Draft ETSI TR 103 404 V0.0.5 (2016-03)

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

Reference
<Workitem>

Keywords
<keywords>

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 – NAF 742 C
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

This Technical Report (TR) has been produced by {ETSI Technical Committee NTECH} <long techbody> (<short techbody>).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

1 Scope

The present document covers the Instantiation of the Reference Model for Autonomic Networking, Cognition and Self-Management onto the architecture defined in ETSI TS 123 401 and TS 123 402, by superimposing GANA Decision Elements (DEs) into node/device architectures and the overall network architecture, so that the DEs and their associated Control-Loops can be further designed to perform autonomic management and control of the specific resources (Managed Entities) in the target architecture. Recommendations on the basic behaviours of the GANA Functional Blocks (FBs) in the above context will be developed. 3GPP specifications on policy control (TS 123 203) and network management will be taken into account (TS 123 32x series).

2 References

2.1 Normative references

Not applicable.

2.2 Informative references

[i.1] 3GPP TS 23.002 Network architecture

[i.2] 3GPP TS 23.401 General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access

[i.3] 3GPP TS 23.203 Policy and charging control architecture

[i.4] 3GPP TS 32.501 Telecommunication management; Self-configuration of network elements; Concepts and requirements

[i.5] 3GPP TS 32.541 Self-healing Concepts and Requirements

[i.6] ETSI NTECH AFI White Paper (draft); The GANA (Generic Autonomic Networking Architecture) Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services

[i.7] ETSI TR (draft) Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity-enabled Ad-hoc and Mesh Network Architecture

[i.8] ETSI GS AFI 002 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)

[i.9] Requirement Specification (2008) NGMN Recommendation on SON and O&M Requirements

[i.10] Andrea Fabrizi," NFV self-adaptive networks; Integrate your control plane with analytics", HP Viewpoint paper, July 2015

[i.11] “Industry Harmonization for Unified Standards on Autonomic Management & Control of Networks and Services, SDN, NFV, E2E Orchestration, and Software-oriented enablers for 5G”, Ranganai Chaparadza (Ipv6 Forum & representative in ETSI / NTECH/AFI WG), Tayeb Ben Meriem (ETSI /NTECH/ AFI WG),John Strassner (TMForum ZOOM, ETSI NFV, ONF Architecture and Frameworks), Steven Wright (ETSI NFV ISG) — (also invited: TBC), Joel Halpern (Contributor to IETF)

[i.12] “RAN Evolution Project, Backhaul and Fronthaul Evolution”, by NGMN Alliance, 31-March-2015

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply:

Decision Element: Decision-Making-Elements (DMEs) referred in short as Decision Elements (DEs), each of which is designed and assigned to autonomically manage and control some Managed Entities (Mes) assigned to be managed and controlled by a concrete DE. An ME is a protocol or a mechanism implemented by some functional entity. A Decision Element (DE) implements the logic that drives a control-loop over the “management interfaces” of its assigned Managed Entities (Mes). Therefore, in AFI, self-* functionalities are functionalities implemented by Decision Element(s).

Autonomic networking: What is autonomic networking? It is the ability of systems to be more self-managing. The term autonomic comes from the autonomic nervous system, which controls many organs and muscles in the human body. Usually, we are unaware of its workings because it functions in an involuntary, reflexive manner—for example, we don't notice when our heart beats faster or our blood vessels change size in response to temperature, posture, food intake, stressful experiences and other changes to which we're exposed. And our autonomic nervous system is always working.

Self Configuration: An autonomic application/system should be able to configure and reconfigure itself under varying and unpredictable conditions.

Self Organizing: A self-organising function in network includes processes which require minimum manual intervention**.**

Self Optimisation: An autonomic application/system should be able to detect suboptimal behaviors and optimize itself to improve its execution

Self-monitoring: The ability of a component or system to observe its internal state, for example, including such quality-of-service metrics as reliability, precision, rapidity, or throughput.

