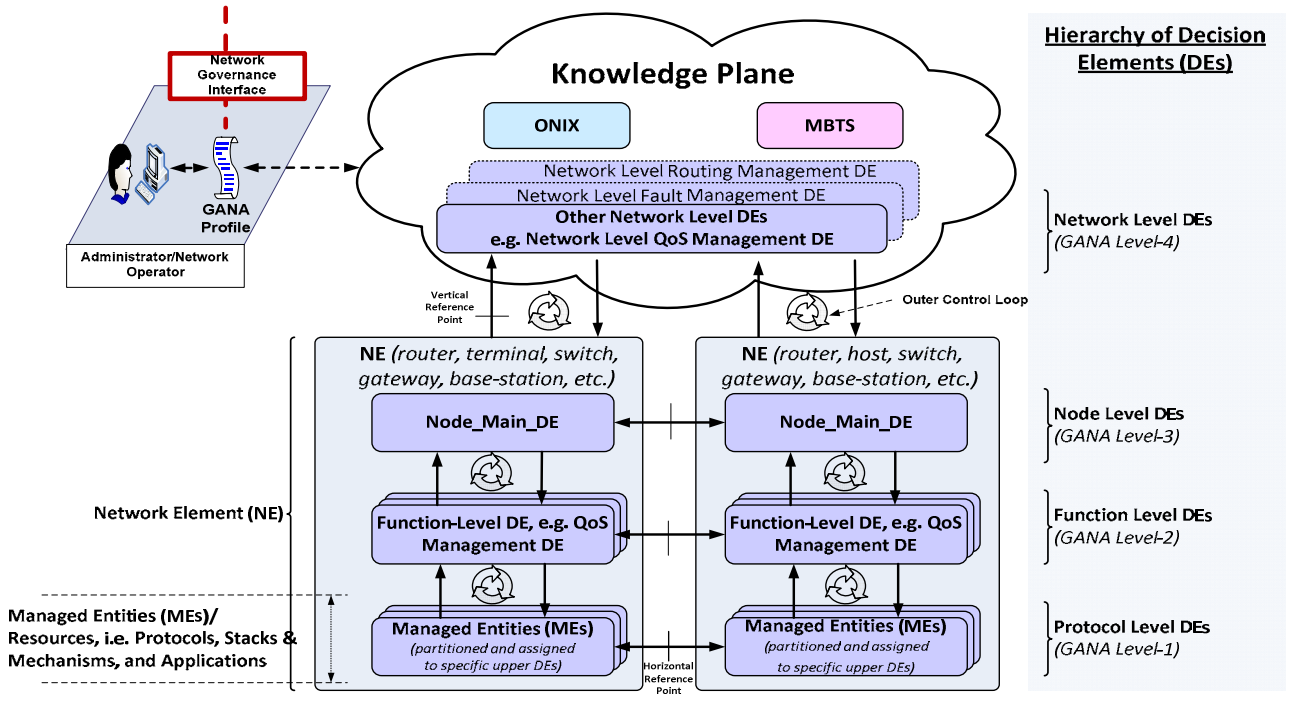

Figure 1: GANA Framework

The two layers (abstraction levels) of Security-management DEs that should be of focus in introducing Autonomic (Closed-Loop) are the Security DE in Network Level DEs for slow control loops and the Security DE in Node Level DEs for Fast control loops

The Security-Management-DEs are expected to implement **Self-Protection** and **Self-Defending** Policies and Operations for specific Network Segments/Domains as driven by whole GANA KP Platforms.

The definitions of **Self-Protection** and **Self-Defense** behaviours that help implementers of Security-Management-DEs in implementing the DEs at the two GANA levels and make them to interwork:

- **Self-Protection** involves the capability by which individual NEs/NFs of the network (thanks to embedding Security Management-DEs) automatically apply security policies and software patch updates that help protect the NE/NF and services using it from being compromised by security attacks (including intrusions, violations, etc.) and vulnerabilities/risks/threats (both, known and unknown attacks and vulnerabilities). This low-level security enforcement on NE/NF level should be complemented (enhanced and controlled) by a security enforcement capability that operates on the level of management and control systems of the network (thanks to Network-Level Security Management-DEs). The complementary capability at the network level dynamically computes and applies security policies for the whole network (e.g. a specific network segment) and services using any knowledge of known attacks that may occur to Nes/NFs and network services, and applying software patches as may be necessary to protect the network resources from being compromised by attacks and any vulnerabilities.

- **Self-Defense** involves the capability by which individual NEs/NFs of the network (thanks to embedding Security Management-DEs) automatically exercise the ability to detect security attacks (including intrusions, violations, etc.) and vulnerabilities(risks/threats) and apply security policies or software patch updates in reaction (defense) to any detected attacks or vulnerabilities/risks, and if the capability is more intelligent, then exercise the ability to predict security attacks and vulnerabilities and apply appropriate defense techniques. The effect of the self-defense actions is to minimize impacts of the detected or predicted attacks or vulnerabilities/risks/threats on services that depend on the NE/NF. As in the case of Self-Protection, the low-level security enforcement and security hardening on NE/NF level should be complemented (enhanced and controlled) by a capability that operates on the level of management and control systems of the network (thanks to Network-Level Security Management-DEs). The complementary capability at network level dynamically computes and applies security policies for the whole network (e.g. a specific network segment) and services using the knowledge of attacks or risks detected or predicted by a NE(s)/NF(s). In addition, applies software patches to defend and protect the network resources from being compromised by detected or predicted attacks or vulnerabilities/risks such that their impacts on network services is none or minimal. Self-Defense is closely related to the concept of **Resilience** (reactive and proactive resilience).

NOTE 2: The term security "**attack**" is generalized in the present document, to include all forms of security attacks or violations, including Denial of Service (DoS) Attacks for example, intrusions, and other forms of violations of the security of a system, service or network. There are various sources in literature that provide taxonomy on network, services and systems related security matters, e.g. [i.24].

A Security-Management-DE can be configured to operate in "Open-Loop Mode" or "Closed-Loop Mode". In Open-Loop Mode (allows human in the loop operation) the DE produces recommendations on actions the human operator can take to meet certain security enforcement or assurance objectives. ETSI GANA describes in much more detail these two modes of configuring a DE. The following aspects relate to how the ASMC part of the broader AMC is supposed to be realized by the interworking of the Security-Management-Des hierarchically (at the two levels) and horizontally (for certain ASMC strategies and algorithms that may be implemented in a distributed fashion within and across NEs/NFs of network):

a) Node Level Security-Management-DE. The autonomics (closed-loop(s)) of this DE includes orchestration of security mechanisms/techniques within a Network Element (NE) / Network Function (NF) in order to achieve self-protection and self-defence against security threats and attacks detected or predicted. Also the DE is responsible for planning and executing strategies for dynamically enforcing secure communications between the NE and the outside world, e.g. firewalling of traffic, tunnelling of traffic (including dynamic Virtual Private Networks (VPNs) provisioning to meet certain security objectives), encryption, use of trust models, etc.

b) GANA KP Level Security-Management-DE. The autonomics of this DE includes Dynamic Security Policies computation and their enforcement by the KP Level Security Management DE onto the lower Node level Security-Management-DE. In addition, the DE's autonomics include dynamic programming of security-policy-enforcement such as SDN controllers and specialized security functions of the network such as Firewalls, Security Gateways, Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs). This is because the KP Level Security Management-DE is the DE responsible for the security assurance and self-protection and self-defence of the whole domain (network segment) against security attacks and threats. The KP Level Security-Management-DE should also exhibit intelligence (thanks to autonomics algorithms for achieving **self-protection, self-healing, and self-defence** for the network and its services) that causes the DE to dynamically orchestrate or (re)-configure security functions wherever they may be needed on demand in response to security threats detection and prediction. Such dynamic configurations by the KP level Security Management DE apply to physical security functions as well.

c) Specialized Security Functions such as firewalls, IPSs, and IDSs, as NEs may need to embed the Node-level Security-Management-DE, like in the case of certain NEs such as routers and switches. In this way the DE can also serve as an embedded agent that should be policy controlled by the one at the KP level.

d) E2E ASMC in 5G should be achievable by way of Federation of the KP-Level Security-Management-DEs across multiple autonomics network domains (RAN, X-Haul Transport, Core Network), following the principles for federated AMC outlined in the NGMN 5G E2E Architecture Framework [i.10]. E2E Autonomic (Closed-Loop) service assurance should be achievable through a federation of Multi Domain KPs (MDKPs) that implement components for AMC intelligence for specific network segments (viewed as domains). Various types of common and generic information may be exchanged by federated KPs, and such information should include the following types of information:

- Synchronization of actions across multiple GANA KPs: This is required, for example, to realize an effective E2E federation of ASMC (adaptive security enforcement and defense) in network infrastructure segments and across multiple domains (Technologically and/or administratively diverse domains). Examples of such networks domains are Radio Access Network (RAN), X-Haul Transport Network (i.e. Fronthaul, Midhaul, Backhaul, etc.), "Multi-Access Edge Computing" (MEC) site or Core Network. E2E security AMC should be achievable through a federation of KPs for the various network segments (domains) associated with a given E2E scope. In this case, the policy of each KP level DE controls and governs the DEs at the node level within the network segment they are responsible for.

- The KP level Security Management-DE implements the security policies for self-protection and self-defense of associated Node level DEs and for securing a network zone under the responsibility of the DE, complemented by NE/NF level DEs required to realize 'fast control loops' within the Nes/NFs, in accordance with the generic autonomic networking principles (ETSI White Paper No.16 [i.1]).

- In this case, the policy of each KP level DE controls and governs the DEs at the node level within the network segment they are responsible for. The KP level Security Management-DE implements security policies to protect and defend the associated node level DEs and secure the network zone under its responsibility. This is complemented by DEs at the Node level, which enable fast control loops within the NEs, following the GANA principles (ETSI White Paper No.16 [i.1]).

- Security event information (regarding a description of a detected security incident): An example is detected threats that may impact a peer domain, which could trigger an investigation of the detected threat that is identified by the collaborating KPs. The exchange of such security threats detection or predictions information may result in the KPs collaboratively negotiating an adaptation strategy (self-adaptation without human involvement) for adjusting security enforcement policies that each KP then applies to realize self-protection and self-defense for its associated network segment/ domain against the detected or predicted threat(s). For example, there may be some security threats detected in the access network domain by the KP for the access network that could have impact on X-Haul transport network domain as a peer domain or may have impact on the core network as the peer domain in terms of impact scope of the security threat(s).

- Trust model (e.g. a reputation-based trust model) between the AMC administrative domains: An example of such a trust model would be a kind of trust model that spans across AMC domains, with the associated network infrastructure segments and their associated KPs, where each particular network segment has a KP.

- Security related Service Level Agreement (SLA) violation detection: The detection of an SLA violation, requires the associated KPs to initiate a resolution through a collaboration across the KPs to resolve the SLA discrepancies by reacting to resolve the detected discrepancies for an alignment with the configured SLA clauses in the SLA contracts that were established by the associated domain owners or stakeholders/partners.

NOTE 3: The Information that needs to be exchanged on a KP-to-KP Federation Reference Point, as well as the messages and communication means should be candidate for standardization (e.g. in ETSI TC INT AFI WG).

As illustrated on Figure 2, Security Modules in a Network Architecture are required at the three (3) hierarchical GANA Levels:

- GANA KP Platform level, by the Network Level Security Management -DE.
- Node Level, by the Node main Level Security-Management-DE and this includes normal NEs and Layer4-Layer7 (L4-L7) Security Functions like IDS, IPS, Firewalls (FWs).

- Protocol Level (some security mechanisms may be intrinsically present in some protocols of the protocol stack of a NE/NF or some protocols may have been designed to employ various security enforcement mechanisms/techniques in their operations.

Security modules implemented to operate in NEs/NFs are policy controlled by the Security-Management-DE operating as a Security Policy Engine in the associated GANA KP Platform. A GANA KP Platform enriches the Control Plane and the Management Plane as illustrated by the Integration of GANA KP with other management and control systems such as SDN Controllers, Orchestrators, OSS/BSS, MANO stacks, etc., as described earlier in the present document and in [i.11] and [i.8].

On those levels the following module types/examples should be considered:

- **GANA KP Platform Level:** → Security API (Application Programming Interface) Library should be designed for the Security-Management-DE such that some inputs to the DE can be supplied through the API. And some specialized security Applications (runnable software) for addressing different aspects of ASMC can be developed such that they can be selectively invoked and managed by the Security-Management-DE. Such Applications may be developed to empower the Security Management-DE to offer "**Security-as-a-Service"** (SECaaS) for the various contexts addressed by the Applications. The Applications could be "composed" into "Security Services" that form a Service Container Library for the Security-Management-DE. The specialized security Applications that should be invoked and managed by the Security-Management-DE employ various security enforcement mechanisms/techniques such as encryption methods, tunnelling management, authentication methods, etc.

- **GANA Node Level (i.e. NE/NF):**→ A NE/NF of the type like a router or a switch should embed a Security-Management-DE as prescribed by the GANA principles, so as to implement a fast control-loop for self-protection and self-defense intelligence for the NE/NF. There are other types of Nes/NFs like L4-L7 security functions such as a Firewall, IDS, and IPS, that can be made to embed a Security-Management-DE to realize a fast control-loop for self-protection of the network and services the security function is meant to protect. And to some extent, the fast control-loop can also be meant for realizing self-defense of the NE/NF against certain attacks that may be aimed at rendering the NE/NF cease to function well. Some specialized Security Applications (runnable software) meant for addressing different aspects of ASMC can be developed such that they can be selectively invoked and managed by the Security-Management-DE. And such Applications may be developed to empower the Security Management-DE to offer "Security as a Service" for the various contexts addressed by the Applications that could be "composed" into "Security Services" that form a Service Container Library for the Security-Management-DE. The types of Nes/NFs that could offer "**Security-as-a-Service**" are L4-L7 types of Nes/NFs such as Firewall, IDS, IPS.

- **GANA Protocol Level or GANA Level 1 in general:** → At Protocol Level, some security mechanisms may be intrinsically present in some protocols of the stack of the NE/NF or some protocols may be designed to employ various security enforcement mechanisms/techniques in their operations. Other types of MEs at GANA level-1 may also embed security mechanisms or may be designed to employ various security enforcement mechanisms/techniques (e.g. encryption methods, tunnelling management, authentication methods, etc.) in their operations. All the various security enforcement mechanisms/techniques that can be applied on a global scale within the NE/NF can be considered as forming a security enforcement mechanisms/techniques Library of the NE/NF. Such that the mechanisms/techniques can be orchestrated and employed by various entities within the NE/NF that require to employ them as required and enforced by the Security-Management-DE of the GANA Node(NE/NF).

NOTE 4: In Figure 2, the security enforcement capabilities (e.g. mechanisms and logic) at GANA Level-1 and GANA Level-3 of an NE/NF may be activated in certain types of Nes/NFs of the network.

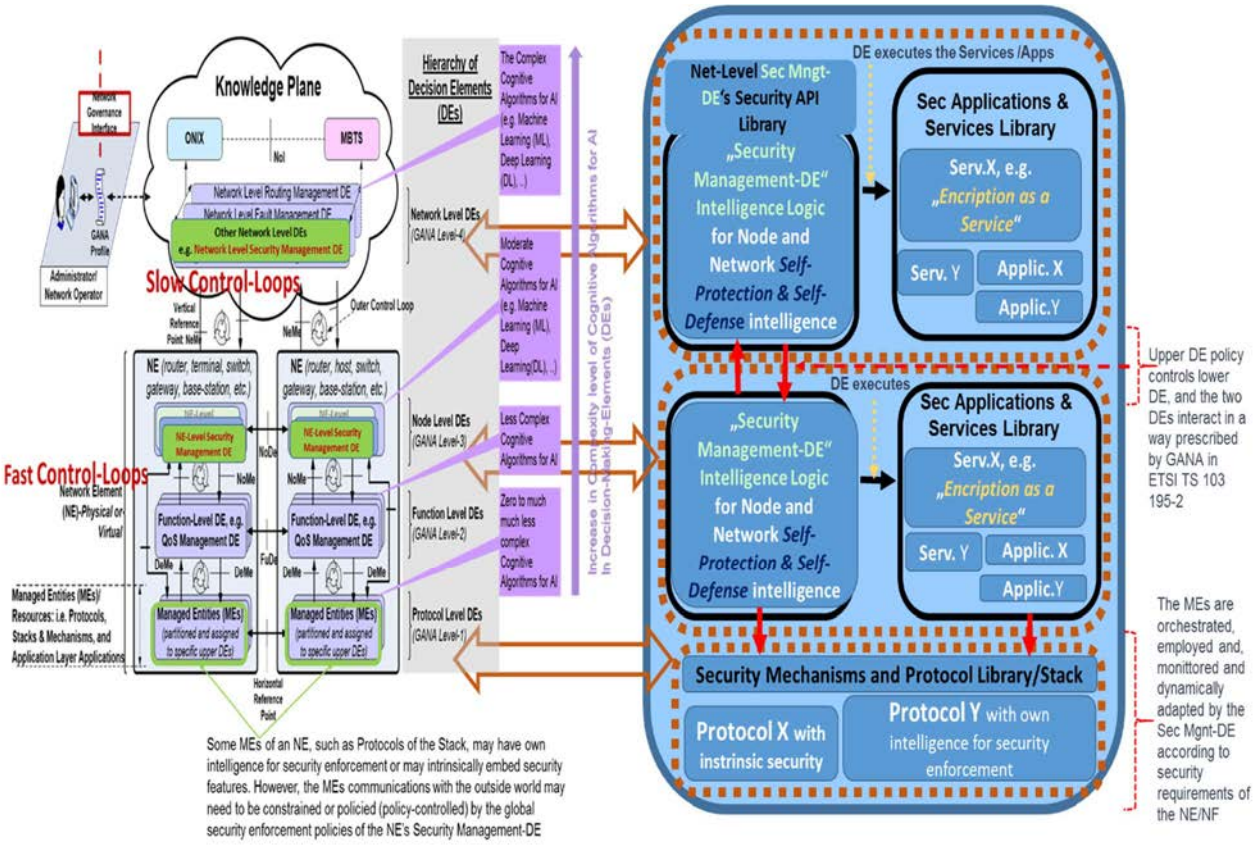

Figure 2: Hierarchical Security Management in GANA Framework

Figure 3 provides an illustration of how a Network Level (KP Level) Security Management-DE can be implemented to drive autonomics control-loop over Security Functions as its MEs and dynamically program them to meet Self-Protection and Self-Defense Objectives of the network (e.g. as illustrated in [i.18], [i.19] and [i.20]) (more details on approaches to designing GANA DEs are found in ETSI TS 103 195-2 [i.2]).

NOTE 5: The subject of Self-Protection and Self-Defense behaviours is further discussed later in clause 4.9.