Self-regulation: The ability of a component or system to regulate its internal parameters so as to assure a quality-of-service metric such as reliability, precision, rapidity, or throughput.

Self-descriptive: The ability of a component or system to provide a description of its self-model, capabilities and internal state.

Self healing: An autonomic application/system should be able to detect and recover from potential problems and continue to function smoothly

Self Protecting: An autonomic application/system should be capable of detecting and protecting its resources from both internal and external attack and maintaining overall system security and integrity

Self-advertise: An autonomic entity should be able to advertise its self-model, capability description model, or some information signalling message (such as Ipv6 routing advertisement) to the network in order to allow communication with it or to allow other entities to know whatever is being advertised.

Self Awareness: An autonomic application/system "knows itself" and is aware of its state and its behaviours. Knowledge about "self" is described by a "self-model".

Context Aware: An autonomic application/system should be aware of its execution environment and be able to react to changes in the environment.

Overlay: A logical network that runs on top of another network. For example, peer-to-peer networks are overlay networks on the Internet. They use their own addressing system for determining how files are distributed and accessed, which provides a layer on top of the Internet's IP addressing.

Autonomic Behaviour : Autonomic function desired element's behaviour in order to learn, influence, or changed on how it turns its affect on other elements or groups of element or network.

Management entities: Mes can be protocols, whole protocol stacks, and mechanisms

3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

<1st symbol> → *[tab]*<1st Explanation> *(style EW)*
<2nd symbol> → *[tab]*<2nd Explanation> *(style EW)*
<3rd symbol> → *[tab]*<3rd Explanation> *(style EX)*

3.3 Abbreviations

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

AF	Autonomic Function
CEP	Complex Event Processing
DE	Decision Element
DHCP	Dynamic Host Configuration Protocol
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GANA	Generic Autonomic Network Architecture
IETF	Internet Engineering Task Force

Ipv4	Internet Protocol version 4
Ipv6	Internet Protocol version 6
ME	Managed Entity
MME	Mobility Management Entity
MPLS	Multi-Protocol Label Switching
NE	Network Element
OCS	Online Charging System
OFCS	Offline Charging System
OSPF	Open Shortest Path First
P GW	PDN Gateway
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
RCAF	RAN Congestion Awareness Function
S GW	Serving Gateway
TcoSH	Trigger Condition of Self-Healing
TCP	Transfer Control Protocol

4 Background

Autonomic Networking & Services Management is intended to help operators and enterprises in reducing OPEX and handling the increasing complexity of network Management. The ETSI AFI WG of TC NTECH produces specifications for the Autonomic Networking & Services Management, namely the Generic Autonomic Network Architecture (GANA). The TC is now progressing in producing technical reports on instantiation of the GANA Reference Model onto existing network architectures and emerging ones to embed self-management capabilities.

The objective of the present work is to develop a Technical Report on the instantiation of the GANA model on the mobile backhaul and the Evolved Packet Core (EPC) deployed as per 3GPP Architecture specifications.

The work has been divided into several tasks which are reflected in the following clauses. The first task consisted in defining the 3GPP reference architecture. This is reported in Clause 5. In a second step, a mapping of the GANA model to the 3GPP architecture was defined for a basic scenario with the 3GPP EPC and the mobile backhaul networks as standalone networks. This is reported in Clause 6. The final task consists in considering autonomic behaviours across multiple segments. This [will be] reported in clause 7.

5 Reference scenario

5.1 Reference architecture

The identification of a reference architecture for the 3GPP LTE Core Network is important in order to have a consolidated basis for the instantiation of the GANA DEs. Moreover, the consideration of the mapping of the GANA model and Knowledge plane onto this reference architecture should encompass the relevant layers and respective functionalities. Following the previous assumptions, the reference architecture is depicted in Figure 1, where the main functional and network entities of the EPC and PCC are depicted. In this figure the control plane and data plane interactions are highlighted and for completeness, the respective access network entities (which are not in scope of this work) are marked in grey. The PCRF and PCEF are the nodes and functional entities that have direct relation with the operator policies in a 3GPP network and therefore it is important to follow through the reference architecture the evolution of the knowledge and policy management after the mapping of the GANA related knowledge plane and control loops.

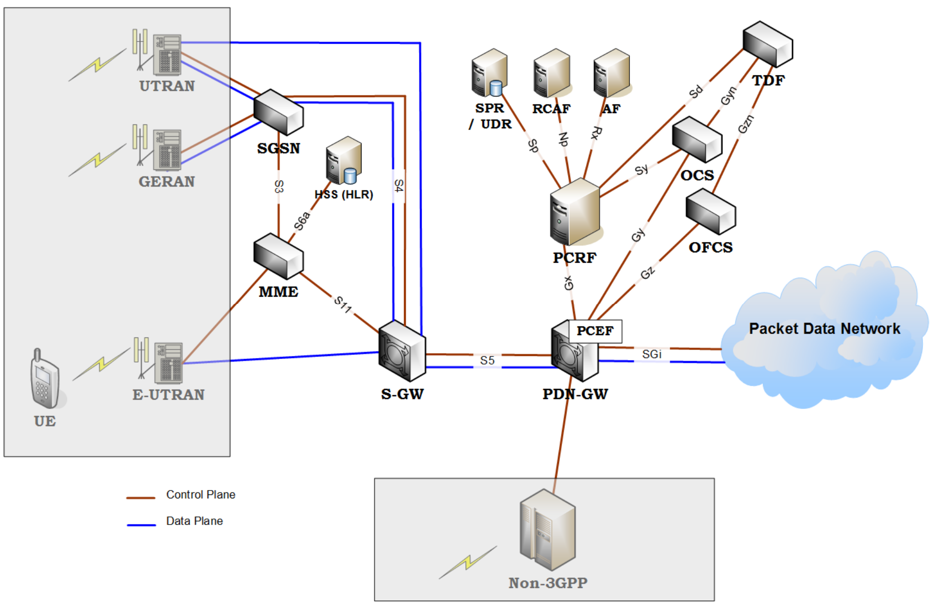

Figure 1 Reference 3GPP architecture

In Figure 2, the 3GPP Core Network reference architecture is presented, highlighting the management plane along with the control and data plane providing a more consolidated view of the reference entities and interfaces to be considered during the GANA instantiation. The mapping of GANA model will consider the placement of decision making entities, the coordination of the entities and collaboration of functional blocks, feedback loops and policies. This may affect the 3 different views of the 3GPP CN (control/data/management plane).