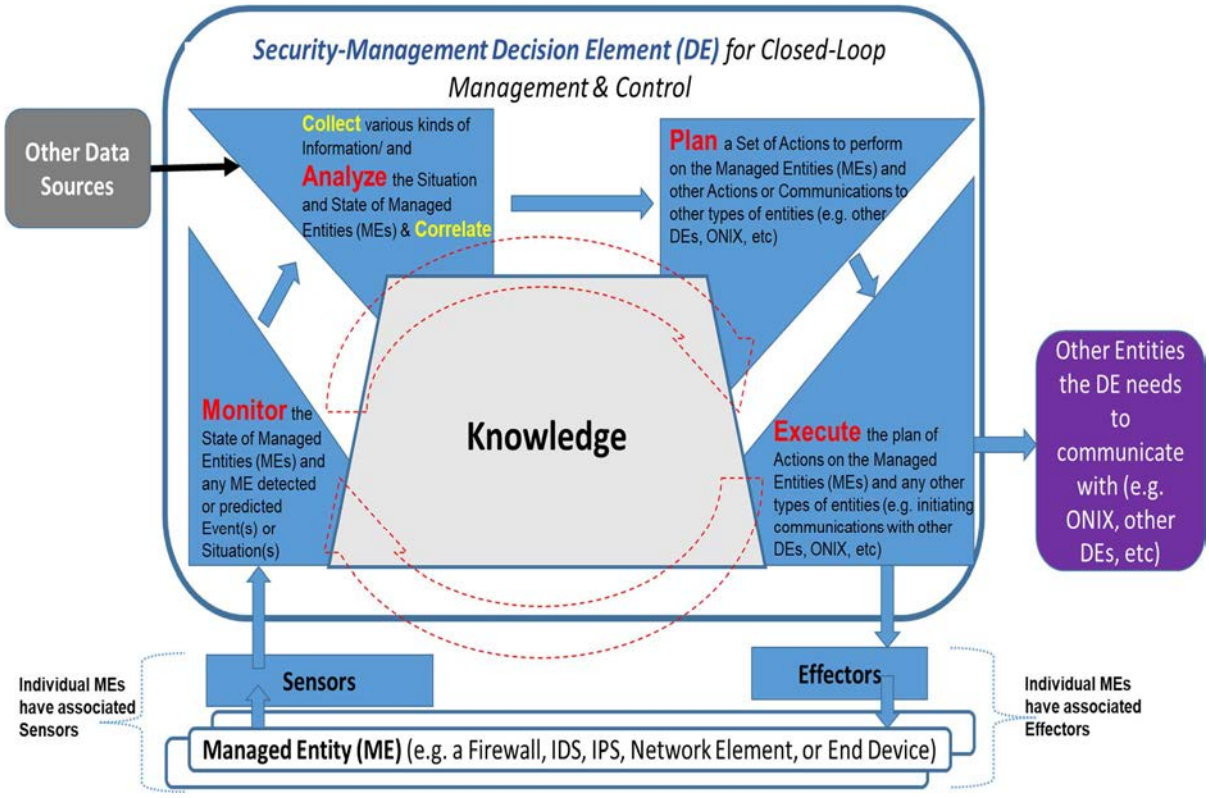

Figure 3: Illustration of how a Knowledge Plane Level GANA DE can be implemented

4.2 Security Requirements for GANA AMC

Another aspect of security in relation to AMC that needs to be considered in ASMC operations by DEs relates to the following requirements:

- Identity Management for Autonomics components (e.g. GANA DEs).
- Application of Encryption mechanisms and protocols, and application of other mechanisms/techniques for securing DE to DE communications (as such communications should never be compromised), DE to ME communications, and for any other communications involving the enablers for AMC such as ONIX and its services.

4.3 Security Testing of Components for GANA AMC and their Services

ETSI White Paper No.16 [i.1] provides insights on the nature various potential suppliers of DEs as Software Components. The DEs that can be loaded into NEs/NFs or into a GANA KP Platform. While Testing a Cognitive DE(s) like a Cognitive Security-Management-DE is about testing a deployable AI Model before the DE-Under-Test can be on-boarded into the production environment. The functional and performance tests of the DE should be complemented by Security Testing of the DE against certain security requirements deemed necessary by the network operator (just like for any software modules).

While Functional and Performance Tests for a Cognitive Security Management-DE is aimed at assessing the quality of decision-making capability, security tests of such a DE may involve the assessment of certain integration requirements for software components aimed at ensuring that the software component does not introduce security holes when on boarded into the production environment. The White Paper No.5 of the ETSI 5G PoC [i.44] covers the subject of Testing AI Models and Testing GANA Functional Blocks.

4.4 Drivers of ASMC for SECurity as a Service (SECaaS) in 5G

4.4.1 Overview

Security as a Service (SECaaS) is the delivery of security technologies - traditionally found in enterprise data centres or regional gateways - as a cloud service. With SECaaS, a service provider delivers security solutions such as email security, Identity and Access Management (IAM), endpoint security, incident response, and others through a subscription-based model rather than hardware.

[i.55] and [i.39] provide insights on the value of SECaaS in 5G and how it can be realized.

The value Autonomics bring to SECaaS is that GANA Security Management DEs can play a role in the orchestration of security assurance mechanisms required for a particular SECaaS and keep monitoring the behaviour and performance of the mechanisms to ensure that they keep delivering the security service required.

NOTE: The roles that GANA KP Platforms can play in SECaaS are described in the subsequent subclauses of clause 4.

4.4.2 Drivers for Differentiated Security: SECaaS by Default for 5G Telcos

Drivers for Differentiated Security: SECaaS Model by Default for Telcos:

- 5G/Cloud/EdgeCloud scene;
- Single Operator, multiple tenants (users) and user groups (customer classes, differentiated QoS, differentiated subscribed security services);
- Subscribed security services (based on Enhanced Mobile Broadband (eMBB) default-slice): → **Implying the Concept of "Security Quality of a Slice offered"**:
  - **Example Scenario Use Case A:** Real-time Threat Protection (Security as a Service (SECaaS)) granularity and composability → microservices in the form of multimedia flows within eMBB compose/form the overall slice), with diversified Protection Classes:
    1) Protection Class 0 → no security service subscription;
    2) Protection Class 1 → low security protection: threat detection of Distributed Denial of Service (DDoS) attack on user device;
    3) Protection Class 2 → medium security protection: threat detection of DDoS attack on user device and infrastructure;
    4) Protection Class 3 → high security protection: threat detection as in Class 2 SECaaS and additionally encryption per segment (MEC, Transport, Core) or/and E2E;
  - **Example Scenario Use Case B**: Real-time Self-Protection Against Attacks/Threats (Security Services Mix through KP Federations' Operations), with diversified Protection Classes:
    1) Protection Class 0 → no security service subscription;
    2) Protection Class 1 → low security protection: scope only covering the mobile edge;
    3) Protection Class 2 → medium security protection: scope covering mobile edge and metro transport/access;
    4) Protection Class 3 → high security protection: scope covering E2E mobile edge, access, transport and core part of services;
    5) **Protection Class 4: Protection of Slice User (Consumer) from Infected Documents that can be downloaded or exchanged with Peers (see Demo on this example protection class in** (in Webinar [i.48]).

The following are the SECaaS Segmentations Models that can be considered:

1) SECaaS Vertical Segmentation (see Figure 4):

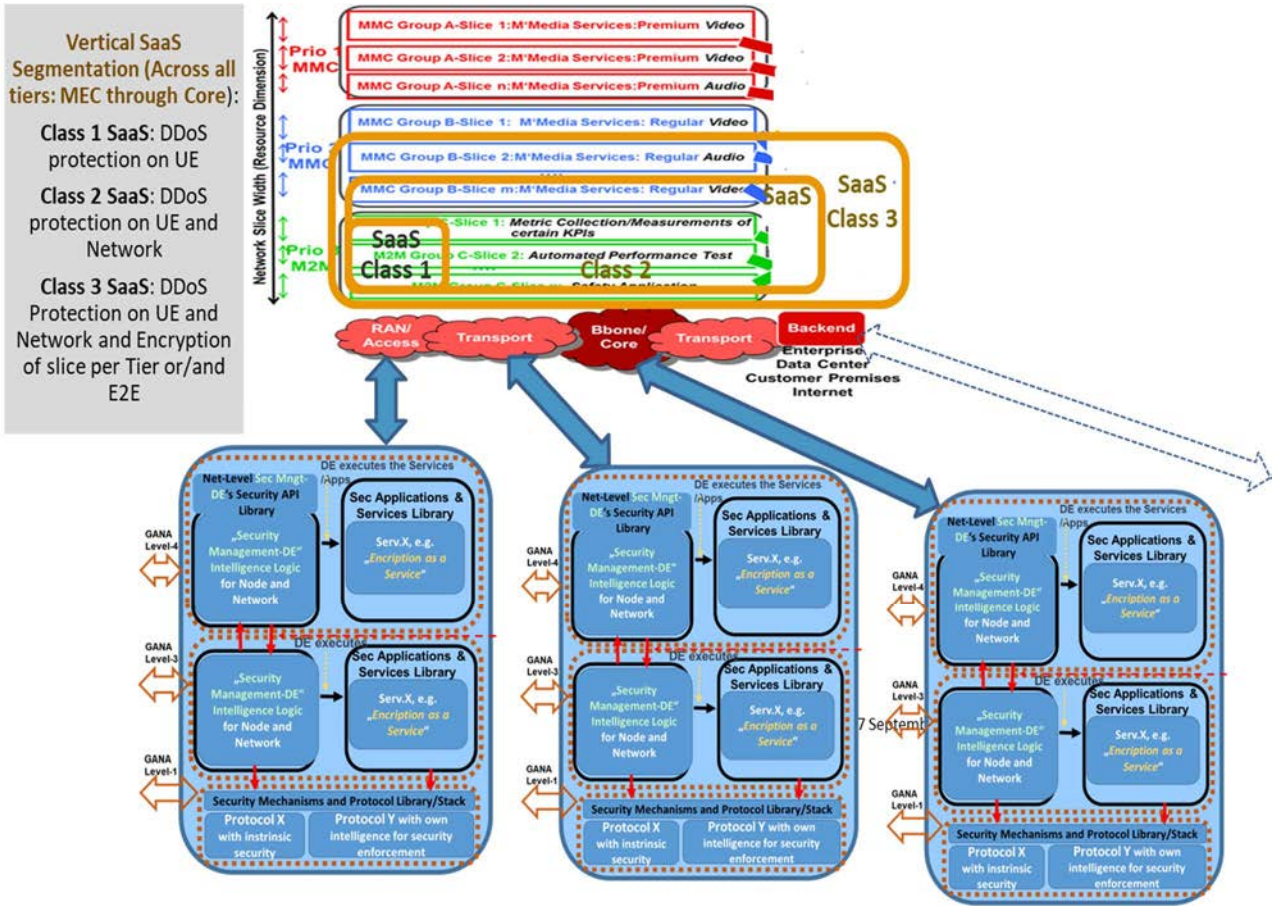

Figure 4: SECaaS Vertical Segmentation

2) SECaaS Horizontal Segmentation (see Figure 5):

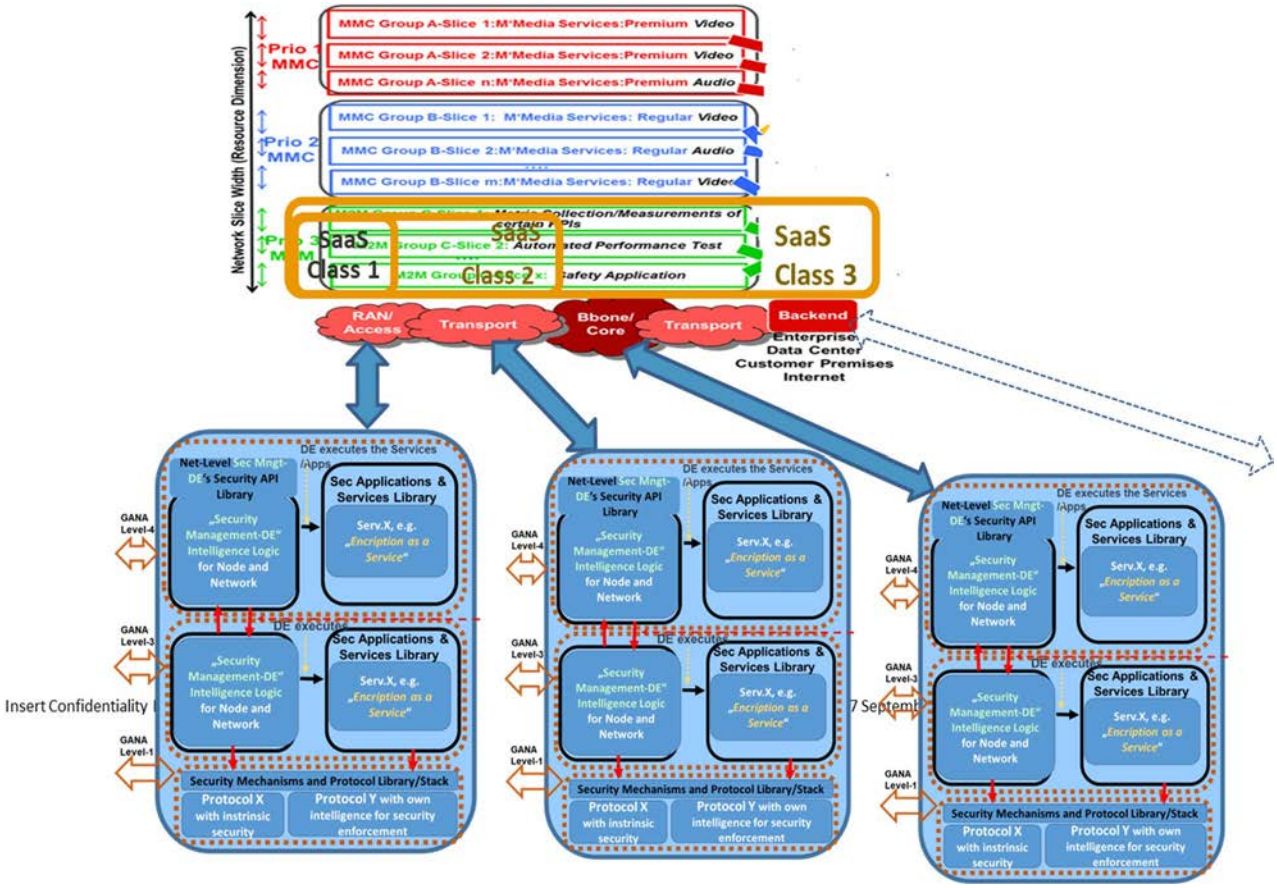

Figure 5: SECaaS Horizontal Segmentation

4.4.3 Autonomic SECaaS Assurance for Differentiated Security SLAs for 5G Slices

This clause presents Autonomic Security Assurance for Differentiated Security SLAs for 5G Slices, while applying Security-as-a Service Model for Telcos, supported by illustration/demo of Security SLA in an eMBB Slice Service as example.

[i.48] and [i.1] present the PoC Demo carried out in ETSI on GANA Autonomics in SaaS SLA for "Protection Class" in a 5G Slice: Protection of Slice User/Consumer from Infected Documents that can be downloaded or exchanged with Peers.

4.4.4 Summary of Core Principles, Design, and Commonalities towards Standardization and Harmonization

In compact form, the core principles of Security as a Service (SECaaS) include:

- Softwarization and digitalization of IT and Telco assets that cover functional and non-functional features, including Security
- Modularization of Security and Security-relevant functionality, structured and grouped on different (abstraction/stack/service) layers; analogous to a multi-layer service architecture
- Development of capabilities for Security software modules (services) for:
  - Indexing, labelling, being discoverable and listed
  - Combining several components into a single service while streamlining them

- Interfacing, referencing, and interacting with standardized methods and means (APIs, Reference Points, Service Templates and Catalogs)

Key Design Guidelines for SECaaS (towards consolidated requirements for enabling Security as a Service (SECaaS)) should include:

- Use Multi-layer Reference Architectures for Autonomic Management and Control (such as the ETSI GANA) as a Blueprint to which to map the Security Service Architecture
- Incorporating Orchestration and Dynamics into the behaviour of the system which uses basic building blocks (including for security) as a basis for forming the use-case and the workflow
- Place each designed Security Building Block (BB) at the right service-architecture layer and with a label that covers its scope so as to apply and use it in the right created complex multi-component service (turnkey SECaaS)
- Key requirements for enabling Security as a Service (SECaaS) should be expressed in a Checklist format
- Main interrelationships and cross-influence Factors among SECaaS Requirements should be considered
- Generic High-Level Model of Consolidated Requirements for Enabling SECaaS (for use in Blueprints, Federated Models, and other scenarios)

NOTE: The Key Design Guidelines for SECaaS enable multi- network operator E2E cognitive security modelling and collaboration (behavioural modelling and orchestration using GANA DEs) - thanks E2E Advanced ASMC Principles enablers in GANA Autonomics.

4.5 Multi-Domain Federated GANA KPs for E2E ASMC for 5G Slices

4.5.1 Overview

This clause defines a Framework for guiding implementers in designing and implementing GANA Security Management DEs of the KP Platforms responsible for autonomic (closed-loop) security assurance of specific network segments/domains in the context of the E2E 5G Architecture. The framework also includes the enablers for achieving autonomic security assurance across multiple network operators (as collaborating domains) by way of federated Information sharing regarding security attacks and threats; as well as Orchestration and Programmability requirements for Security functions responsible for securing a network segment. In short, the Framework outlines the following aspects as part of what is desired of such a Framework:

- The Key Concepts.
- The Aspects of the Generic Framework that pertain to E2E ASMC across Multiple Domains (Network Segments).
- Why it is desirable that Security Analytics by the GANA KP Security Management DE can dynamically trigger and program On-Demand Monitoring of certain Traffic in the Network, and the role of Passive Probing and Analytics of Traffic copied from Network.
- Security Functions Placement/Orchestration in 5G Networks and Autonomic/Dynamic Orchestration of Security Enforcement Policies as Driven by Network Slicing Dynamics.
- Programmability Requirements for Security Functions, and Autonomic/Dynamic Security Policies Enforcement by KPs, as Driven by Security Attacks Detection (including Intrusion Detection or other forms of Violations Detection) and Threats Predictions.
- Implementing Self-Protection and Self-Defending Behaviours for specific Network Segments/Domains by GANA KP Platforms, within Single Network Operator and across Multiple Network Operators.

NOTE 1: Throughout these various aspects, the 5G PoC White Paper No.6 [i.12] presents illustrative Capabilities that enable to implement the requirements of the **Generic Framework**.

NOTE 2: The term security "**attack**" is generalized in the present document, to include all forms of security attacks or violations, including Denial of Service (DoS) Attacks for example, intrusions, and other forms of violations of the security of a system, service or network. There are various sources in literature that provide taxonomy on network, services and systems related security matters, e.g. [i.24].

4.5.2 Security Challlenge of 5G slice for ASMC

5G network slices are associated with different Service Level Agreements (SLAs) and require strong isolation per slice so as to prevent threat propagations across network slices. The implication of network slicing is that slice specific security policies should be instantiated and applied for security assurance per slice.

This clause provides a summary of security challenges that should be handled by way of automated security policies instantiations and installations at various points in network segments and at security perimeters between network segments or domains. Security challenges that should also be addressed by way of closed-loop (autonomic) monitoring for security attacks/threats, attacks/threats detection and predictions, autonomic planning of policies for adaptive security assurance and execution of actions that employ various methods for self-protection and self-defense for the network infrastructure and network services (including slices). NGMN has produced security requirements for 5G and continues to look into security challenges for 5G [i.13] and [i.15]. European Union Agency for Network and Information Security (ENISA) published a "Threat assessment for the fifth generation of mobile telecommunications networks (5G)" [i.32]. [i.42] and [i.45] discuss the growing and strong requirement and call for Security Standards for 5G.

Efforts by the industry and research communities to capture such kinds of security challenges for 5G continue. For example, [i.39] discusses a recent survey on various security challenges for 5G (readers can read more on this survey in [i.39]), challenges such as the following:

- Security as a service (SECaaS) and the need for proactive security for known and unknown attacks
- Cloud RAN security, including fronthaul and backhaul security
- Core network signalling security
- 5G Roaming network signalling security
- Areas and contexts of susceptibility to Fraud (calling for fraud detection then)
- Signalling protection against multi-protocol attacks
- The need to look into automating real-time security policy
- Need for visibility in RAN and core network by content inspection

While some efforts have focused on looking at the security challenges that need particular focus on the RAN and core network, it is widely understood that there are various security challenges in other network segments such as the MEC edge, the X-Haul Transport Network and Data Centers, that have potential impact on other network segments, including RAN and core network. Therefore, there is a need for a holistic approach to correlation of attacks and threats, and the E2E collaboration of security platforms that automate real-time security policy for the various segments (or domains). Hence the need for a "**Generic Framework for Multi-Domain Federated GANA KPs for E2E ASMC for 5G Slices, Networks/Services"**.

There are other various sources that provide very valuable insights on security challenges in 5G, such as [i.13], [i.21] and [i.15]. As another example of documented security challenges in 5G, a Table of security challenges in 5G (e.g. DoS attacks, signalling storms, configuration attacks, User identity theft, Transmission Control Protocol (TCP) level attacks, man-in-the-middle attacks, hijacking attacks, IMSI catching attacks, etc.) is presented in [i.22] and readers should read [i.22] for more details. There are many more sources worthy to consider on security challenges in 5G, e.g. [i.23], [i.30], [i.31], [i.32], [i.33], [i.34], [i.35], [i.37] and [i.38].

Figure 6 illustrates two implementations Options for the interactions of a Security-Management-DE in the KP Level with a Security Function (e.g. Firewall, IPS, IDS, Security Gateway) or a NE/NF in general that can be programmed for security enforcement objectives.

NOTE: The two options apply to the other DEs of the KP as well in their interactions with NEs/NFs, i.e. with or without the use of an MBTS function.

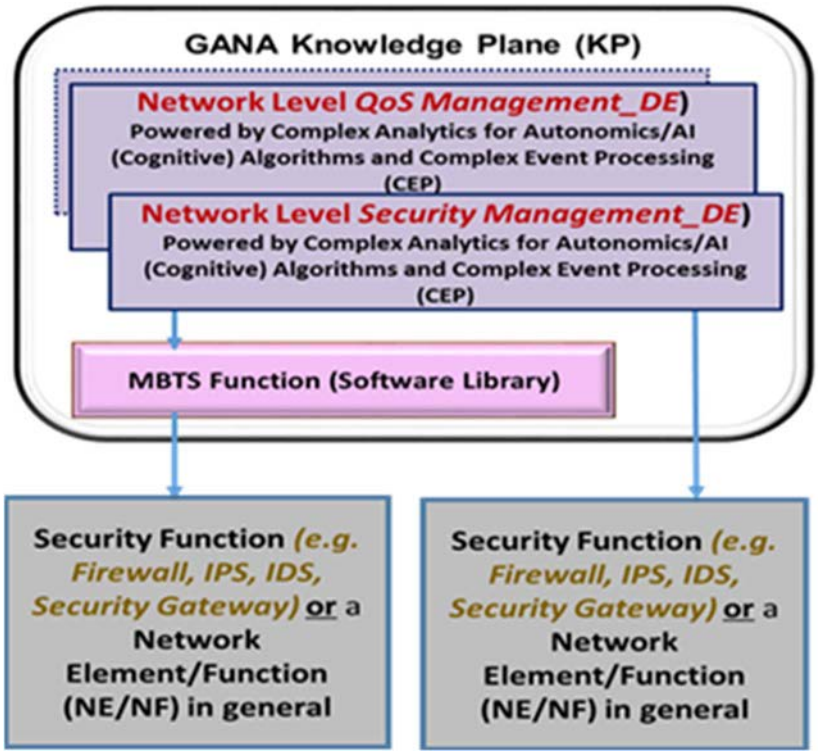

Figure 6: Two implementations Options for the interactions of a Security-Management-DE in the KP Level with a Security Function l

With respect to the 3GPP 5G SBA (Service Based Architecture), the Network Level Security Management-DE in the KP Platform should also be connected to the GANA Node Level (i.e. the Node-Level (NF-Level)). Meaning it should be connected to a Security Management-DE that may be embedded (as a capability) within each node or be connected to an NF in general that does not embed a Security Management-DE. Such integration of the SBA functions (e.g. functions in the control plane) with the KP enables to achieve the following objectives:

- at least AMF (to know UE location and to manage UE mobility);
- SMF (to know traffic flow characteristics and to manage flows);
- UDM (to know which NF manage a UE, and manage UE subscription);
- PCF (to manage the policy);
- NRF (to know the load of each NF or a slice and manage NF selection);
- the user plane UPF (to detect certain anomalies such as traffic related anomalies);
- NWDAF prediction, statistics on abnormal UE communication or mobility behaviour.

The Network Level Security Management-DE in the KP Platform should also be connected to the NEF (to protect the NEF, which exposes services to an AF (Application Function) and to manage security protection with third party AFs).

[i.33] presents some examples of some insights on security requirements in the 5G SBA. Also, functions such as the Network Data Analytics Function (NWDAF) [i.36] and [i.41] and the Management Data Analytics Service (MDAS) [i.9] should be integrated with the KP Platform for the core network so that events and KPIs data (results from analytics services) from the functions can be used by KP DEs in their autonomic operations (as discussed further in clause 4.6). The KP Level Security Management-DE for the SBA Core Network can leverage the NWDAF's analytic services such as the observed service experience (which enables the Security Management-DE to be aware of traffic communications prediction). And so the KP Security Management-DE can also be aware of abnormal traffic behaviour, and in case the UE causes a change in predicted traffic behaviour or predicted location area, an AS (Application Server) could be notified. The KP DE needs to be aware of abnormal behaviour related network data analytics services (communication related or mobility related), and such an event could be triggered to an Application Server (AS) (any kind of third party server or Mobile Network Operator (MNO) AS server) which subscribed to such an event through the NEF in case the AS is an Over the Top (OTT) server. The AS could then request the PCF according to its rules of abnormal behaviour to bar (delete temporarily a device) the UE (i.e. Subscriber Identity Module (SIM)) within the UDM (Home Subscriber Server (HSS)) through the PCF. The KP may need to know of such dynamics in order to compute new decisions and plans of actions to execute.

In 5G, each network slice has its own security requirements and SLAs (Service Level Agreements) that need to be fulfilled. When a Network Slice has been orchestrated (w.r.t both an E2E Slice or a Slice within the scope of a specific network segment, e.g. RAN, X-Haul Transport, or Core Network), the security needs(policies) for the specific slice should be provisioned and the security requirements of the slice should be assured by autonomic means (closed-loop operations). The autonomic security assurance of the slice is meant to be achieved by the Security Management-DEs responsible for the security assurance of the slice during the lifetime of the slice. E2E autonomic security assurance of slices should be achieved by way of federation of Security Management DEs across all the network segments as illustrated and described in the later clauses and clauses of the present document. What network slicing requires is that Security Management-DEs should be capable of fulfilling security requirements/needs of specific network slices. Network slice providers will desire to be able to select from the marketplace the appropriate Security Management-DEs software or whole KP platforms according to security requirements and SLAs that the Security Management DEs would be expected to fulfil when deployed for live operations. This is because Security Management-DEs capabilities and services may be different in terms of different level of security services they can provide (as discussed earlier on the subject of "Security Services" that form a Service Container Library for the Security-Management-DE). The following types of network slices have different security requirements/needs: network slice for defense industry, network slice for emergency services, network slice for Industry 4.0 vertical, network slice for Internet services, other types of network slices. This subject is covered in more detail in the later clause on "Security Functions Placement in 5G Networks and Autonomic/Dynamic Orchestration of Security Enforcement Policies as Driven by Network Slicing Dynamics".

Figure 7 illustrates the fact that in the GANA KP Platform, DEs interact in exchanging information/knowledge that enable the coordinating DEs to use the information in their decisions on (re)-configuring their respective MEs - which include the lower level DEs in NEs/NFs that are policy controlled by the KP DEs. The figure shows the Reference Point (RfP) regarding DE-to-DE communications that may be necessary in some AMC objectives (with illustrations using **Security-Management-DE**, **QoS-Management-DE**, **Routing-Management-DE**, and **Forwarding-Management-DE**, and **"other" network level DEs** such as **Fault-Management-DE**).

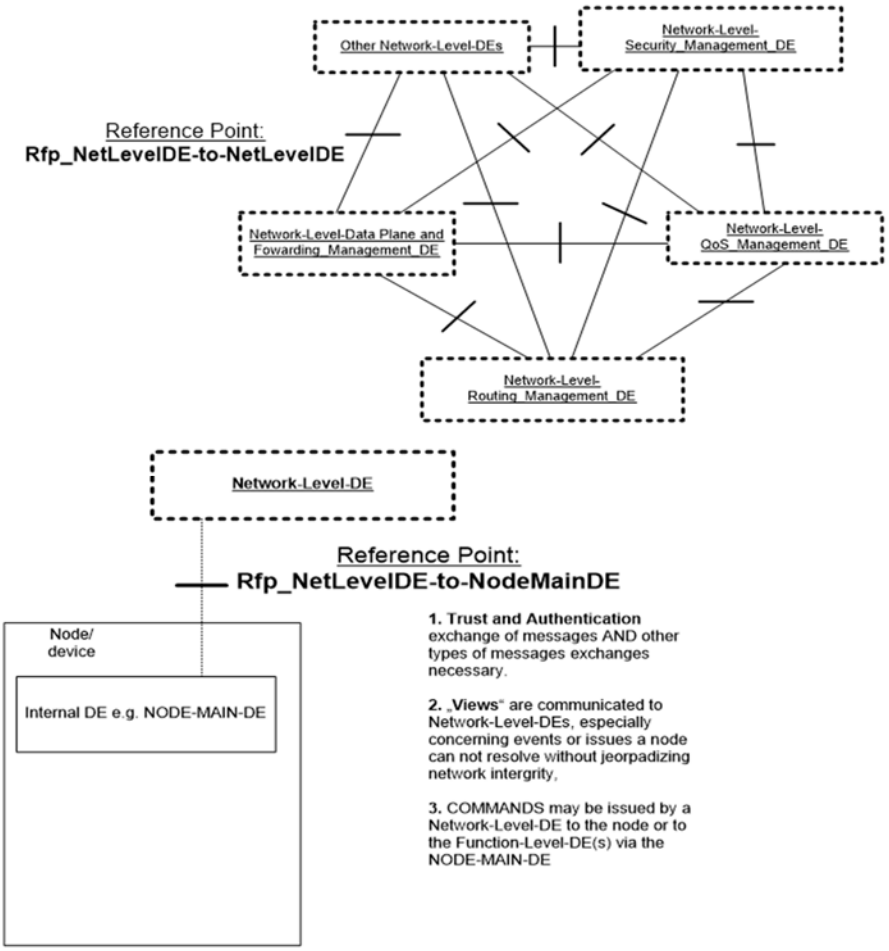

Figure 7: KP DEs interactions in exchanging information that enable their decisions on their respective MEs

Figure 8 presents elaboration on KP DEs interactions in exchanging information/knowledge that enable the coordinating KP DEs to use the information in their decisions on dynamic/adaptive (re)-configuring their respective MEs.

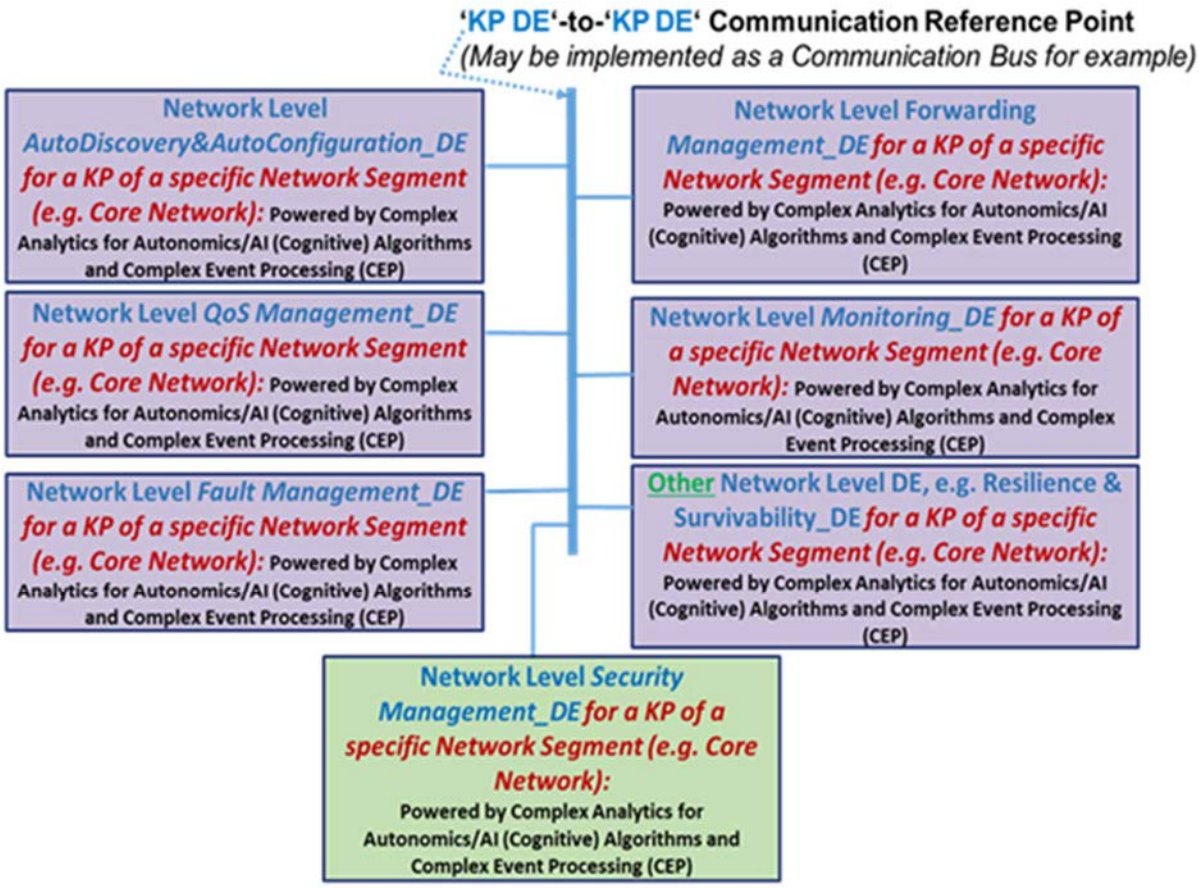

Figure 8: Coordination of KP DEs for Cognitive Decision Making on MEs

4.5.3 Integration of the GANA KP Platform for 5G Core Network with MDAS and NWDAF

This clause addresses integration of the GANA KP Platform for 5G Core Network with MDAS and NWDAF Functions/Services, and how KP Security Management-DE can benefit from the Analytics Services of the Functions/Services.

In brief, MDAS [i.9] and/or NWDAF [i.36] and [i.41] provide analytics services of which a KP Security Management-DE could request for such analytics services independently of whether the analytics services are offered by the MDAF or the NWDAF or complementarily by both functions. And having said that, both functions (MDAS/NWDAF) may be needed by the KP DEs (the Security Management-DE and the other DEs of the KP Platform) at the same time depending on the analytics services that complement each other and yet implemented in the two functions separately. Given the type of analytics services required by KP DEs for certain autonomic operations objectives (use cases) targeted by KP DEs, the KP DEs can rely on analytics services provided by both MDAS and NWDAF. All what matters is that the two functions (MDAS /NWDAF) needs to be integrated with KP Platform such that the KP can selectively trigger or consume analytics services offered by the two functions according to the KP's DEs algorithms' targeted objectives. Such analytics services of the functions include User Equipment (UE) communications related analytics, UE mobility related analytics, abnormal behaviours related analytics, QoS related analytics, Service experience related analytics, NF load related analytics, network congestion related analytics, network performance analytics, and Slice load related analytics, etc.

Security Management-DE could request analytics services offered by the MDAS or NWDAF by describing the analytics that the MDAS or NWDAF should offer to the KP Security Management-DE. For example, upon a Security Management-DE having identified(detected) a general security threat, the Security-Management-DE may want to request for specific analytics services per UE (User-Equipment) to be performed by the MDAS or NWDAF to identify the UE that is posing security problems. The Security Management-DE may want to request for analytics services only for a particular device (i.e. UE)) that has been subscribed to advanced security services. In addition, DE should dynamically request (on-demand) for the analytics services to be performed by the MDAS and/or NWDAF only when the services are needed in order to avoid loading the network with unnecessary traffic monitoring. The Monitoring-DE in association with the Security Management-DE should identify(deduce) the situation or context as to when the analytics services of the MDAS and/or NWDAF should be requested for and for which period of time are the analytics services required by the DEs (either continuously, periodically, or starting at a specific time and for a certain duration, etc.).

A Security Management-DE that subscribed to receive results of such analytics services of an MDAS or NWDAF could be triggered to take certain actions by events from the MDAS or NWDAF in case a certain device (UE) is showing some abnormal behaviour (in terms of communications or mobility behaviour).

The Security Management-DE might also be able to identify the traffic pattern, location pattern which need to be applied by the NWDAF or MDAS such that the NWDAF or MDAS does not need to learn the behaviour of a certain device. An attack could be identified(detected) within other networks and could be used by the KP Security Management-DE and Monitoring-DE to define how to monitor abnormal behaviour in their own network segment they are responsible for.

4.5.4 Real-Time Security federated Threats Repository

Figure 9 illustrates the need for a Database or Repository (Real-Time Inventory) for Detected Security Attacks/Threats, Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies. Such a Database/Repository can be implemented as a member of ONIX System of Federated Information Servers. [i.7] presents ideas on how some ONAP Components can be used to implement a GANA ONIX Server and possibly ONIX's Multiple Federated Information Servers as well. According to the principles of federation of information servers of ONIX for the purpose of building up federated knowledge across the information servers, algorithms should be implemented on each of the ONIX member servers for the purpose of building links and associations among information elements stored on one information server with other information elements stored on other information servers. This then makes the federated ONIX servers appear as forming a single Information/Knowledge Base with correlated information elements, according to the extent to which relationships among information elements can be built. For example, the Information stored in the "Database/Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks" can be linked by the construction of association relationships with information such as Services or Network Slices data stored on other ONIX servers. Such constructed relationships among information elements enable that the information in the "Database/Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks" be enriched with other information such as Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies.

NOTE 1: The indicated Items may be stored in different Databases/Repositories instead, but it may be desirable to store them in the same Repository such that algorithms can be implemented on the Repository to keep the various items correlated to the extent possible and be kept updated in real-time.

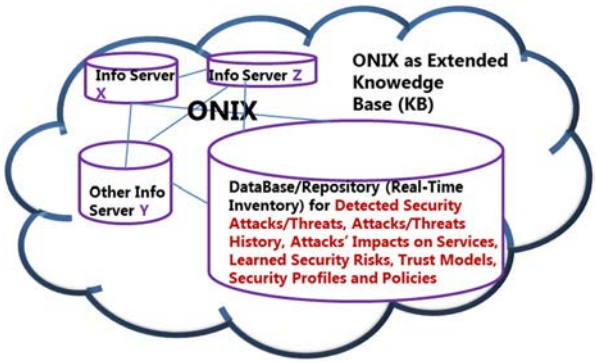

Figure 9: GANA ONIX security database

Figure 10 illustrates the concept of Federation of ONIX systems between two technical and/or administrative domains. A federation translation function (Federation - "Model Based Translation Service" (F-MBTS)) may be required if data models and communication methods for federations employed by the two domains are different. It depicts the architecture of real-time security databases and repositories that store comprehensive threat inventories. These systems enable the detection of security attacks and threats by analysing historical attack data, evaluating the impact of attacks on services, and utilizing AI models to predict future security risks.