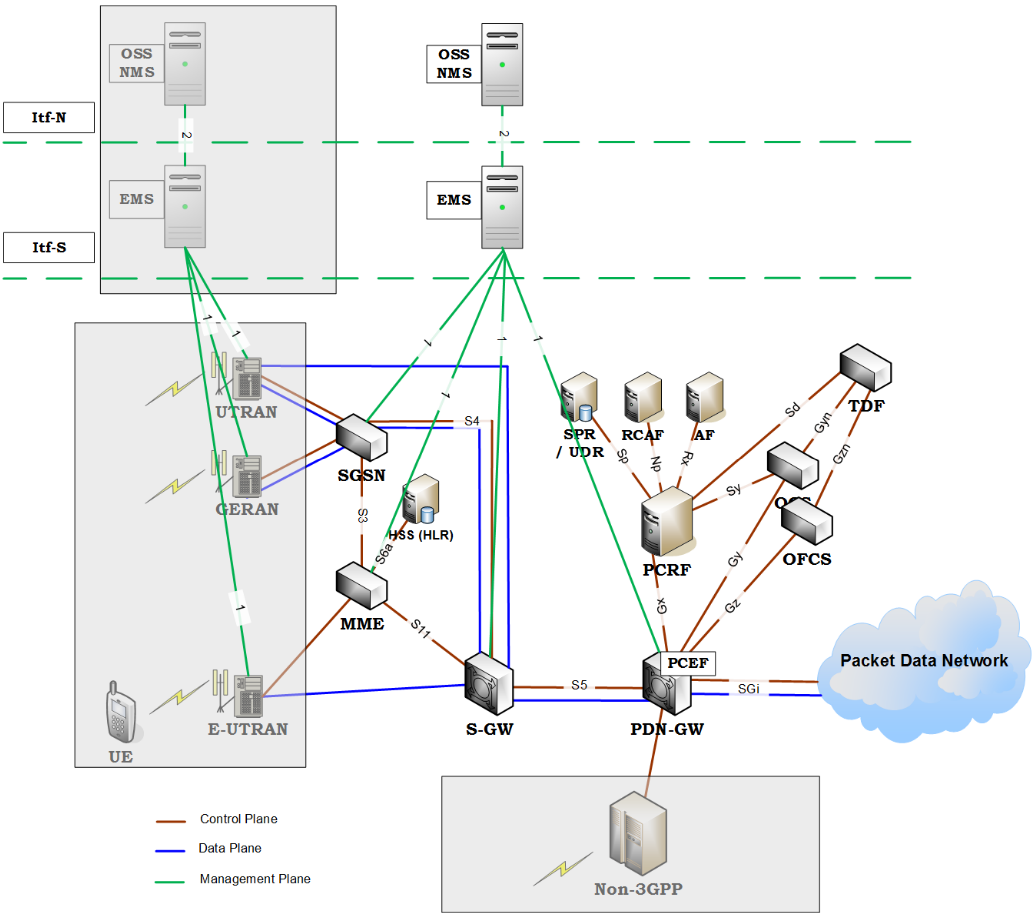

Figure 2: Management plane for the non-aggregated scenario

Figure 3 depicts the assumed reference architecture for the mobile backhaul part of the network. In principle this covers IP/MPLS enabled routers that are typically used for backhauling the traffic from the 3GPP access networks (including controllers in case of earlier releases) to the EPC core. The figure also depicts the systems responsible for the management of the backhaul network in whole and per element.