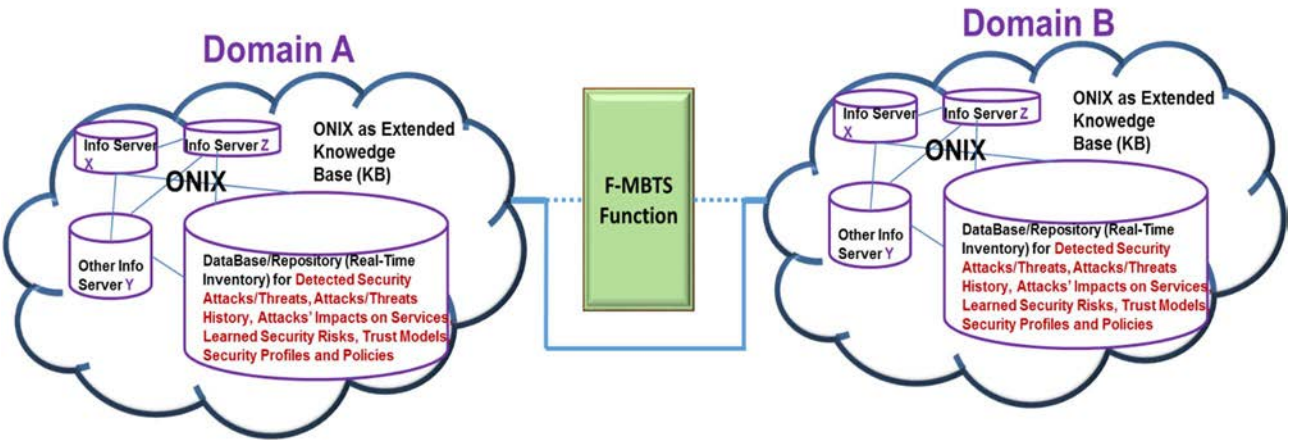

Figure 10: Towards Cross-Domain Federated ONIX Systems and Federated Security Databases

NOTE 2: In the cross-domains federations of Security Databases/Repositories (Real-Time Inventories) for Detected Security Attacks/Threats, Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies, some information may be constrained from being shared across two domains if the domains are administrative (e.g. two different network operators). For example, Trust Models, Security Profiles and Policies, may be constrained from leaking between domains.

ETSI TS 103 195-2 [i.2] defines and describes the F-MBTS Federation Reference Point that involves MDKP communications, whereby MBTS services may be required between the KPs. [i.3], [i.14], [i.7], [i.11] and [i.10] discuss more details on KP to KP federations. Examples of Information that can be exchanged between Domains, e.g. between GANA KPs across multiple Domains—information that may need to be exchanged between Peer Domains are illustrated below (including security related information), as extracted from the White Paper by NGMN [i.10]:

- **KPIs (examples):**
  - Trust Levels (as measure of trustworthiness)
  - Threats Counts of potential impact "**To**" Peer Domain and Severity
  - Threats Counts of potential impact "**From**" Peer Domain and Severity
  - Aggregate state of the Domain in terms of Workload or Load Levels
  - Weights that are indicative of willingness of the Domain to deliver certain services (e.g. transport services)
  - Many Other Types of KPIs that function as security indicators can be identified and defined (and exchanged between KPs)
- **Other Types of Information:**
  - Domain Type(s): DT(s)
  - Domain Identifier: Did
  - Synchronization of actions across multiple GANA KPs
  - Security event information, e.g. Detected Threats/Incidents that may impact Peer Domain
  - Trust Models Information

- Security SLA Violations unresolved
- Load Situations and other types of Situations (e.g. as described in ETSI TR 103 404 [i.5] and ETSI TR 103 473 [i.4])
- Various Types of Information and State Information that enable Multi-Domain State Correlation and resources programming by the GANA KPs for the collaborating Domains (e.g. Access, X-Haul (Fronthaul, MidHaul and Backhaul), Edge/MEC (Multi-Access Edge Computing), Data Center (DC), IP Backbone, and Core Networks, etc.), as outlined in ETSI TR 103 404 [i.5] and ETSI TR 103 473 [i.4] for examples

4.5.5 E2E ASMC across Multiple Domains

Figure 11 and Figure 12 illustrate the key layers (abstraction levels) by which collaborative ASMC can be achieved through the ETSI GANA Model principles, namely:

1) the **NE/NF Level**; (2) the **Network Level**, by NE/NF-Level (Node-Level) Security-Management DE and the Network-Level Security-Management DE, respectively.

There are two options that can be pursued regarding implementing Federated GANA KPs for E2E ASMC for 5G Slices, Networks/Services. Figure 11 presents the **Option-A** (Horizontal Federation), by which the GANA KP Platforms for the specific network segments federate horizontally with each other without the need for an overlay Umbrella Hierarchical GANA KP Platform. Figure 12 presents the **Option-B** (Hierarchical Federation), by which the GANA KP Platforms for the specific network segments federate vertically through an overlay Umbrella Hierarchical GANA KP Platform that receives information from the lower level KPs and coordinates the lower level KPs.

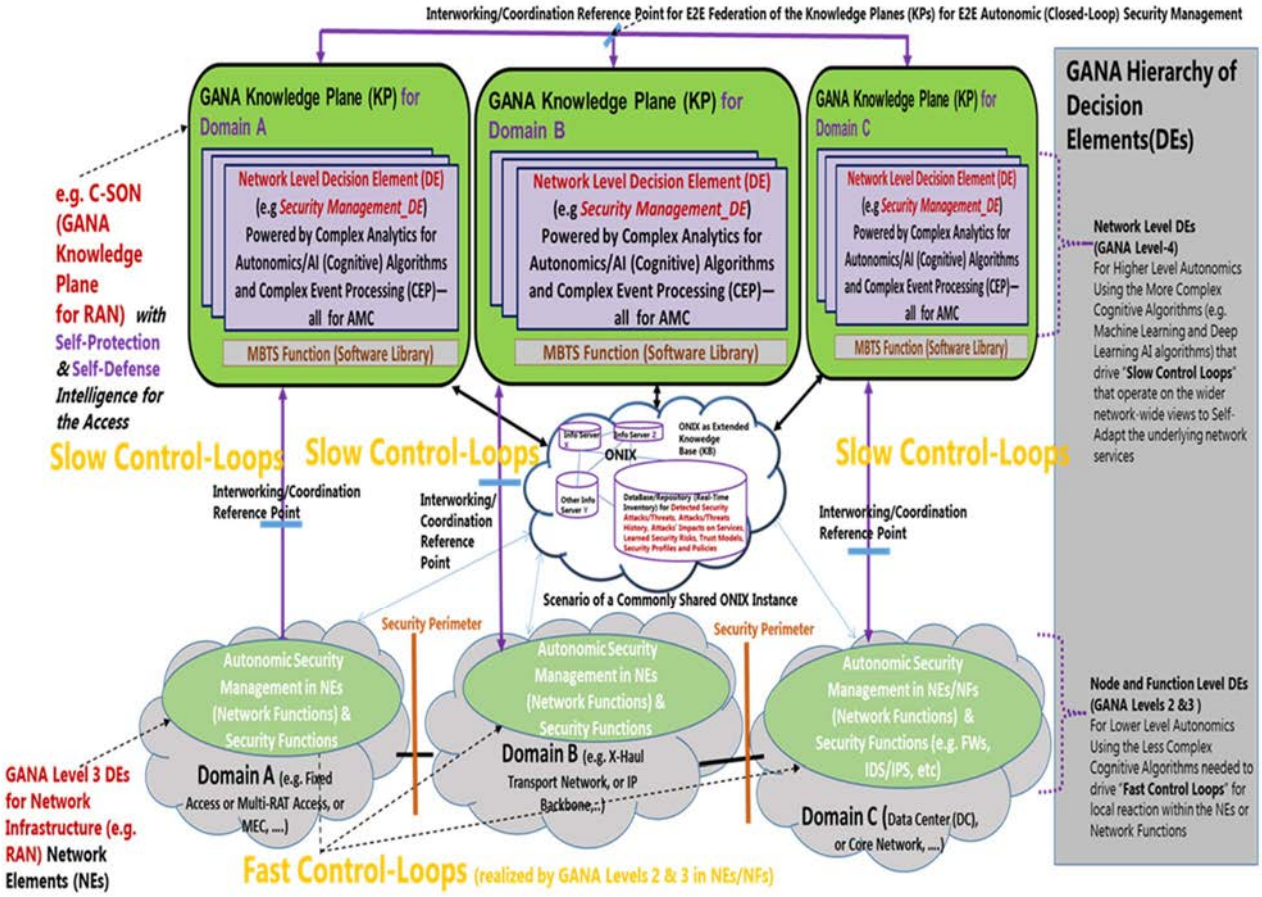

Figure 11: Option-A: Horizontal Federation of GANA KP Platforms from different network segments

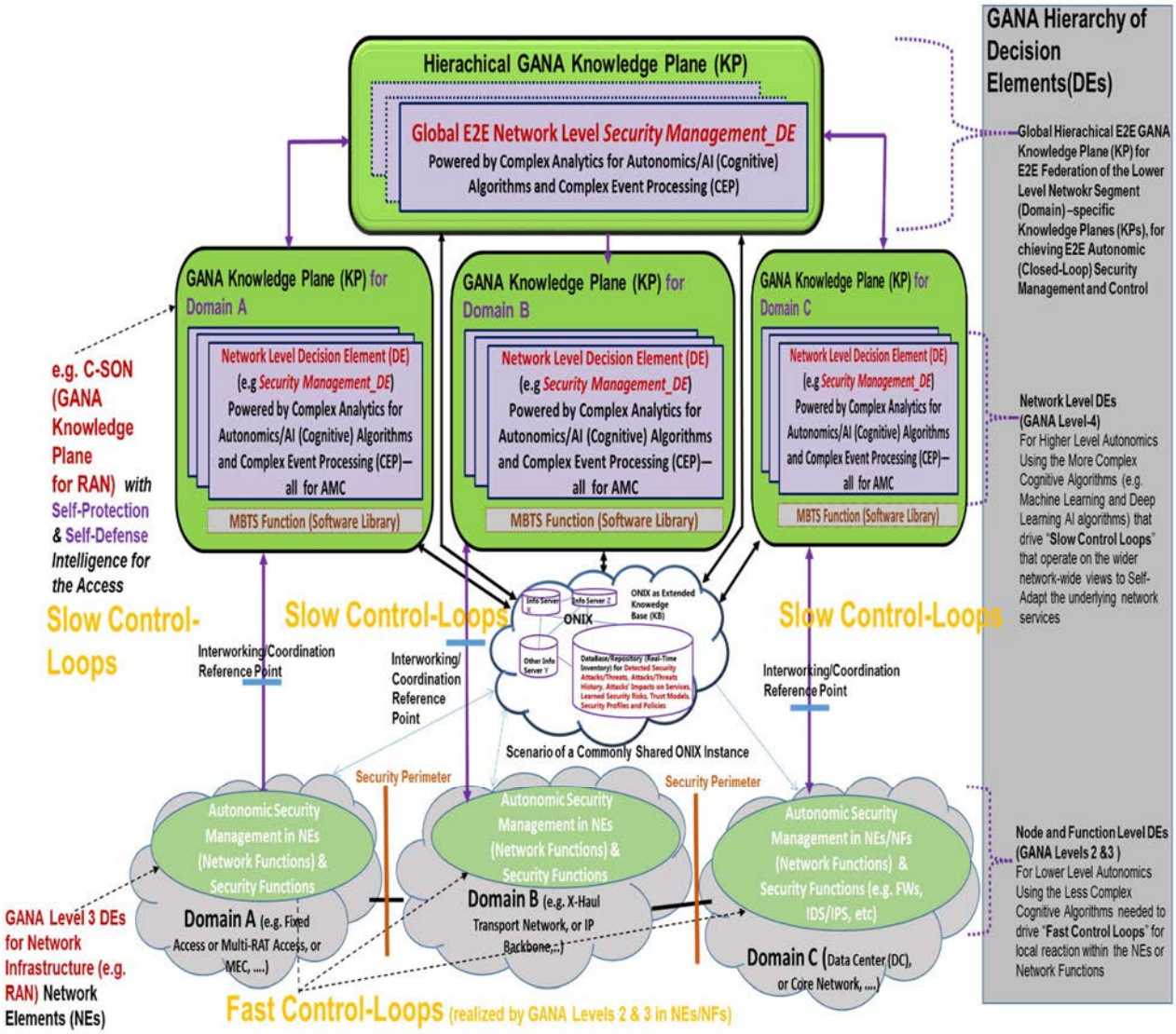

Figure 12: Option-B: Hierarchical Federation of GANA KP Platforms from different network segments with hierarchical E2E GANA KP for coordination

NOTE: 5G PoC White Paper No.6 [i.12] provides some illustrative Capabilities for Implementing Federated Real-Time Security Threats Repositories as ONIX Repositories Federated across Multiple Network Operators.

4.5.6 ASMC

This clause describes why the importance of security analytics by the KP's Security Management DE dynamically triggering and programming On-Demand Monitoring of certain traffic in the network, and the role of Passive Probing and Analytics of traffic copied from the network in that process.

Figure 13 presents a framework on KP driven "Open-Loop" and "Closed-Loop" (Autonomic) Service and Security Assurance for SDN Environments, with the desirable capability of the Security Management DE and the Monitoring DE of the KP in being able to collaboratively trigger On-Demand Traffic Monitoring in the Network. The figure shows some components that may need to integrate with a KP Umbrella Analytics Platform for E2E Autonomic (Closed-Loop) Service and Security Assurance (powered by AI), and also an illustration on a Closed-Loop structure and the associated kinds of interactions between the KP Platform and SDN Controller(s) of the production network. To summarize the interactions flow between the entities in the depicted framework:

- By interacting with the SDN Controller of the Production Network, the Closed-Loop Analytics KP Platform Executes Remediation Strategies automatically by making Certain Configuration Changes to the Network via SDN Controllers for the Production Network. And the Analytics Platform (the KP) continuously retrieves Health Scores data, Monitoring/Telemetry Data, Topology and Configuration-Data from the SDN Controllers for the Production Network and from NE/NF as well.

- Through the SDN Controller for the Test Access Point (TAP) and Switched Port Analyser (SPAN) Aggregation Network, the KP DEs (particularly the Monitoring-DE) can trigger the SDN Controller to configure SPAN Sessions on-demand via SDN Controller for the Production Network to force copied traffic to flow to the Out-Of-Band (OBB) Visibility Aggregation Network that is programmable by the SDN controller for the OOB. The OOB is then programmed to forward traffic to various Analytics Tools in the Centralized Analytics Tools Farm (e.g. Probes and Security Analytics Tools). ETSI TS 103 195-2 [i.2], [i.6] and [i.25] provide insights on how the Monitoring-DE (Network Level Monitoring DE) in the KP Platform can be implemented.

- There are other systems that can serve as Data Sources of the KP Platform, e.g. Performance Management System (PM) and Fault-Management System (FM) for Network and for Information Technology (IT) environments; and NEs/NFs

- The KP Platform may need to send some messages to the components and systems such as the ones indicated on Figure 13. For example, the KP DEs such as the Security Management-DE need to integrate with Ticketing Systems in order to consume events from the Ticketing Systems. The Security Management-DE may be interested in events that may be linked to security attacks incidents and use such events to compute and apply self-defense strategies for the network (the concept of self-defense is covered in more details in clause 4.9). When a problem linked to a particular security incident related Ticket has been resolved and fixed by the KP as a whole, the Ticket is then cleared by the KP Auto-Configuration_and_Auto-Discovery-DE or directly by the KP Security Management-DE. The clearance of the Ticket is performed by the KP as "Dynamic Updates" on Tickets Resolutions/Clearance by KP DEs. i.e. the KP DE accesses the Ticketing System to clear the Ticket if the problem has been found and fixed by the KP.

- A human Service and Network Troubleshooter needs to primarily interface with KP Platform for certain needs linked to Service and Network Troubleshooting in case the KP is operating in an "Open-Loop" Mode in particular and the human in the loop is required during troubleshooting scenarios. The human user may choose to interact with the components marked as "Secondary Service Troubleshooting Position" when necessary.

The capabilities of the Security Management DE and the Monitoring-DE of the KP to trigger On-Demand Traffic Monitoring in the Network can be achieved by the Security Management-DE triggering (on-demand) the copying of traffic from the production network to Analytics Tools (e.g. Probes and Security Analytics Tools) by interacting with the SDN Controller of the Out-Of-Band (OBB). The SDN Controller of the OOB in turn interacts with the SDN Controller of the production network to create dynamic SPAN sessions on certain Nes/NFs to copy traffic to the OOB network. The Security Management-DE may instead go through the Monitoring-DE to cause it to trigger the process via the SDN Controller of the OOB Network and/or installing traffic-monitoring behaviours in certain Nes/NFs directly or via the SDN Controller(s) of the Production Network in addition. This is because the Security Management-DE continuously does analytics and correlation of various events to detect or predict security attacks or risks and may require to trigger, on-demand, the copying/probing and monitoring of certain traffic from the production network for analytics and for a certain duration. Moreover, this on-demand traffic monitoring may be triggered in addition to any traffic being currently monitored in the network and delivering meta-data or events data of interest to the Security-Management-DE. The Security Management-DE should communicate with the Monitoring-DE of the KP so that the Monitoring-DE triggers the monitoring behaviours required by the Security Management-DE. ETSI TS 103 195-2 [i.2], [i.6] and [i.25] provide insights on how KP DEs can be made to request monitoring services through the Monitoring-DE.

NOTE: White Paper No.3 [i.6] presents design principles for **autonomic monitoring using the Monitoring-DE**. Figure 13 also illustrates this aspect by which Security Tools are dynamically fed with traffic that the Security Management-DE of the KP dynamically wants to be copied from the production network for a certain duration, monitored and analysed by the Security Analytics Tools. The intelligence of the Security Management-DE may suspect that certain suspicious traffic is flowing in the network, and so it may decide to trigger the coping of suspected traffic from the network to Security Analytics Tools and obtain the results for further decisions. Such decisions may involve installing firewall rules to block the traffic or using the SDN controller of the production network for that. The OOB Aggregation Network and/or the SDN Controller of the Out-Of-Band (OOB) Network may supply to the Security-Management-DE (or the whole KP Platform) certain meta-data. The meta-data may include data such as KPIs and Metadata created out of raw traffic copied from the production network by the Visibility Solution in place for a particular network (e.g. IETF standardized IP Flow measurements metadata such as sFlow, NetFlow/IPFIX, etc.).

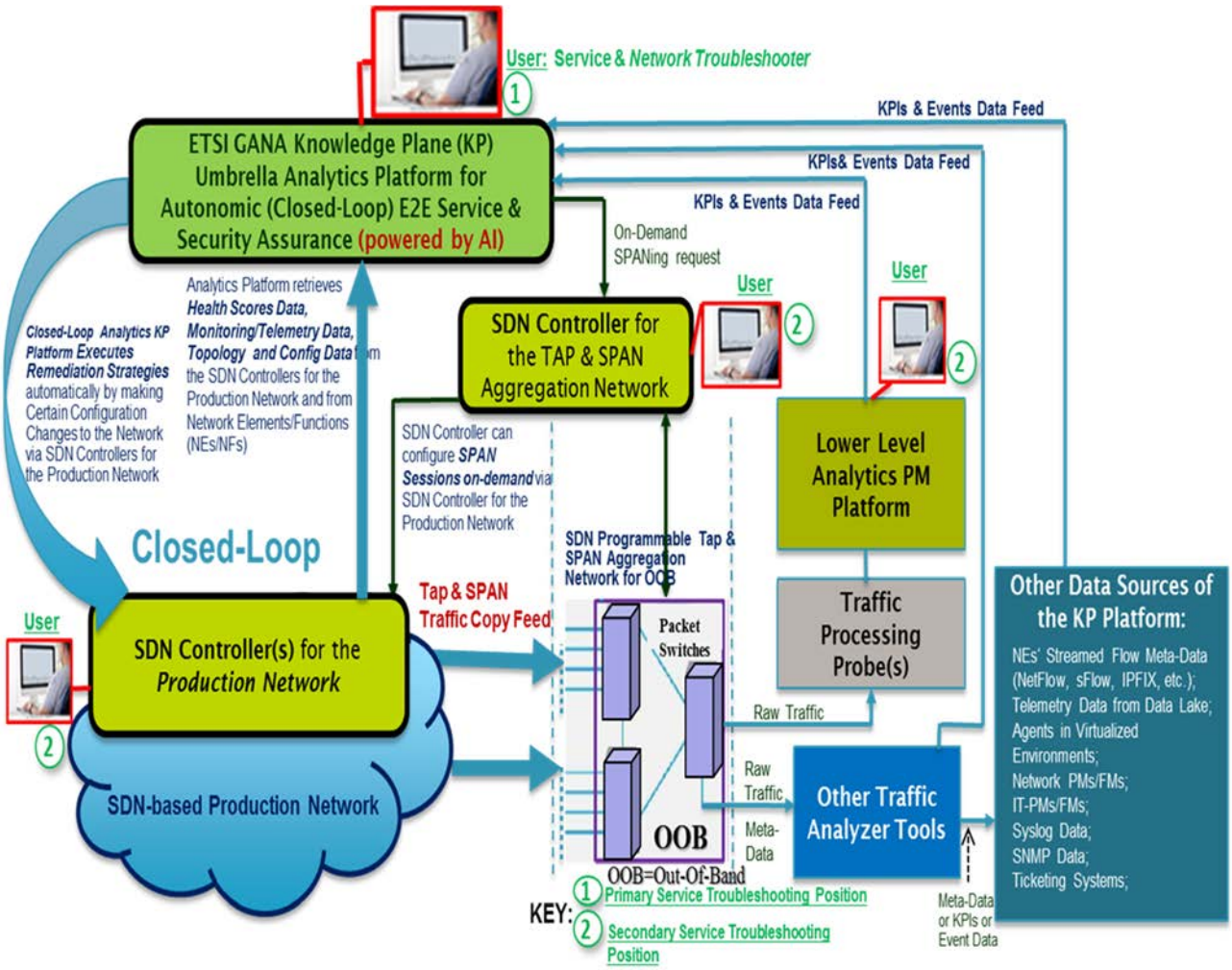

Figure 13: ASMC open and closed loops

4.6 Security-DEs Orchestrations

This clause covers Security Functions Placement/Orchestration in 5G and Autonomic/Dynamic Orchestration of Security Enforcement Policies as Driven by Network Slicing Dynamics, and Security-DEs Orchestrations.

Types of Placement and Orchestration of Security Functions and Security Management-DEs specific to a Network Slice:

1) Static Placement/Orchestration of a Security Function: Security Functions that come in form of Physical Network Functions (PNFs) and those hosted in Nes/NFs in form of PNFs such as some routers or switches are statically placed at specific points in the network topology and infrastructure. Orchestration aspects at such functions involves security service orchestration by simply configuring the physical security function to perform the security enforcement role.

NOTE 1: Programmability requirements aspects for security functions are covered in the next clause 4.7.

2) Dynamic Placement and Orchestration of a Security Function: There are security functions that can be dynamically instantiated as Virtual Network Functions (VNFs), and such VNF based security functions can be dynamically instantiated (placed) at any desirable point in the network where a Network Functions Virtualisation Infrastructure (NFVI) environment is available for orchestrating and managing the VNFs' lifecycles. Orchestration aspects at such functions involves instantiations using a MANO stack and performing the configuration of the virtualized security function.

NOTE 2: Programmability requirements aspects for security functions are covered in the next clause.

3) Security Management-DEs Orchestration: Every network segment should have a GANA KP Platform associated with the network segment as illustrated in the present document. A single instance of a KP Platform is assumed to be responsible of the whole network segment and slices instantiated in that network segment. However, there may be some need to scale the KP Platform or its components according to the size of the network and workload, bearing in mind that the KP Platform may be deployed as a Virtualized Platform. Orchestration and Configuration of the KP Platform's components such as DEs can follow the approach presented in ETSI TS 103 195-2 [i.2]. Here, for network slices instantiated in the network segment the expectation is that a single KP Platform and its Security-Management-DE instance is responsible for service and security assurance of all the Slices instantiated in the underlying network segment. In the underlying Nes/NFs of the network, particularly in those in which a security function or service is required, a single Node-Level Security-Management-DE associated with the NE/NF needs to be orchestrated and configured to realize the "fast control-loop" for self-protection and self-defense from the viewpoint of local observations on whether security is being compromised. The NE/NF level Security-Management-DE is also expected to listen for any policy changes from the KP level Security-Management-DE and apply them while also participating in synchronizations of actions for guaranteeing stability of control-loops as prescribed in ETSI TS 103 195-2 [i.2]. The NE/NF local DEs are called "dDEs" (distributed DEs). "dDEs" are the DEs implemented to operate in NE/NF to realize the "fast control-loops" and also to implement distributed control-loops within the network infrastructure through horizontal interactions with other dDEs across a network scope. Such dDE horizontal interactions relate to a form of "in-network management" - in the case when implementer(s) of the autonomics chose to implement the autonomics through a distributed algorithm than using a centralized approach through the KP level DE(s).

NOTE 3: In the present document the subject of security functions placement is also discussed in other clauses of the present document (with additional illustrations in chapter 7 of the White Paper No.6 [i.12].

Regarding autonomic/dynamic orchestration of security enforcement policies as driven by Network Slicing Dynamics and Security Management-DEs orchestrations, the following aspects come into play:

- The framework for service and security of assurance of network slices is required to be integrated with the framework for Slice Service Fulfilment (including Slice Creation and Orchestration). When a Network Slice definition has been created and passed to platforms used for the provisioning of the slice some data about the Slice Definition data should be passed to the KP Platform responsible for the service and security assurance of the slice. This means a "Specification" of the Network Slice's Objects and Parameters for configuration and the associated Configuration-Data should be passed to the KP Platform as necessary. The KP Platform's Security Management-DE, Monitoring-DE, and QoS Management-DE in particular, need to be provided with the specification of the inputs data pertaining to Slice Definition data (including associated SLAs definitions). They need such inputs in order to perform autonomic service and security assurance of the slice, while also participating in federation with other peer DEs in other KP Platforms within the single Network Operator (as Domain) and across partnering (peering) Network Operator Domains.

NOTE 4: The subject of the various kinds of data/information that can be supplied as **inputs** for the operation of a KP is covered in ETSI TS 103 195-2 [i.2].

- Orchestration and Configuration of the Security Management- DEs of the various KP Platforms to be involved in E2E Autonomic (Closed-Loop) Service and Security Assurance of the E2E Slices.

- Collaborations that may be required between a Security-Management-DE and a DE in the same KP Platform, e.g. a QoS Management-DE and a Monitoring-DE, which programs the required monitoring services in the network. The key design question that needs to be addressed here, with respect to the collaborations of the DEs, is to identify system-critical and other resources in the network and information base that are relevant to the two non-functional feature categories that need to be enabled in connection with slicing, namely: security and resource management (including QoS). If Resource X and Resource Y are both relevant to an E2E or Single-Tier Slice A, then the orchestration and/or (re)-configuration of a Security Functions (SFs) and QoS Functions (QFs) required by the Slice should be jointly (collaboratively) put into consideration by the Security-Management-DE(s) and QoS-Management-DE(s), respectively, in order to see how to access, modify, block, or release Resources X and Y so as not to affect the integrity of Slice A or the proper functioning and consistency of state and information from either SF perspective, QF perspective, or a global overall perspective. Following GANA principles (in ETSI TS 103 195-2 [i.2], [i.6] and [i.25]), the Security Management-DE should communicate with the Monitoring-DE of the KP so that the Monitoring-DE triggers the monitoring behaviours required by the Security Management-DE. ETSI TS 103 195-2 [i.2], [i.6] and [i.25] provide insights on how KP DEs can be made to request monitoring services through the Monitoring-DE. The Security-Management-DE then consumes the monitoring data it requires from the network as necessary for its autonomic behaviours. The Security-Management-DE may require to coordinate with other DEs of the KP Platform, e.g. the QoS Management-DE, to coordinate on joint actions in reaction to impact of detected or predicted attacks on a network slice. The same applies for the function level DE such as QoS Management-DE, it should communicate with the Monitoring-DE of the KP so that the Monitoring-DE triggers the monitoring behaviours required by the QoS Management-DE. The QoS Management-DE then consumes the monitoring data it requires from the network as necessary for its autonomic behaviours. Such that when QoS requirements and SLAs for the Slice are being challenged (as per monitored network conditions and incidents), the QoS Management-DE can (re)-tune QoS provisioning mechanisms of the network adaptively. In addition, or alternatively, the QoS-Management-DE may communicate with the Security-Management-DE so that the DEs can jointly compute paths or resources that can be created or switched over to by traffic flows such that QoS SLAs and Security SLAs for the Slice are jointly assured. Such DEs coordination may require the participation of the Monitoring-DE and/or other DEs of the KP Platform.

- Behaviours expected of Security Management DEs of each KP Platform in response to various dynamics of network slices and security problems that may be detected or predicted concerning their impacts on specific slices and SLAs. Some scenario examples that convey this conceptual idea are as follows:

  - In an E2E slice covering the tiers of access, edge, metro, transport, and core, the Security-Management-DEs of the KP Platform of each tier may use different security mechanisms in each tier for anomaly or threat detection regarding which parameters and patterns are analysed (differently for each tier) to detect and mitigate potential threats or attacks on the network that are affecting the slice under protection and many other valuable/critical resources.

  - When specific SLAs are binding, even on an E2E slice, the implementation and the mechanisms for achieving this same SLA often differ and depend on what tier is under question. For instance, protecting with encryption or fingerprinting/signature an application flow/stream which is part of a slice is different in terms of the mechanism used on the edge and access part of a network as compared to that in the transport or even core part. As illustrated on Figure 14, the Framework recommends having a set of KPs, each of which covers one tier of the E2E chain, and employing a distinct type of security mechanism for the same functionality.. Upon federating those KPs to cover the E2E path, the various security mechanisms for the same functionality would be aligned and streamlined to form an E2E consistent service.

- Examples of data and messages that may be exchanged by the KP Platforms involved in the E2E Federation to effect actions by other KP receiving the data and messages include but are not limited to:

  - State messages regarding behavioural information detected or deduced based on the captured and processed metrics in a KP covering a specific tier of the E2E chain; this information helps other KPs which cover other tiers of the E2E chain in their decision-making process and actions and enable consistency and synergies in the operation of the functions under focus (security functions, resource management (including QoS) functions) on an E2E basis across multiple KP Platforms.

  - Specific state messages regarding the status of e.g. encryption or anomaly detection in a specific KP (and its corresponding tier) passed on to an adjacent federated KP platform.

- Other kinds of data and messages as described in clause 4.6 and in NGMN's 5G E2E Architecture Framework [i.10] and [i.16].

Figure 14 illustrate the aspect of Federation of Security Policy Enforcement Engines (namely Security Management DEs) over the value chain tiers (Access/Edge, Transport, Core, etc.) with E2E 5G Slices.

NOTE 5: The lower part of Figure 14 is based on Figure 2 that is readable.

The other aspects discussed in the present document on E2E Federation of GANA KP Platforms complement Figure 14.

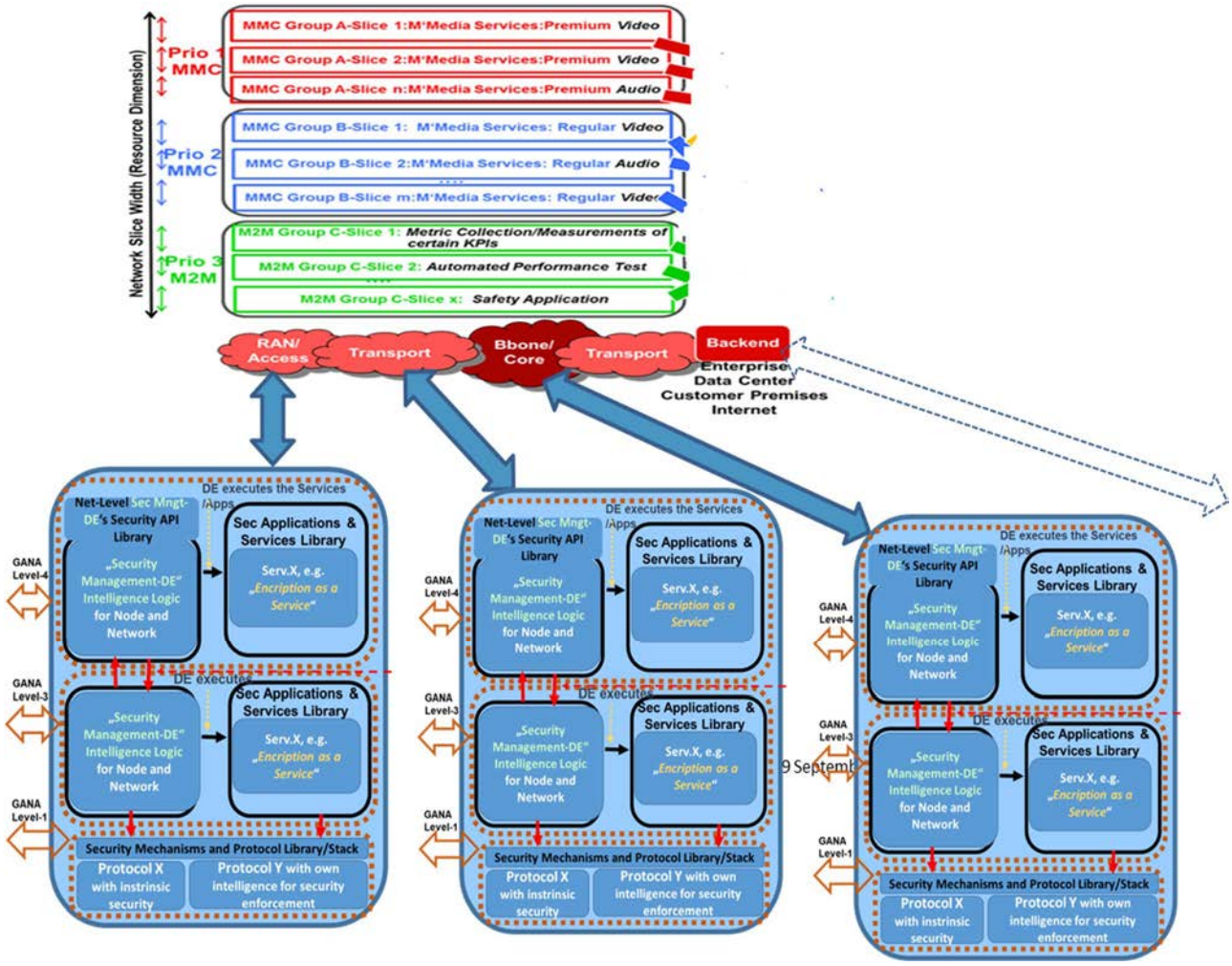

Figure 14: Federation of Security DEs for E2E 5G Slices

4.7 Programmability of security attacks detection and threats/risks predictions

Security Functions such as Firewalls, Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) need to expose programmatic interfaces through which Security-Management-DEs can program the functions by adaptively configuring them with security policies that should be applied by the Functions. While at the same time the security functions should enable the Security Management-DE to obtain/receive events data, KPIs data, and logs from the NE/NF. As demonstrated in White Paper No.6 [i.12] there are suppliers of Security Functions that are programmable and enable implementers of Security-Management-DEs to program them as driven by the intelligence of the DEs, as illustrated by security functions/platforms programmability presented in White Paper No.6 [i.12] as examples (there many other suppliers already offering such capabilities).

Based on the structural model for realizing/implementing AMC Control-Loop(s) of a Security Management-DE meant to operate at Network Level (in the GANA KP), Figure 15 provides insights on an example of how a Security Management-DE that operates on network level DE in the KP can be implemented. This refers to implementation guide terms of the various data and event sources that can be considered by the implementer/supplier of the DE, and the systems and components the DE may need to interact with for various purposes. For example, the DE may interact with the various entities indicated, for the purpose of programming security functions or causing resource or service backup entities to be orchestrated and instantiated. Below, a summary of some of the entities that the Security Management-DE should be able to interact with (the numbers on communication flows are simply there to distinguish the types of interactions and not necessarily the ordering of the communications), and the reasons for the desired interactions:

- **Orchestrator**: The interaction between an Orchestrator (e.g. Service Orchestrator) with a GANA KP Platform in general relates to the KP's need to consume events that an Orchestrator may be able to propagate to the high level platform (i.e. the KP). KP consumption of such events is needed for its Complex Event Processing (CEP) and capabilities in reasoning about the state of the network and computing plans of actions as necessary. The events may be of interest to all the KP DEs or to specific DEs such as the Security Management-DE. The interaction is also for the purpose of the KP's needs to invoke the services of the Orchestrator dynamically based on the requirements for adapting the underlying network or to orchestrate new instances of resources or services in a strategy to remediate and ensure continuous network services delivery and guarantee SLAs and security. The KP DEs also need to consume various kinds of KPIs that may be shared by the Orchestrator. KP strategies such as remediation against problems may be applied reactively or proactively to detected or predicted problems, respectively. More details on this subject can be found in ETSI TS 103 195-2 [i.2] and [i.3], [i.7], [i.6], [i.11] and [i.8].

- **SDN Controller of the Production Network**: The interaction involves the KP Platform being able to (re)-configure (program) the network via the SDN controller. The interactions also involve the SDN Controller dynamically supplying Information to the KP Platform, e.g. Topology Data, Telemetry, Health scores data (concerning the underlying network), Configuration-Data (as configured for dissemination to the KP by the KP level Monitoring-DE on the SDN Controller). The configuration on the SDN Controller, regarding the data and information the SDN Controller should disseminate to the KP platform or Data Lakes may be done by the KP level Auto-Configuration and Auto-Discovery-DE. As discussed in [i.3], [i.7], [i.6], [i.11] and [i.8], the KP Platform may selectively program the network directly via the SDN Controller or other management and control systems available in the environment.