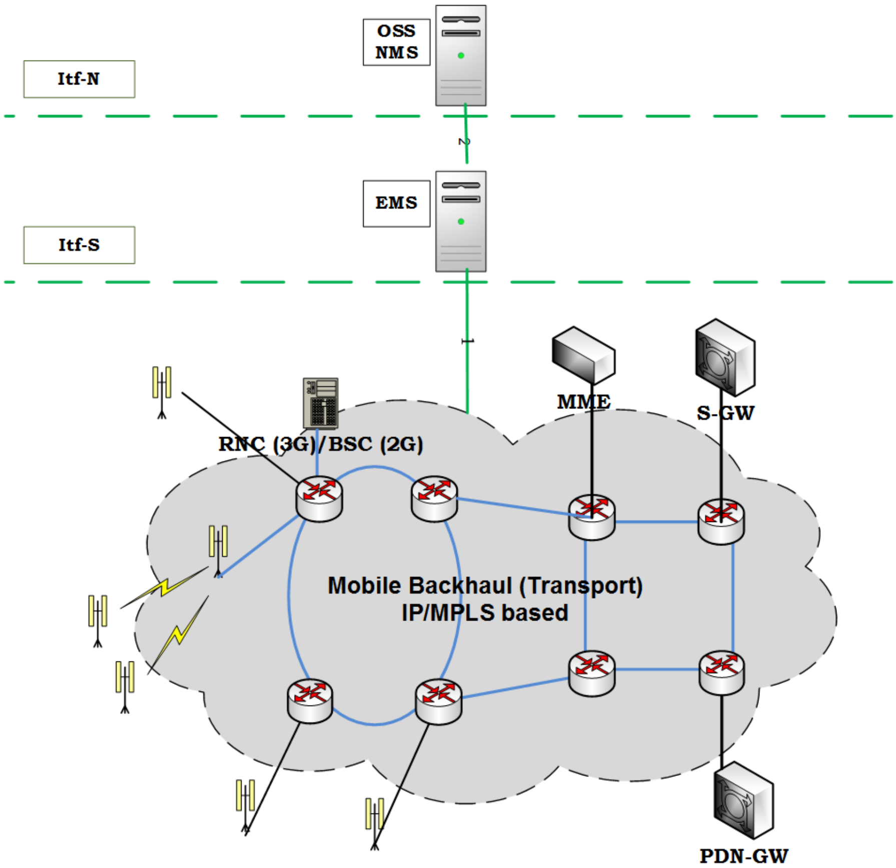

Figure 3: Reference architecture for the backhaul

Current requirements and evolution for the backhaul can be assessed by the efforts depicted in the NGMN evolution report [i.12]. Moreover, other approaches can be addressed, for example self-backhauling for SMARTER, e.g., in recent 3GPP TSG-SA WG1work items.

5.2 Assumptions for the report

5.2.1 Assumptions for the EPC

The EPC includes an extensive number of nodes and functionalities, which cover a large extent of use cases. The remainder of the present report focuses on specific use cases, which comply with the following assumptions.

- 3GPP EPC architecture to consider
  - Non-Roaming: the simplest EPC architecture case
  - Include PCC architecture (PCRF, PCEF)

  Rationale: Considering both the EPC and the PCC architectures provides a good coverage of the main functions to be managed in the Core Network. A simple case of roaming may be considered at a later stage.

- EPC interactions with 2G/3G PS Core nodes
  - Consider 2G, 3G (KP only), 4G (KP + DE)
  - 3PPP RAT mobility + QoS and their impact

Rationale: The report addresses the latest version of MNO networks, i.e. the LTE-Advanced release of 3GPP. However, since 2G and 3G accesses are part of these networks, they have been included in the study, focusing mainly on their possible impact on the Knowledge plane.

- Non-3GPP access (e.g. WLAN)
  - Focus only on the CN (not the AN), impact of non 3GPP Access on the CN (decision placement, interaction / collaboration / coordination b/w DE , policies, …)

  Rationale: Same as for 2G and 3G RAN, the non-3GPP access is included in the study mainly for its impact on the decisions made at the CN level.

- Consider all 3 different views
  - User/Data plane view
  - Control plane view
  - Management plane view

  Rationale: With the objective to be comprehensive, the report considers the three planes that are involved in the operation of a CN.

5.1.2 Assumptions for the backhaul

The backhaul network is responsible for the forwarding of the messages between the different entities of the MNO. It may be constituted of a very varied set of peripheral nodes, operating either at layer 2 or layer 3 (network layer) of the OSI model. The present report focuses on a restricted scenario, the results provided in the next clauses being extendable in a similar fashion to more complex scenarios. This scenario implies the following assumptions:

- Mobile backhaul network based on IP/MPLS enabled (P, PE) routers
- No Convergence Architecture Scenario ("Current Scenario" in NGMN document [i.9])
- With 3 independent components : Access Network, Backhaul, Core Network
- RAN OSS/NMS/EMS only for its impact on the CN Management plane

6 Basic scenario

6.1 Introduction

The present clause aims at identifying the need for instantiating Autonomic Functions (AF) in the EPC and its core Networks Elements (Nes). The analysis below covers the build-up and operation/maintenance phases of the life-cycle of a mobile network, which leave room for simplification through automation, namely:

- SC : Self-Configuration/Commissioning
- SO : Self-Optimization
- SH : Self-Healing

6.2 General considerations

6.2.1 3GPP entities and reference points

In clause 5, the CN reference architecture has been drawn. Table 1 shows the distribution of the basic entities of the backhaul and Core networks that will be taken into consideration for the mapping. For completeness, it additionally shows the entities of the RAN and the external PDN, but they are greyed to indicate that only their impact on the CN is considered.