- **Monitoring-DE in the KP**: The interactions that may be implemented, regarding KP DEs such as the Security-Management-DE interacting with the Monitoring-DE are as follows: All the KP DEs may express monitoring needs, regarding the specific needs to receive monitoring data from the network to the Monitoring-DE implemented as part of the KP Platform. The Monitoring-DE in turn configures and tunes the monitoring services of the network (including monitoring services/functions within the NEs/NFs and also the Out-Of-Band (OOB) traffic copying and analytics tools). For more details on the subject of the functionality of the KP level Monitoring-DE, readers should refer to ETSI TS 103 195-2 [i.2]. The other source that offers important insights on Autonomic Monitoring functionality and services of the Monitoring-DE at KP Level is [i.6]. ETSI TS 103 195-2 [i.2], [i.6] and [i.25] provide insights on how KP DEs can be made to request monitoring services through the Monitoring-DE, including insights on how the Monitoring-DE (Network Level Monitoring DE) in the KP Platform can be implemented in general.

NOTE 1: White Paper No.3 [i.6] in particular, together with Demo material presented at the 5G PoC site in White Paper No.3 [i.6], present design principles for **autonomic monitoring using the Monitoring-DE**. Also, when it comes to monitoring in NFV environments, ETSI GS NFV-REL 004 [i.47] and ETSI GS NFV-SEC 013 [i.46] provide very useful insights on monitoring in virtualized environments, including Security Monitoring in such NFV environments.

- **SDN Controller of the Out-Of-Band (OOB) Visibility/Aggregation Network:** The Security Management-DE may require that some traffic be copied from the network on-demand to the Out-Of-Band (OOB) Visibility Network. The traffic is then analysed by some Analytics Tools in the Tools Farm and results in form of KPIs or Detected Network Events be communicated by the Analytics Tools to the Security Management -DE in the KP Platform. The Security-Management-DE may trigger this via the Monitoring-DE in the same KP Platform to which the Security Management-DE belongs (as shown on Figure 13), instead of directly interacting with the SDN Controller of the Out-Of-Band (OOB) Network. The intelligence of the Security Management-DE may suspect that certain suspicious traffic is flowing in the network, and so it may decide to trigger the coping of suspected traffic from the network to Security Analytics Tools and obtain the results for further decisions. Such decisions may include installing firewall rules to block the traffic or using the SDN controller of the production network for that. The OOB Aggregation Network and/or the SDN Controller of the Out-Of-Band (OOB) Network may supply to the Security-Management-DE (or the whole KP Platform) certain meta-data such as KPIs and Metadata (e.g. IETF standardized IP Flow measurements meta-data created from the raw traffic copied from the network such as sFlow, NetFlow/IPFIX, etc.). There are various ideas on how such Metadata can be used in security attack detection or predictions, e.g. the following sources provide insights on this subject: [i.26], [i.27], [i.28], [i.29] and [i.40].

- **Data Lake:** Various Data that may be available through a Data Lake may be of interest to the Security Management-DE to consume in form of the raw data or in form of knowledge that may be synthesized by Data Analytics/AI algorithms running on the Data Lake.

- **NEs/NFs (e.g. Router, Switch) and security-specialized Nes/NFs such as Security Functions such as Intrusion Detection System (IDS), Firewall (FW), Intrusion Prevention System (IPS), Network Data Analytics Function (NWDAF) defined by ETSI TS 129 520 [i.36] and ETSI TS 123 288 [i.41], Management Data Analytics Service (MDAS) defined by ETSI TS 128 533 [i.9]:** The Security Management-DE may interact with the Nes/NFs directly in order to dynamically program them to install security policies, and also to receive KPIs, Event and Log data feed that may be required by the Security-Management-DE's Algorithms (and even by other KP DEs), from the Nes/NFs.

NOTE 2: Clause 4.6 provides detailed insights on this subject.

- **Management and Orchestration (MANO) Stack:** The Security-Management-DE may decide to orchestrate via the MANO, the instantiation of some security functions in response to some security attacks or vulnerabilities/risks/threats detected or predicted. KPI and event data feed from the instantiated security functions need to flow to the Security Management-DE. With a that, "Remediation Actions" against detected or predicted security attacks/threats/vulnerabilities may be executed by the Security Management DEs on certain NEs/NFs such as the security functions instantiated as Virtual Network Functions (VNFs).

- **Ticketing Systems:** The Security Management-DE needs to integrate with Ticketing Systems in order to consume events from the Ticketing Systems that may be linked to security attacks incidents and use such events to compute and apply self-defence strategies for the network (the concept of self-defence is covered in more details in clause 4.9). When a problem linked to a particular security incident related Ticket has been resolved and fixed by the KP as a whole, the Ticket is then cleared by the Security Management-DE as Dynamic Updates on Tickets Resolutions/Clearance by KP DEs, i.e. the DE accesses the Ticketing System to clear the Ticket if the problem has been found and fixed by the KP.

- **ONIX:** The Security Management-DE needs to exercise Information Storage and retrieval from ONIX by the DE, particularly with the DataBase/Repository (Real-Time Inventory) of the ONIX that stores Detected Security Attacks/Threats, Attacks/Threats History, Attacks' Impacts on Services, Learned Security Risks, Trust Models, Security Profiles and Policies.

NOTE 3: As demonstrated in White Paper No.6 [i.12] there are suppliers that offer capabilities that enable to implement Security Management-DE and the Control-Loop(s) Structure presented in this clause. White Paper No.6 [i.12] provides illustrative examples on the subject of the enabler capabilities that can be leveraged in implementing a Security Management-DE, namely: **Firewall Security Functions**, the **Data Lake**, and an **ONIX Real-Time Repository (Real-Time Inventory) for Detected Security Attacks/Threats and Risks**.

Figure 15 presents a desirable capability of the Security Management DE to operate in Open-Loop and Closed-Loop Mode and its operation in Correlation and ASMC.

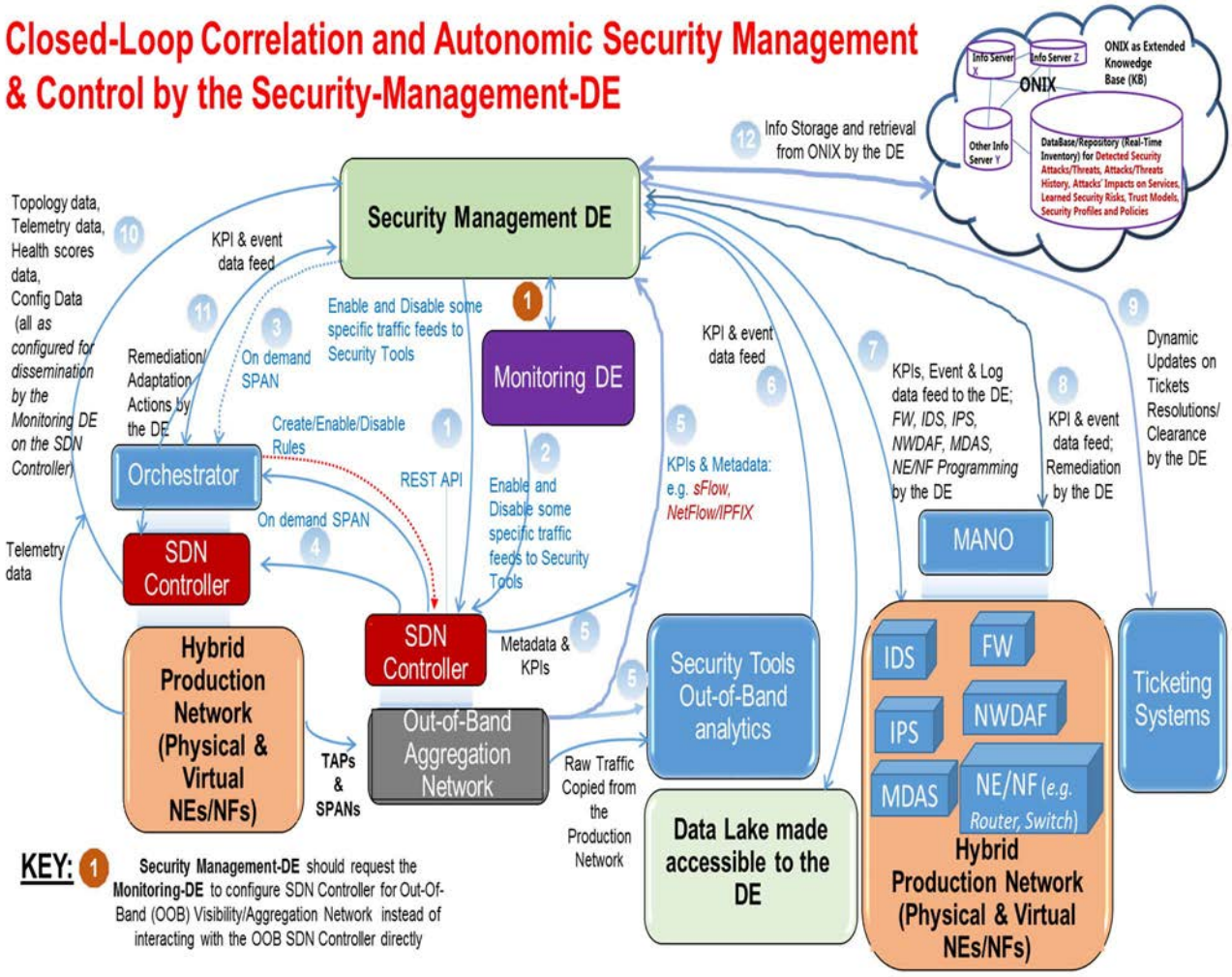

Figure 15: Capability of the ASMC DEs to operate in Open-Loop and Closed-Loop Mode

4.8 "Self-Protection" and "Self-Defending " 5G E2E ASMC

This clause covers the subject of implementing "Self-Protection" and "Self-Defending Behaviours" for specific Network Segments/Domains by GANA KP Platforms, within Single Network Operator and across Multiple Network Operators.

This clause provides insights to implementers of ASMC on how to leverage research results emerging from various Research and development (R&D) projects on Autonomic/Cognitive Networks (i.e. Self-Organizing/Self-Adaptive Networks) and their associated Autonomic Management and Control Systems. Leveraging such results in implementing Security-Management-DEs that are based on the ETSI GANA standard and conform to the Framework presented in the present document. It is possible to map the features prototyped in the various R&D projects, with respect to security management components that employ AI in automating security policing and dynamic network and service security management aspects, to Security Management-DEs meant to operate at specific GANA Levels. That enables to implement the DEs that fully conform to the ETSI GANA standard and the Framework presented in the present document. With the definitions of Self-Protection and Self-Defense provided earlier, implementers of Security-Management-DEs can be guided accordingly on how to make a DE exhibit both capabilities/features. And implementers can use the definitions in mapping the features prototyped in the various R&D projects, with respect to security management components that employ AI in automating security policing and dynamic network and service security management aspects, to Security Management-DEs meant to operate at specific GANA Levels. Then they can transform the prototyped components into products that conform to the GANA standard and the Framework, accordingly. For example, the following sources provide insights on some prototype implementations of components for implementing **self-protection and self-defending strategies and behaviours for the network** [i.18], [i.19], [i.20], [i.21], [i.22] and [i.24].

Additionally, the following sources provide some insights that can help implementers of Security-Management-DEs' self-protection and self-defense behaviours for the network and its services: [i.30], [i.31], [i.32], [i.33], [i.34] [i.35], [i.37] and [i.43]. [i.39] provides useful insights on automated security policies road-mapping. [i.17] provides useful insights for consideration in tools for network automation that can also be considered when implementing KP DEs in general.

The following are example Use Case Scenarios for **Self-Protection** and **Self-Defense Behaviours**:

- A Use Case on **Self-Protection** of the Network within Single Network Operator and across multiple Network Operators: User-plane integrity, roaming security, and flash-network traffic are use case scenarios where self-protection within 5G can be very essential. In a partially proactive manner, the security system can check the cryptographic protection integrity of the use data plane at regular intervals and report in a timely manner via a trigger if any anomaly is detected. This way, the protection of user plane data and its integrity from a security (and mainly cryptography) viewpoint is established. When it comes to roaming, updating security-parameters related to roaming in 5G as users move across multiple operators is a key aspect; for proper self-protection, those parameters need to be passed on in real-time, processed correctly, mapped among operators, and also protected from unauthorized access. Flash network traffic is a use case which comes into play upon a massive amount of entities and/or messages they generate, typically, e.g. in an Internet of Things (IoT) (or massive-IoT) scenario in 5G. For appropriate self-protection, differentiated scaling of the control and data planes by the collaboration of the GANA KP Platforms and management and control systems (including MANO stack) responsible for each network segment has to be done. CUPS (Control and User Plane Separation) is a significant step towards standalone 5G. The intelligence of the GANA KP Platform(s) to dynamically orchestrate and/or scale control and data plane functions include KP(s) strategies to address autonomic slice service fulfilment, service assurance and security assurance requirements (SLAs), and such KP operations include both, single KP and KP federated operations. The self-protection strategies by the KP Platforms should put in place (trigger) the monitoring of each of the planes and adjust the scaling accordingly in order not to overload any of the planes with massive requests.

- A Use Case on **Self-Defense** of the Network within Single Network Operator and across multiple Network Operators. A signalling storm and a DoS attack on the infrastructure (as opposed to a DoS attack on the end-user device level/tier) are two out of many other scenario examples that confront 5G systems with significant threats and where systematic self-defense mechanisms and strategies that a KP Platform should orchestrate are essential in mitigating those threats. With many distributed control systems being directly or per-proxy coordinated and managed by 5G, mechanisms analogous to NAS (Non Access Stratum) in 3GPP such as EPS Mobility Management (EMM) and EPS Session Management (ESM) use signalling to set the scene for 5G-based data transfer and application flow. A popular attack type and eminent threat is producing a signalling storm, meaning an "strongly inflated beyond manageable bounds" amount of messages (e.g. NAS EMM and ESM), causing the draining of system-critical bottleneck resources in the processing (signalling, control chain). Self-defense in 5G by KP Platforms within a single operator or across multiple operators would activate a protective shield for critical resources and entities, e.g. the ones preforming NAS functionality including EMM and ESM, and then throttle the flow of incoming signalling requests that collectively form the attack.

4.9 Summary

This clause provides a Summary of Roles that should be played by Artificial Intelligence (AI)/ML Models/Algorithms, Distributed Ledger Technologies/Blockchain, NFV, SDN, and Big Data in the Framework for E2E Federated GANA KPs for AI/ML-powered ASMC Across Multi-Domain 5G Networks.

Role of Artificial Intelligence (AI)/ML Models/Algorithms in the Framework: The role is elaboratively discussed in the present document with respect to AI/ML algorithms a GANA Security Management DE (just like in the case of other GANA DEs as discussed in clause 4 of the present document) may be designed to employ.

Role of Distributed Ledger Technologies/Blockchain in the Framework Regarding the question of the role or relevance of Distributed Ledger Technologies/Blockchain in the Framework, the following are some examples from literature:

- [i.56] presents what the authors call a proposal that suggests monitoring transaction metrics on a blockchain to enable an adaptive machine to adjust operational parameters of the consensus protocol or even switch to a different consensus strategy, arguing that this autonomic approach enhances the overall performance of the blockchain by utilizing self-defined policies and goals. In this regard, the adaptive machine being referred to in [i.56] could be GANA Security Management DE in the GANA KP Platform level, or possibly even a Security Management DE GANA level 3 implemented in a certain NE/NF.

- Another perspective of relevance is that of Identity and Access Management (IAM) using distributed ledger technology, such as discussed in [i.57]. In this regard, a GANA Security Management DE may be designed to employ distributed ledger technology in Identity and Access Management (IAM) if it is meant to implement IAM.

Role of NFV in the Framework: The role or consideration of NFV in the Framework is as follows:

- As presented in [i.78], NFV MANO stack should be made to integrate with the GANA KP together with various management and control systems through which the KP can selectively program the network, while also taking into account KP integration with Event Sources, Data Sources and Info/Knowledge Sources.

- Figure 1 presents the two layers (abstraction levels) of Security-Management DEs that should be of focus in introducing Autonomic (Closed-Loop) Security Management and Control. The Security Management DE at GANA level 3 for fast control loop in a NE/NF implies that the DE may be implemented in a physical NE/NF or a VNF.

- Figure 3 presents an illustration of how a KP Level GANA DE can be implemented (more details on approaches to designing GANA DEs are found in ETSI TS 103 195-2 [i.2]). Some security functions such as Firewalls, IPS, IDS, or Security Gateway, may be implemented as VNFs and not as PNFs.

- Figure 6 presents two implementations Options for the interactions of a Security-Management-DE in the KP with a Security Function (e.g. Firewall, IPS, IDS, Security Gateway) or a NE/NF in general. Some security functions such as Firewalls, IPS, IDS, or Security Gateway, may be implemented as VNFs and not as PNFs.

- Figure 15 presents Capability of the Security Management DE to operate in Open-Loop and Closed-Loop Mode and its operation in Correlation and ASMC. Some security functions such as Firewalls, IPS, IDS, or Security Gateway, may be implemented as VNFs and not as PNFs.

Role of SDN in the Framework: The role or consideration of SDN in the Framework is as follows:

- As presented in [i.78], SDN controller(s) should be made to integrate with the GANA KP together with various management and control systems through which the KP can selectively program the network, while also taking into account KP integration with Event Sources, Data Sources and Info/Knowledge Sources. As described in the corresponding section the SDN controller serves the purpose of exposing an Northbound Interface through which the GANA KP can program the network segment under its responsibility provided that an SDN controller makes sense to be deployed for the particular network segment/domain.

- Figure 13 presents KP driven "Open-Loop" and "Closed-Loop"(Autonomic) Service and Security Assurance for SDN Environments, with the capability of the Security Management-DE and the Monitoring-DE of the KP in being able to collaborate in triggering On-Demand Traffic Monitoring in the Network for Analytics of Suspected Traffic.

- Figure 15 presents Capability of the Security Management DE to operate in Open-Loop and Closed-Loop Mode and its operation in Correlation and ASMC. The value of SDN controller for the production network being steered by the GANA KP Security Management DE and the SDN controller for the Out-Of-Band (OOB) traffic monitoring network is described in clause 4.7 on Programmability Requirements for Security Functions, and Autonomic/Dynamic Security Policies Enforcement by KPs, as Driven by Security Attacks Detection and Threats/Risks Predictions.

Role of Big Data in the Framework: The role or consideration of Big Data in the Framework is as follows:

- As presented in [i.78], certain types of Big Data Applications should be made to integrate with the GANA KP such that the Network level DE can invoke them for certain objectives during its operation, based on the functionality or services offered by the Big Data Applications, or possibly the Big Data applications can be implemented as integral parts of the GANA KP for a specific network segment/domain.

4.10 Other Autonomics Use Cases

The following perspectives should be taken into consideration by implementers of Closed-Loop Self-Adaptive Orchestration and Context-Aware Application of Security Protocols/Mechanisms/Functions in 5G by GANA Security Management DEs and their AI/ML-Algorithms:

1) Embedded AI/ML in 5G security for various entities (networks, devices, platforms, etc.).

2) What is meant by Closed-Loop Self-Adaptive Orchestration of Security Protocols/Mechanisms/Functions in 5G by GANA Security Management DEs and their AI/ML-Algorithms.

3) Closed-Loop Self-Adaptive Context-Aware Application of Security Protocols/Mechanisms/Functions in 5G by GANA Security Management DEs and their AI/ML-Algorithms.