Table 1 Identification of entities of the Core Network (CN) and backhaul network to be managed

Basic entities			***Service Specific Entities***	***Backhaul***	***Management Plane***	***External PDN entities***
RAN	***GPRS-PS***	***EPC PS***				
e-UTRAN UTRAN GERAN non-3GPP Access UE???	SGSN	MME S-GW P-GW HSS (HLR) EIR	PCEF PCRF OCS OFCS TDF SPR / UDR RCAF AF	IP/MPLS Router (P, PE)	CN-EMS CN-NMS	BG

Table 2 lists the reference points standardized in the 3GPP network architecture [Ref 23.002] that operate at the functional level. These reference points allow visualizing the interactions that take place between the CN entities and their associated functionalities. In the table, they are shown with their 3GPP names, the entities that they connect as well as a short description of the functionalities and mechanisms they provide, with a reference to the 3GPP standard where they are specified.

Table 2 Identification of functional reference points

Name	***Entities***	***Function***
S3	MME and SGSN	Enables user and bearer information exchange for inter 3GPP access network mobility in idle and/or active state [29.274].
S4	S-GW and SGSN	Provides related control and mobility support between GPRS Core and the 3GPP Anchor function of Serving GW. In addition, if Direct Tunnel is not established, it provides the user plane tunnelling [TS 29.274 & TS 29.281].
S5	S-GW and P GW	Provides support for functions for packet data services towards end users [TS 29.274 & TS 29.281].
S6a	MME and HSS	Used to exchange the data related to the location of the mobile station and to the management of the subscriber [TS 29.272].
S6d	SGSN and HSS	Used to exchange the data related to the location of the mobile station and to the management of the subscriber [TS 29.272].
S11	MME and S-GW	Used to support mobility and bearer management between the MME and S-GW [TS 29.274].
Sgi	PDN GW – packet data networks	may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provision of IMS services [29.061]

Table 3 lists the reference points standardized in the 3GPP Policy and charging control (PCC) architecture [Ref 23.203]. They are shown with their 3GPP names, the entities that they connect as well as a short description of the functionalities and mechanisms they provide, with a reference to the 3GPP standard where they are specified.

Table 3 Identification of PCC reference points

Name	*Entities*	*Function*
Rx	PCRF – AF	allows for dynamic QoS and charging-related service information to be exchanged between the Policy and Charging Rules Function (PCRF) and the Application Function (AF). This information is used by the PCRF for the control of service data flows and IP bearer resources [23.203].
Gx	PCEF – PCRF	Provides transfer of policy and charging rules from PCRF to PCEF in the P-GW [29.212].
Gy	OCS – PCEF	allows for the online charging based on the Diameter credit control application between the Online Charging System (OCS) and the PCEF [32.251 & RFC 4006].
Gyn	OCS – TDF	allows for the online charging based on the Diameter credit control application between the Online Charging System (OCS) and the TDF [32.251].
Gz	OFCS – PCEF	allows for the offline charging based on the charging record data transfer between the Offline Charging System (OFCS) and the PCEF [32.295].
Gzn	OFCS – TDF	allows for the offline charging based on the charging record data transfer between the Offline Charging System (OFCS) and the TDF [32.295].
Np	RCAF – PCRF	enables transport of RAN User Plane Congestion Information sent from the RCAF to the PCRF [23.203].
Sp	SPR – PCRF	allows for the PCRF to request subscription information from the SPR and the SPR to notify the PCRF when the subscription information has changed if the PCRF has requested such notifications [N/A].
Sd	TDF – PCRF	enables a PCRF to have dynamic control over the application detection and control behaviour at a TDF [29.212].
Sy	OCS – PCRF	enables transfer of information relating to subscriber spending from OCS to PCRF [29.219].

Table 4 lists the management plane interfaces identified in the 3GPP Telecommunication Management Architecture [Ref 32.102] that operate on top of the Core Network. They are shown with their 3GPP names, the entities that they connect as well as a short description of the functionalities and mechanisms they provide.