4) Levels at which AI/ML Algorithms for AMC by Security-Management-DEs is desirable (high level description as Use Cases that DE vendors should consider):

   - NE/NF Level Security Management DE (in certain NEs/NFs, including in security functions like Firewalls, IPS, IDS, etc.).

   - Security Management DE in a UE (for certain UEs).

   - Security Management DE in an End User Terminal such as an IP Host such as a Laptop or Desktop.

   - Security Management DE in the KP Platform level.

   - Security Management DE in other type of connected device of some sort.

NOTE 1: Relevant insights on this subject provided in earlier clause of clause 4 should also be considered along with the insights provided in this clause.

Table 1: 5G Security GANA Level DEs

Level at which AI/ML Algorithms for a Security-Management-DE should be considered	Type of Entity that encapsulates/embeds the Security-Management-DE	What AI/ML Algorithms, and Type/Kinds of Algorithms, can be employed to achieve for ASMC within the specific scope	Examples of Behaviours the Security-Management-DE could execute w.r.t. the autonomics targets related to Self-Protection and/or Self-Defense, including dynamic or adaptive (re)-orchestration and/or (re)-configuration of Security related MEs e.g. Protocols and Mechanisms like Secure Sockets Layer (SSL), Transport Layer Security (TLS), Protocol for N32 Interconnect Security (PRINS) [i.63], etc.
1) **GANA Level 3 (Node-Level) for every NE/NF** (ideally for guaranteeing secure-by-design principles for an NE/NF).	**NE/NF in general, such as a Router, a Switch, a next Generation Node Base Station (gNB), Mobile Core NEs/NFs; Firewalls, IPS, IDS, etc.).**	There is already a lot of work in literature on what AI/ML algorithms of various Types/Kinds can bring to the Security related aspects for **Security hardening** for the NE/NF or for **self-protection** policies and configuration, and **self-defence** against detected or predicted security attacks/risks/threats by the NE/NF autonomically and autonomously (without human intervention).	GANA Node Level Security Management DE may execute various autonomic behaviours (or autonomous behaviours that remove the need for human intervention/involvement) based on its intelligence towards implementing self-protection and self-defence of the NE/NF or entities that a special NE/NF like Firewalls, IPS, IDS, etc. is responsible for protecting or defending. Some autonomic/autonomous behaviours of the GANA Node Level Security Management DE may include dynamic or adaptive (re)-orchestration and/or (re)-configuration of Security related MEs e.g. Protocols and Mechanisms like SSL to TLS to ensure that their related security policies and parameters employed by the NE/NF as a whole or its internal entities are dynamically computed and enforced to meet certain objectives. See note 1. As described earlier in the present document, the Security Management DE should also be responsible for morning for security patches and upgrades software that become available from the supplier of the NE/NF or internal components, fetch and apply them. The Security Management DE should continuously monitor and assess the performance of its Security related MEs e.g. Protocols and Mechanisms and take actions in case of performance problems, such as requesting the host Operating System (OS) to allocate more resources to the MEs as may be required.

Level at which AI/ML Algorithms for a Security-Management-DE should be considered	Type of Entity that encapsulates/embeds the Security-Management-DE	What AI/ML Algorithms, and Type/Kinds of Algorithms, can be employed to achieve for ASMC within the specific scope	Examples of Behaviours the Security-Management-DE could execute w.r.t. the autonomics targets related to Self-Protection and/or Self-Defense, including dynamic or adaptive (re)-orchestration and/or (re)-configuration of Security related MEs e.g. Protocols and Mechanisms like Secure Sockets Layer (SSL), Transport Layer Security (TLS), Protocol for N32 Interconnect Security (PRINS) [i.63], etc.
2) **GANA Level 4 (Network-Level) for every Network Segment**, e.g. Access Network, Transport Network, Core Network, Data Center Network, Telco Cloud for a network segment of some sort, (ideally for guaranteeing secure-by-design principles for a network segment).	The **GANA KP Platform** for the specific network segment, e.g. Access Network, Transport Network, Core Network, Data Center Network, Telco Cloud for a network segment of some sort.	There is already a lot of work in literature on what AI/ML algorithms of various Types/Kinds can bring to the Security related aspects for **Security hardening** for the Network Segment or for **self-protection** policies and configuration, and **self-defence** against detected or predicted security attacks/risks/threats by the GANA KP for the Network Segment autonomically and autonomously (without human intervention).	GANA Node Level Security Management DE may execute various autonomic behaviours (or autonomous behaviours that remove the need for human intervention/involvement) based on its intelligence towards implementing self-protection and self-defence of the NE/NF or entities that a special NE/NF like Firewalls, IPS, IDS, etc. is responsible for protecting or defending. Some autonomic/autonomous behaviours of the GANA Network Level Security Management DE may include dynamic or adaptive (re)-orchestration and/or (re)-configuration of Security related MEs e.g. Protocols and Mechanisms like SSL to TLS to ensure that their related security policies and parameters employed by the NE/NF as a whole or its internal entities are dynamically computed and enforced to meet certain objectives. For example, the concept of Security Controller described in [i.62] and is responsible for TLS Autonomous Management and maintaining a complete view of the network located in the data plane and holds the TLS Security Policies that should be applied to the nodes residing in the data plane, would be implemented as the GANA KP level Security Management DE. The GANA KP Security Management DE would be responsible for configuring and managing TLS connections in a dynamic and autonomous manner. See note 1. The Security Management DE should continuously monitor and assess the performance of lower level Security Management DEs in NEs/NFs and take actions in case of performance problems, such as requesting the NFVO to re-orchestrate the VNF if the VNF's security becomes compromised or of high risk level, as may be required. This may include rebooting of the NE/NF by the Security Management DE in the case of a PNF.

Level at which AI/ML Algorithms for a Security-Management-DE should be considered	Type of Entity that encapsulates/embeds the Security-Management-DE	What AI/ML Algorithms, and Type/Kinds of Algorithms, can be employed to achieve for ASMC within the specific scope	Examples of Behaviours the Security-Management-DE could execute w.r.t. the autonomics targets related to Self-Protection and/or Self-Defense, including dynamic or adaptive (re)-orchestration and/or (re)-configuration of Security related MEs e.g. Protocols and Mechanisms like Secure Sockets Layer (SSL), Transport Layer Security (TLS), Protocol for N32 Interconnect Security (PRINS) [i.63], etc.
3) **User Equipment (UE) like Mobile Device,** e.g. Smartphone, as a GANA Node (for certain UEs).	**User Equipment (UE).**	There is already a lot of work in literature on what AI/ML algorithms of various Types/Kinds can bring to the Security related aspects for **Security hardening** for the UE or for **self-protection** policies and configuration, and **self-defence** against detected or predicted security attacks/risks/threats by the UE autonomically and autonomously (without human intervention).	For Further Study. See note 2.
4) **End User Terminal such as an IP Host such as a Laptop or desktop**, as a GANA Node.	**End User Terminal such as an IP Host.**	There is already a lot of work in literature on what AI/ML algorithms of various Types/Kinds can bring to the Security related aspects for **Security hardening** for the End User Terminal or for **self-protection** policies and configuration, and **self-defence** against detected or predicted security attacks/risks/threats by the End User Terminal autonomically and autonomously (without human intervention).	Similar behaviours to the case of a Security Management DE at GANA Level 3 (Node-Level) for every NE/NF (ideally for guaranteeing secure-by-design principles for an NE/NF).
5) **Other type of connected device of some sort**, viewed as a GANA Node.	**Other type of connected device of some sort.**	There is already a lot of work in literature on what AI/ML algorithms of various Types/Kinds can bring to the Security related aspects for **Security hardening** for the End User Terminal or for **self-protection** policies and configuration, and **self-defence** against detected or predicted security attacks/risks/threats by the End User Terminal autonomically and autonomously (without human intervention).	For further study.
NOTE 1: The case for Security Management DE autonomics use cases for protocols such as SSL and PRINS [i.63] is open for further study. NOTE 2: There are some behaviours that a Security Management DE in a UE may share in common with the case of a Security Management DE at GANA Level 3 (Node-Level) for every NE/NF (ideally for guaranteeing secure-by-design principles for an NE/NF).			

NOTE 2: Although GANA defines what is called GANA Level-1 DEs (Protocol level DEs), i.e. for a DE embedded inside a protocol that makes the protocol intrinsically to embed a closed control-loo that makes its autonomic (self-adaptive), the ETSI GANA standard recommends to focus particularly on GANA Levels 2 up to 4 when introducing autonomics in network architectures and their associated management and control architectures.

5 Zero Trust Principles and Smart Contracts to GANA KPs Platforms Federations

This clause presents insights on applying Zero Trust Principles and Smart Contracts to GANA KPs Platforms Federations for E2E Agile Service Delivery and Self-Management and Control of Networks and Services by dynamic resource orchestrations and (re-) configurations by the jointly collaborating GANA KPs.

This clause provides brief insights on the topic while the more detailed elaborations are to be found in the work of the deliverable number 4 "How Zero Trust and Security Principles should be applied in GANA KP-to-KP Federations" of the NIST Multi-Domain KPs for Service Federation for 5G and Beyond Public Working Group (MDKP-PWG) [i.61]. Considering E2E Federated GANA KPs for AI/ML-powered Autonomic Management and Control Operations Across Multi-Domain 5G Networks in general as discussed in ETSI TR 103 747 [i.78], [i.61] and as illustrated in Figure 11 and Figure 12, the GANA KP Platforms should implement and employ Zero Trust Principles (ZTP) in interacting with other KPs and with their network segment they are responsible for through their KP Security Management DE or a standalone Zero Trust DE that should be part of the DEs set of the GANA KP. That means the same applies in the E2E Federated GANA KPs for AI/ML-powered ASMC Across Multi-Domain 5G Networks.

The Zero Trust Architecture was introduced by NIST in [i.64]. Implementation Frameworks for Zero Trust and application of Smart Contracts have been emerging, also for the 5G context. The following sourcing provide various useful insights on this subject [i.65], [i.66], [i.67] and [i.68].

The following are aspects that need further study in the light of Applying Zero Trust Principles and Smart Contracts to GANA KPs Platforms Federations (possibly this would be covered by the NIST MDKP PWG [i.61]):

- The Role of Autonomics (closed control loops) and AI/ML in the application of Zero Trust Principles by GANA KP Platforms.
- Application of Zero Trust Principles (ZTP) by GANA KP in interacting with other KPs and with their network segment they are responsible for.
- The consideration of a design principle on whether to have a Zero Trust DE as standalone DE among the GANA KP DEs set or as part of the Security Management DE.
- The interworking of the GANA KP Security Management DE (possibly with Zero Trust DE part being embedded within it or as standalone DE in the GANA KP Platform) with a Security Management DE implemented in the upper "Service Federation Management, Orchestration and AMC Platform" that may be integrated with a GANA KP Platform via the KP's Northbound Interface as being studied in [i.61]. The hierarchical "Service Federation Management, Orchestration and AMC Platform" requests a GANA KP for orchestrating network connectivity and services required within the domain the GANA KP is responsible for, while the GANA KP may also interact with other GANA KPs for networks that are required to establish end to end network connectivity services required by the "Service Federation Management, Orchestration and AMC Platform" as being studied by the work in [i.61].

NOTE: If Zero Trust DE functionality is not implemented as integral part of a GANA KP Security Management DE then a Zero Trust DE in the GANA KP should also interact with a Zero Trust DE in a Service Federation Management, Orchestration and AMC Platform".

6 Quantum Cybersecurity use cases in 5G and Verticals

This clause provides brief insights on applying Quantum Computing and Autonomics to certain Networking Use Cases in 5G and Verticals. Also, this clause provides brief insights on the topic while the more detailed elaborations are to be found in the work of the deliverable number 4 "How Zero Trust and Security Principles should be applied in GANA KP-to-KP Federations" of the NIST MDKPs for Service Federation for 5G and Beyond Public Working Group (MDKP-PWG) [i.61].

The other subject covered by this clause is on progress in Quantum Computing and Cybersecurity Standards that need to be taken into consideration, both in the scope of: (1) Quantum Computing and AMC for 5G and Beyond networks-(e.g. 6G networks); and (2) certain Networking Use Cases in 5G and Verticals.

The subject of Quantum Computing and AMC for 5G and Beyond networks (e.g. 6G networks) and for verticals is a subject that is receiving attention in research and will continue to be researched. Of particular interest in the Framework presented by the present document is Quantum Computing and Autonomics or AMC for 5G and Beyond networks (e.g. 6G networks), to understand the impact on the design of GANA DEs (e.g. GANA Security Management-DEs of the GANA KP Platforms and their associated AI/ML algorithms. The following are some examples of work in literature and ongoing work in ITU-T that is of relevance to the subject of Quantum Computing and AMC for 5G and Beyond networks (e.g. 6G networks):

- There is ongoing work in ITU-T on Recommendation ITU-T Y.3819 [i.70] on "Quantum key distribution network - Requirements and architectural model for autonomic management and control".
- The study report in [i.69] on Machine Learning and quantum computing for 5G/6G communication networks.

NOTE: Possibly the subject of Quantum Computing and AMC for 5G and Beyond networks (e.g. 6G networks) would be covered by the NIST MDKP PWG [i.61]).

Regarding progress in Quantum Computing and Cybersecurity Standards that need to be taken into consideration certain Networking Use Cases in 5G and Verticals, ETSI established the first two specific standardization working groups for addressing quantum technologies, dealing with standardization of quantum communication listed below:

- The Industry Specification Group on Quantum Key Distribution (ETSI ISG-QKD) focused on quantum cryptography and quantum communication technologies. Special emphasis is given to security proofs and to security certification of quantum key distribution products.
- The Technical Committee Cyber Security Working Group for Quantum-Safe Cryptography (ETSI TC Cyber security (CYBER) WG Quantum Safe Cryptography (QSC)) aims to assess and make recommendations for quantum-safe (i.e. safe from a quantum computer) cryptographic primitives protocols and implementation considerations. The focus is on the practical implementation of quantum-safe primitives, including performance considerations, implementation capabilities, protocols, benchmarking and practical architectural considerations for specific applications.

Finished ETSI Technical Reports (TRs)/Technical Specifications (TSs) are [i.71], [i.72], [i.73], [i.74], [i.75], [i.76], and [i.77], as well as the following ones:

- The two ETSI Technical Reports ETSI TR 103 616 [i.73] and ETSI TR 103 823 [i.79] give descriptions facilitating understanding and easy comparison of each of the schemes in the third round of the NIST standardization process.
- ETSI TR 103 619 [i.76] defines migration strategies and recommendations for Quantum-Safe schemes and ETSI TS 103 744 [i.71] defines methods and architectures for combining a quantum-safe key encapsulation method with a classical key exchange method to ensure the resulting negotiated keys are as secure as the strongest of the individual schemes being combined.

The ETSI Technical Reports (TRs)/Technical Specifications (TSs) whose output should also be considered are:

- ETSI TR 103 949 [i.80]: Migration to QSC for Intelligent Transport Systems (ITS)
- ETSI TR 103 966 [i.81]: Deployment Considerations for Hybrid Schemes
- ETSI TR 103 965 [i.82]: Impact of Quantum Computing on Cryptographic Security Proofs

- ETSI TR 103 967 [i.83]: Impact of Quantum Computing on Symmetric Cryptography

7 Telco Data space in ASMC Applications

TM Forum and ETSI TR 103 195-1 [i.84] are introducing the topic of Telco Data Space (Data Sharing Framework) for data-driven network automation role in enabling developments of AI/ML powered Autonomic Security Management Applications that include Security SLAs Driven Resource(s) and Service(s) Orchestration in Autonomic/Self-Management of 5G Networks. This clauses looks into the importance of Telco Data Space in fuelling the development of AI/ML Models for various types of GANA DEs, thanks to various kinds of data that can be made available through Telco Data Space Framework to GANA DE innovators and developers and suppliers to develop and train the AI/ML models employed by specific GANA DEs.

The TM Forum has recently started an initiative on Telco-Data Space, supported by so-called catalysts projects that are aimed and implementing and demonstrating various use cases for the Telco Data Space concept [i.50]. The following are insights extracted from TM Forum's initiative:

1) General Definition of a Data Space: A Data Space is system designed to allow sovereign and secure exchange of data within a "trusted eco-system" involving multiple stakeholders.

2) General value of what a Data Space brings in enabling data-driven networking:

   - Achieving sovereign data exchange and processing within a common framework (e.g. the Telco Data Space framework defined by TM Forum).

   - Fostering better collaboration among stakeholders - thereby enhancing cross-data analytics scenarios.

3) TM Forum has defined a Framework for single Telco Data Space infrastructure for the sharing and processing of Telco dataset that covers the following aspects:

   - Defining Data Usage constraints blueprint.

   - Providing Telco data space catalogue services for management and control of data space per Use Cases.

   - Prototyping of Use Cases with data-space nodes (connectors) for enforcing the consortium data governance.

   - Leverage on emerging initiatives Gaia-X [i.51] and [i.52] and International Data Spaces Association (IDSA) [i.53] and [i.54].

- Example Use Cases TM Forum Catalysts considered that are of relevance to Autonomic/Autonomous Networking:

  - Trusted AI model with ISV (Independent Software Vendor) to develop an Autonomous Network (and the questions that needed to be answered in such a catalyst project):

    - Share Dataset access with usage control to train an AI model? Monetization/Certification?

    - Share trained AI model with usage control? Monetization/Certification?

    - AI Model Lifecycle Management (LCM) usage control? Monetization/Certification?

  - "Steering roaming" Application and Energy saving Application development and implementation based of data sharing by network operators.

  - Cognitive Module and DE concept in the context of ETSI TC INT/AFI GANA DEs and 3GPP NWDAF/MDAS.

From this study by TM Forum it can be noted that Telco Data Space can play a very important role in fuelling the development of AI/ML Models for various types of GANA DEs, thanks to various kinds of data that can be made available through Telco Data Space Framework to GANA DE innovators and developers and suppliers to develop and train the AI/ML models employed by specific GANA DEs such as the Security Management DE meant for implementation on GANA Level-3 (Node Level) or on Network level (GANA KP level Security Management DE). The other aspect to be learnt from the study by TM Forum is that the AI/ML models and even the GANA DEs (as software modules or Apps) can also be shared among stakeholders in Telco Data Space through the same Telco Data Space Framework.

NOTE: More details such as the Telco Data Space Framework Architecture and various Use Cases prototyped by TM Forum catalysts projects are available in TM Forum's project [i.50].

8 ASMC in Open RAN

This clause discusses perspectives that need to be taken into consideration regarding the impact of Security challenges in Open Radio Access Network (O-RAN) and E2E security assurance solutions deployments on Automated and ASMC in 5G. The focus, when it comes to security in Open RAN, is on security challenges that can be addressed through Automated and ASMC in 5G context. The following sources provides very useful information from which one can derive the kinds of security challenges that can be addressed through Automated and ASMC for 5G networks: [i.58], [i.59], [i.60] and [i.63].

Three perspectives presented below are worthy to consider in the light of the Framework presented by the present document on Generic Framework for E2E Federated GANA KPs for AI/ML-powered Closed-Loop ASMC Across Multi-Domain 5G Networks. The three perspectives are (further elaborated below):

1) Mapping of the GANA Framework onto the O-RAN Architecture to reveal how some of the GANA concepts and principles are addressed in O-RAN architecture.

2) How the Hybrid Self-Organising Network (SON) (Centralized SON (C-SON) and Distributed SON (D-SON)) has demonstrated the implementation of the GANA for traditional RAN.