Table 4 Identification of Management plane interfaces

Name	*Entities*	*Function*
Type 1	NE – EM	allows the use of certain management application layer protocols [CORBA IIOP, NETCONF, SNMP, SOAP]
Type 2 (Itf-N)	EM – NM	used by the network and service management systems to transfer messages, notifications and service management requests via the EM to the NE.

6.3 Self-Configuration/Commissioning

6.3.1 General Description and use cases

The tasks involved in the self-configuration cover the initial and final life cycle of the Network Elements (Nes), as well as the specific cases of updates and upgrades of these Nes. Firstly, these operations manage the dynamic set-up of newly installed Nes from the point of view of their internal pieces of executable programs (software and firmware), and their functional insertion in the network. At the end of the self-Configuration, the NE is able to execute all its planned duties in the network. Secondly, they manage the dynamic update, upgrade or the removal of the NE from the network. Finally, the self-configuration also covers the storage of the configuration data locally in the NE (as described in 3GPP TS 23.401 [i.2], section 5.7) and/or in the management plane.

The list of protocols and mechanisms involved in these tasks depend on the type of the NE and are presented in the sections below.

The subsequent clauses focus on the addition of a ME in the mobile operator network and its initial setup. The other operations, such as deletion, update and upgrade are covered indirectly as the mapping to the GANA DEs would apply in a similar manner in these cases.

6.3.2 Protocol-level entities (GANA Level 1) to be managed

Table 5 shows the operations related to the self-Configuration use case and identifies the entities of the CN and the backhaul network to which they apply. These operations are mainly related to the installation of a new node or a new function in a server and to the recording of configuration data in the node and in the management entities storage.

Table 5 Configuration-related use cases for the mapping

Use cases	Operation	Network Entity								
		IP/MPLS Router	MME	SGSN	S-GW	P-GW	HSS / IER	PCRF	TDF	OCS
Node / function installation in the system	Addition/ deletion/ update/upgrade	*	*		*	*	*	*	*	*
Knowledge information storage	Store the configuration data of the node		*	*	*	*	*			

Some examples of the various protocols and mechanisms involved in the operation of self-configuration are described below, classified into a smaller set of generic high-level mechanisms. Examples of these mechanisms are given in the mapping tables of section 6.3.4.

- Network Protocols Configuration
    - For the configuration of backhaul routers: subnets definition, configuration of routing protocols, routing table convergence.
    - For the allocation of IP address and/or port number: DHCP server discovery, IP address and default gateway acquisition, Ipv6 Neighbour Discovery, TCP/UDP port number allocation and discovery.
- Security
    - Access control mechanisms, certificate passwords mechanisms, encryption key dissemination mechanisms.
- Connectivity
    - To management plane entities: OAM sub-system discovery (IP address and port number, network management protocol).
    - To neighbouring entities: TCP/IP protocols, layer 2 protocols, physical layer protocols.
- Firmware and Software Management
    - Software update and dissemination mechanisms, firmware update and dissemination mechanisms.
- CN Functional Configuration
    - Parameters required for the operation of the CN protocols, e.g. S1-AP, GTP-C, GTP-U, and Diameter applications. Examples of such parameters are user profiles, weight factors, APN …
- Configuration Information Storage
    - Network management configuration data collection mechanisms, inventory systems mechanisms

6.3.3 Identification of GANA DEs for self-configuration

The present clause lists the GANA DEs that orchestrate the autonomicity for the self-configuration use case. This list has been built using figure 17 and Table 1 of ETSI GS AFI 002 [***i.8***] as a reference. Each DE is explained with the type of Managed Entities under its control as of the GANA architecture.

<u>Function level DEs</u>

- Mobility-Management-DE [FUNC_LEVEL_MOM_DE] – Typical Mes are mobility management mechanisms and protocols.
- Service-Management-DE [FUNC_LEVEL_SM_DE] – Typical Mes are services and applications.
- Routing-Management-DE [FUNC_LEVEL_RM_DE] – Typical Mes are routing protocols and mechanisms.
- Generalized-Control-Plane-DE [FUNC_LEVEL_GCP_M_DE] – Typical Mes are the other control plane protocols operating at function level.