3) E2E ASMC by way of Federation of GANA KP Platforms and their Security Management DEs, within a single network operator domain and across multiple network operator domains.

NOTE: The elaborations to the three perspectives are given below.

Mapping of the GANA Framework onto the O-RAN Architecture to reveal how some of the GANA concepts and principles are addressed in O-RAN architecture.

Table 2: Mapping of the GANA Framework onto the O-RAN Architecture by O-RAN Alliance to reveal how some of the GANA concepts and principles are addressed in O-RAN architecture

O-RAN Alliance Architecture Component/functional entity	Mapping to a GANA Concept /Functional Block	Comments
Non Real Time RAN Intelligence Controller (RIC) + rApps	**Upper** GANA KP with DEs being the rApps	The ONIX functionality is not available in the O-RAN architecture; Some level of an MBTS functionality is available in O-RAN architecture but not as fully as defined in ETSI TS 103 195-2 [i.2]
rApp	Network Level (KP level) DE for Upper GANA KP	
Near Real Time RAN Intelligence Controller (RIC)	**Lower** GANA KP with DEs being the rApps	The ONIX functionality is not available in the O-RAN architecture; Some level of an MBTS functionality is available in O-RAN architecture but not as fully as defined in ETSI TS 103 195-2 [i.2]
xApp	Network Level (GANA KP level) DE for lower GANA KP	
NOTE: If concept of dApp will be introduced by the O-RAN Alliance in functions such as Distributed Unit (O-DU), and Centralized Unit (O-CU), etc.	GANA Level 2 and/or Level 3 DE	Even if there would be no concept of dApp, GANA Level 2 and Level 3 DEs can still be implemented in the network functions provided by vendors, such as O-RU, O-DU, O-CU

How the Hybrid SON (C-SON and D-SON) has demonstrated the implementation of the GANA for traditional RAN: As discussed in clauses 4 and 10 of the present document the insights for GANA AMC implementation have been facilitated by the fact that the ETSI GANA Model is a Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI/ML Models for Multi-Layer AMC of Networks and Services. GANA as a Hybrid Model for Multi-Layer Autonomics and associated Multi-Layer AI Algorithms exhibits the following characteristics:

- As described in clause 4 of the present document GANA is a Hybrid Model (ETSI White Paper No.16 [i.1] and ETSI TS 103 195-2 [i.2]):
  - It guides and offers flexibility to implementers on the choice to implement certain autonomics as distributed software and algorithms within certain NE/NF i.e. "Micro Autonomics", while being able to also choose to implement some algorithms as centralized algorithms in the KP Platform ("Macro Autonomics").
- Hybrid SON Model is compatible with GANA (more details in White Paper No.1 of 5G PoC [i.3]):
  - Hybrid SON (C-SON (Centralized SON) and D-SON (Distributed SON)) are considered as an implementation of the GANA Model for the RAN.
  - As illustrated in clause 10 of the present document and in White Paper No.1 of 5G PoC [i.3] C-SON should be viewed as an implementation of the GANA KP for the RAN, while D-SON is an implementation of GANA level 2 and 3 DEs as illustrated by the relevant figures in clause 10 of the present document.

E2E ASMC by way of Federation of GANA KP Platforms and their Security Management DEs, within a single network operator domain and across multiple network operator domains: This subject has been covered extensively in clauses 4 and 10 of the present document as illustrated in the following figures: Figure 11 and Figure 12.

9 NGMN ODiN Requirements call for Security Frameworks and Solutions suitable for ASMC Assurance in E2E Disaggregated Networks

NGMN recently launched some work on CSPs requirements for an E2E Operating Model for use in Operating Disaggregated Networks (ODiN) [i.49]. What this means is that there is need to perform research on how ODiN requirements call for Security Frameworks and Solutions suitable for Self-Adaptive (Autonomic) Security Assurance in E2E Disaggregated Networks.

The following are some of the security analysis points carried out by the NGMN ODiN project regarding operating E2E disaggregated networks, points of which ODiN Requirements' need for Security Frameworks and Solutions suitable for ASMC assurance in E2E Disaggregated Networks are discussed in this clause:

- The systems and processes used for managing security are likely to come under additional strain as the number of vendors, functions, and interfaces in a typical mobile network increase [i.49]. The implication is that instrumenting GANA Security Management DE within the various NEs/NFs and ensuring that the Security Management DE embedded with a NE/NF has visibility into events and monitoring data gathered in real time on all the interfaces of the NE/NF should be implemented to enable the DE to analyse and detect or predict security risks, threats and attacks and compute plan of actions to execute to implement self-protection policies and self-defense policies for the NE/NF. In addition to that GANA KP Platform level Security Management DE of the GANA KP for a specific network segment/domain (for "slow control-loops") helps complement the autonomics by the lower-level Security Management DEs in NE/NF (for "fast control-loops") according to GANA principles on complementarities of the two levels for autonomics DEs and associated control loops.

- As more components and functionalities are introduced, the network potentially becomes vulnerable as there are more integration points [i.49]. This could arise in the open interfaces in any network domain (RAN, Core, Transport), open-source software and off the shelf solutions [i.49]. Functional splits and Edge computing could also contribute to wider physical attacks [i.49]. The implication is the same as described above, i.e. the value of introducing GANA Security Management DE embedded with individual NEs/NFs and complementing that with GANA KP Platform level Security Management DE of the GANA KP for a specific network segment/domain.

- Possibility of more vulnerabilities and attacks as the network tends to be more exposed to the public domain if disaggregation is implying hosting software to the public cloud [i.49]. The implication of this is that there would be need for a consideration for a GANA KP Platform with its Security Management DE would need visibility into the events and interfaces and monitoring data within the public cloud, and this may be a challenge to realize. While still the NFs deployed in the public cloud should provide for an embedded Security Management DE for the NF's implementation of the fast control-loop for security management and assurance.

- Different software and different hardware might cause new vulnerabilities as they are developed separately [i.49]. Each of these vendors or companies have different experiences towards attacks. This is where consolidated monitoring becomes essential [i.49]. Each of the software and hardware needs to be fully monitored to detect any possible intrusion [i.49]. The implication is that monitoring data generated in real time should be made available to the Security Management DEs of the GANA KP Platforms responsible for the specific network segments/domains of which the monitoring data has been generated.

- Extended and distributed network visibility [i.49]. The implication is same as described above: monitoring data generated in real time should be made available to the Security Management DEs of the GANA KP Platforms responsible for the specific network segments/domains of which the monitoring data has been generated.

- Extended "SecOps" and "ZeroTrust" policy introducing security by design and throughout the application life-cycle (development, deployment and operations) [i.49]. The implication is that a GANA KP Platform for a specific network segment/domain with its Security Management DE should be implemented in such a way that the Security Management DE should implement Zero Trust principles in its intelligence for self-protection and self-defense of its network segment/domain.

- DevSecOps approach has also to implement the monitoring of security logs and events as well as in integration and production chains [i.49]. The implication is that the security logs and events should serve as vital data for training the AI/ML models employed by the Security Management DEs at GANA Level 3 (GANA Node Level) and GANA Level 4 (GANA KP level).

NOTE: Overall, the implication of the various points described above (taken from the ODiN study [i.49]) is the need for distributed GANA Security Management DEs implementation in various systems (NEs/NFs) where security risk, threat or attack can potentially be there or potentially occur; and need for autonomics for self-protection and self-defense implementation by GANA DEs at Level 3 and GANA level 4; and then application of Zero Trust principles where possible to apply such principles (particularly at the GANA KP's Security Management DE level).

10 GANA in ETSI 5G PoC Implementations executed by the Industry

This clause describes the framework ecosystem shown below which corresponds to various kinds of Proof of Concepts (PoCs) implementations work whereby GANA Autonomics are being built and demonstrated to the industry. This ecosystem is 5G network slice-centric; meaning the stakeholders are assigned roles of slice consumer or customer and slice producer/provider. Resource management (including allocation, provisioning, monitoring, guaranteeing, and adapting) is governed by GANA Autonomic Management and Control Paradigm (AMC) and uses slices as main instruments of leverage. Whether CSPs, Independent Software Vendors (ISVs), Hardware Vendors, Manufacturers, or End-Customers, all stakeholders get their interactions and service transactions organized using 5G slices with E2E capabilities) and those slices are orchestrated by the Autonomic/Autonomous Network (AN) in the shown ecosystem to form the workflow of the scenario use-cases and shape the behaviour the GANA autonomic management and control components (with capabilities related to AI and ML). The guidelines for behavioural modelling come from high-level policies, objectives (which may be formulated as intents), which are then broken down into smaller objectives and actions by the AN in line with the GANA AMC.

Figure 16 presents the Ecosystem that is the basis for the ETSI INT AFI WG 5G PoC on 5G Network Slices Creation with ETSI GANA AMC of 5G Slices and E2E Orchestration and the Consortium. The depiction of the high-level design principle of the 5G PoC ecosystem and associated actors / roles relationships and interactions that are described in [i.3].

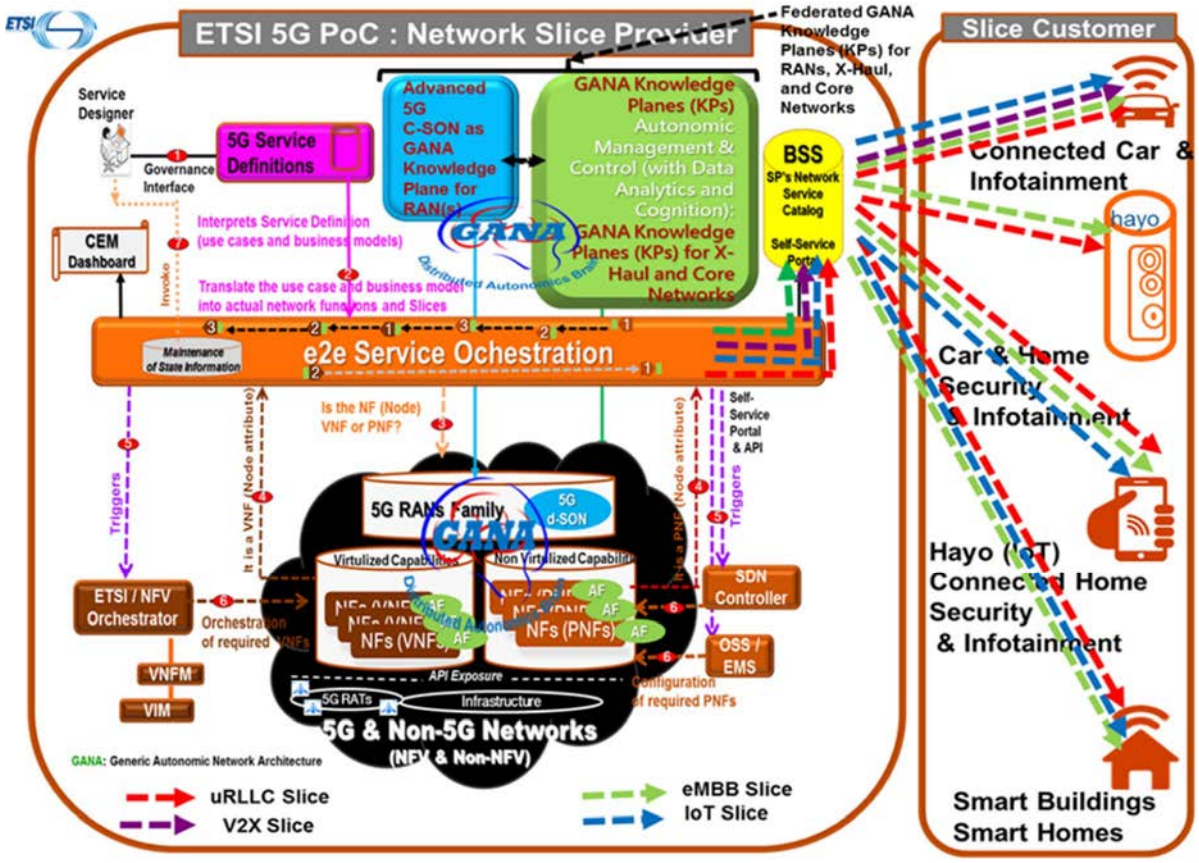

Figure 16: 5G Network Slices Creation and E2E orchestration with ETSI GANA AMC

GANA described architectural frameworks e, g. C-SON as GANA KP for RAN.

While leveraging GANA Autonomics and demonstrating different capabilities of various stakeholders in this discourse, ETSI Proof of Concept (PoC) series instrument within TC INT AFI in different show-cases (PoC series instances) as outlined below:

- **ETSI PoC Demo Instance No.1:** Autonomic Service Assurance for IoT in Smart Insurance and related use-cases. Through closed-loop automation, assuring and guaranteeing service QoS, SLA, and KPI requirements to be maintained and eventually monetized, thanks to GANA Autonomics, and demonstrating the feasibility of the use-case selected and the gained leverage were fully achieved objectives.

- **ETSI PoC Demo Instance No.2:** C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA KPs. The alignment and compatibility of the GANA Autonomics framework and model with Hybrid SON (H-SON) which is a key technology used and endorsed in 3GPP shows a high-potential SDO alignment and synergy showcased in the PoC.

- **ETSI PoC Demo Instance No.3:** Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the ETSI GANA KP for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV/Clouds.

- **ETSI PoC Demo Instance No.4:** Generic Framework for Multi-Domain Federated ETSI GANA KPs for E2E ASMC for 5G Slices, Networks/Services.

- **ETSI PoC Demo Instance 5 (in preparation):** ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for AMC of Networks and Services; and Intent-Based Networking (IBN) via GANA KPs and Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive DEs via a Generic Test Framework for Testing GANA Multi-Layer Autonomics and their AI Algorithms for Closed-Loop Network Automation.

A detailed list of documents, whitepapers, and PoC descriptions can be found at https://intwiki.etsi.org/index.php?title=Accepted_PoC_proposals.

ETSI TR 103 747 [i.78] presents a framework for end-to-end autonomic (closed-loop) service assurance of network 5G slices services using the federation of MDKP across various segments, including RAN (C-SON), front-/backhaul, and core network, complemented by lower-level autonomics in NE/NF. The document describes different federation options for MDKP, such as horizontal federation of KP platforms within a single organization, and hierarchical/vertical federation scenarios, both within a single organization and across multiple organizations.

11 Conclusion and Further Work

The present document has presented the Generic Framework for E2E Federated GANA KPs for AI/ML-powered ASMC Across Multi-Domain 5G Networks. Clause 4 provided the foundation for such a Framework. The main scope of the Framework being on security challenges that can be addressed through Closed-Loop Automated and ASMC in 5G by the two "mirror" GANA Security Management DEs implemented at two levels within the GANA reference model, namely the Security Management DE at the GANA KP level (within a GANA KP for a specific network segment/domain) and a Security Management DE implemented at GANA level 3 (i.e. within a certain NE/NF). The subsequent clauses that follow clause 4 of the present document provide additional perspectives for consideration as part of the Framework presented by the present document.

In some way the present document has provided useful insights to implementers and solution suppliers for ETSI GANA KP platforms for AMC of specific 5G network segments such as Radio Access Network (RAN), X-Haul Transport and Core Network, as well as to implementers of the GANA Security Management DEs discussed in the present document. As such the Framework presented in the present document is implementable as illustrated in clause 10 of the present document and in ETSI TR 103 747 [i.78], thanks to the PoCs that have been implemented on GANA KP Platforms and federation techniques.

The Framework presented in the present document aligns well with emerging trends in network disaggregation in the infrastructure layer and in the management and orchestration and control layer as well, and the framework adopts and aligns with approaches covered in other groups such as:

- Requirements for Autonomic Networking and AMC in NGMN E2E 5G Architecture [i.10]. The ETSI GANA Model and its concept of the GANA KP as a platform for implementing AMC were adopted by NGMN deriving specification of Requirements for Autonomic Networking and AMC in the NGMN 5G E2E Architecture [i.10].

- Work from NIST MDKP for Service Federation for 5G and Beyond Public Working Group (MDKP-PWG) [i.61].

- NGMN and ETSI TC INT AFI WG synergy and common view on the fact that KP Platforms for AMC need to be disaggregated, meaning that KP Platforms should designed and implemented for specific network segments as domains (e.g. RAN, X-Haul Transport, Core Network). Both NGMN and ETSI TC INT AFI WG are in agreement that E2E ASMC in 5G is to be achievable by way of Federation of the Network-Level Security-Management-DEs across multiple network segments/domains (RAN, X-Haul Transport, Core Network), following the principles for federated AMC outlined in the NGMN 5G E2E Architecture Framework [i.10]. According to the NGMN E2E 5G Architecture [i.10], E2E Autonomic (Closed-Loop) service assurance should be achievable through a federation of KPs that implement components for AMC intelligence for specific network segments (viewed as domains). There are many advantages to implementing disaggregated KP Platforms. For example, the ICT infrastructure for a specific network segment may be supplied to a CSP (or even to an enterprise's network(s) environment) by a supplier that should not necessarily be the supplier of the autonomics software or (autonomic-) management and control platforms for the network segment (infrastructure). And also, a CSP or an enterprise may desire to have Solutions suppliers for Autonomics software (e.g. GANA DEs), AMC Platforms like KP Platforms or Management and Control Systems for specific ICT network segments to not be the same supplier for all the network segments or the underlying infrastructures-for various reasons (e.g. to allow for competitive solutions sourcing). This way, disaggregation avoids the problems of "vendor-lockin" for a CSP or enterprise and it also enables for competition and innovations among solution suppliers. Unlike the approaches being taken in 3GPP on analytics platforms that do not follow disaggregation approaches.

Annex A: Bibliography

- International Business Machines White paper: "An architectural blueprint for autonomic computing: MAPE-K", June 2005.
- N. Miloslavskaya, A. Tolstoy: "Big Data, Fast Data and Data Lake Concepts", Elsevier Procedia Computer Science, Vol. 88, pp. 300-305, October 2016.
- ETSI PoC#1: "5G Network Slices Creation, Autonomic and Cognitive Management and E2E Orchestration-with Closed-Loop (Autonomic) Service Assurance for the IoT (Smart Insurance) Use Case".
- ONAP Open Source Project: "ONAP Architecture Overview".
- BBF CloudCO Open Source Project.
- OpenDayLight Open Source Project.
- ETSI OSM (Open Source MANO).
- ETSI TS 129 520 (V16.6.0): "5G; 5G System; Network Data Analytics Services; Stage 3 (3GPP TS 29.520 version 16.6.0 Release 16)".
- ETSI TS 128 533 (V15.0.0): "5G; Management and orchestration; Architecture framework (3GPP TS 28.533 version 15.0.0 Release 15)".
- ETSI GS AFI 002 (V1.1.1): "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture (An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management)".
- Cisco White Paper: "Network as a Security Sensor White Paper", October 26, 2018.
- ETSI TC INT / AFI WG 5G PoC Demo#4: "End-to-End Autonomic (Closed-Loop) Security Management and Control for 5G Networks".

Annex B:
Change history

Date	Version	Information about changes
July 2021	V0.0.1	First version compiled from the content of the ETSI TC INT / AFI WG 5G PoC White Paper No.6 and Slides from the Webinar given by the TC INT / AFI WG 5G PoC Project in December 2020 (Webinar https://intwiki.etsi.org/images/Webinar_Demo4_V1.41.pdf [i.48])
September 2022	V0.0.2	Stable Draft
November 2023	V0.0.3	Version for TB Approval

History

Version	Date	Status
V1.1.1	July 2026	Publication