Node level DEs

- AutoDiscoveryAndAutoConfiguration-DE [NODE_LEVEL_AC_DE] – Typical Mes are discovery protocols and mechanisms for the neighbours and the network.
- Security-Management-DE [NODE_LEVEL_SEC_M_DE] – Typical Mes are security protocols, algorithms and mechanisms operating at node level.
- Resilience-and-Survivability-DE [NODE_LEVEL_RS_DE] – Typical Mes are proactive and resilience mechanisms or restoration and protection mechanisms.

Network level DEs

- AutoDiscoveryAndAutoConfiguration-DE [NET_LEVEL_AC_DE] – Typical Mes are discovery protocols and mechanisms operating at network level.
- Mobility-Management-DE [NET_LEVEL_MOM_DE] – Typical Mes are mobility management mechanisms and protocols running at network level.
- Security-Management-DE [NET_LEVEL_SEC_M_DE] – Typical Mes are security protocols, algorithms and mechanisms operating at network level.
- Resilience-and-Survivability-DE [NET_LEVEL_RS_DE] – Typical Mes are proactive and resilience mechanisms or restoration and protection mechanisms running at network level.

6.3.4 Mapping of self-configuration functions

6.3.4.1 MME

The present clause and the following ones introduce a mapping of some specific protocols and mechanisms in the case of the addition of a node or a function, which is a typical case for self-configuration. They define this mapping for these three different types of Nes: a node (e.g., the MME), a function installed in a pre-configured server (e.g. the HSS) and a backhaul router.

Table 6 provides a one to one mapping between the instantiated DEs and the managed protocols and mechanisms for self-Configuration in the case of an MME NE. The MME involves node mechanisms as well as several embedded functions, so this is the most complex example of mapping for the self-configuration operation. The same would apply to an S-GW or a P-GW for example

Table 6 Mapping table for the MME

Network-Level DEs	Node-Level DEs	Function Level DEs	Protocols & Mechanisms	Examples
NET_LEVEL_RS_DE NET_LEVEL_SEC_M_DE NET_LEVEL_AC_DE NET_LEVEL_MOM_DE	NODE_LEVEL_SEC_M_DE		Authentication of entity	Access control mechanisms, certificate passwords mechanisms, encryption key dissemination mechanisms.
	NODE_LEVEL_AC_DE		Allocation of its own IP address and port number	DHCP server discovery, IP address and default gateway acquisition, Ipv6 Neighbour Discovery, TCP/UDP port number discovery and allocation
		FUNC_LEVEL_MOM_DE	Connectivity to management plane entities	OAM sub-system discovery (IP address and port number, network management protocol)
	NODE_LEVEL_RS_DE		Firmware and software levels management	software update and dissemination mechanisms, firmware update and dissemination mechanisms
		FUNC_LEVEL_SM_DE	Functional configuration in the CN	MME parameters configuration, e.g. weight factor for MME pooling (see section 6.4.5.3)
		FUNC_LEVEL_MOM_DE	Connectivity to neighbouring entities: E-UTRAN, SGSN, HSS, S-GW	Activation of the links underlying the Core Network protocols
		FUNC_LEVEL_GCP_DE	Activation of the CN protocols with neighbour entities	S1-AP, GTP-C, and Diameter applications
		FUNC_LEVEL_SM_DE	Upload of configuration information in the management plane entities (e.g., MIB)	Network management configuration data collection mechanisms, inventory systems mechanisms

Figure 4 illustrates the mapping in the case of an MME NE. The figure shows the three lower levels of the GANA model that may be instantiated in a NE. In the case of the MME, the DEs are complemented with a local information/knowledge repository that stores the information necessary to the operation of the node [i.2]. The grey-scale components represent the inactive components.

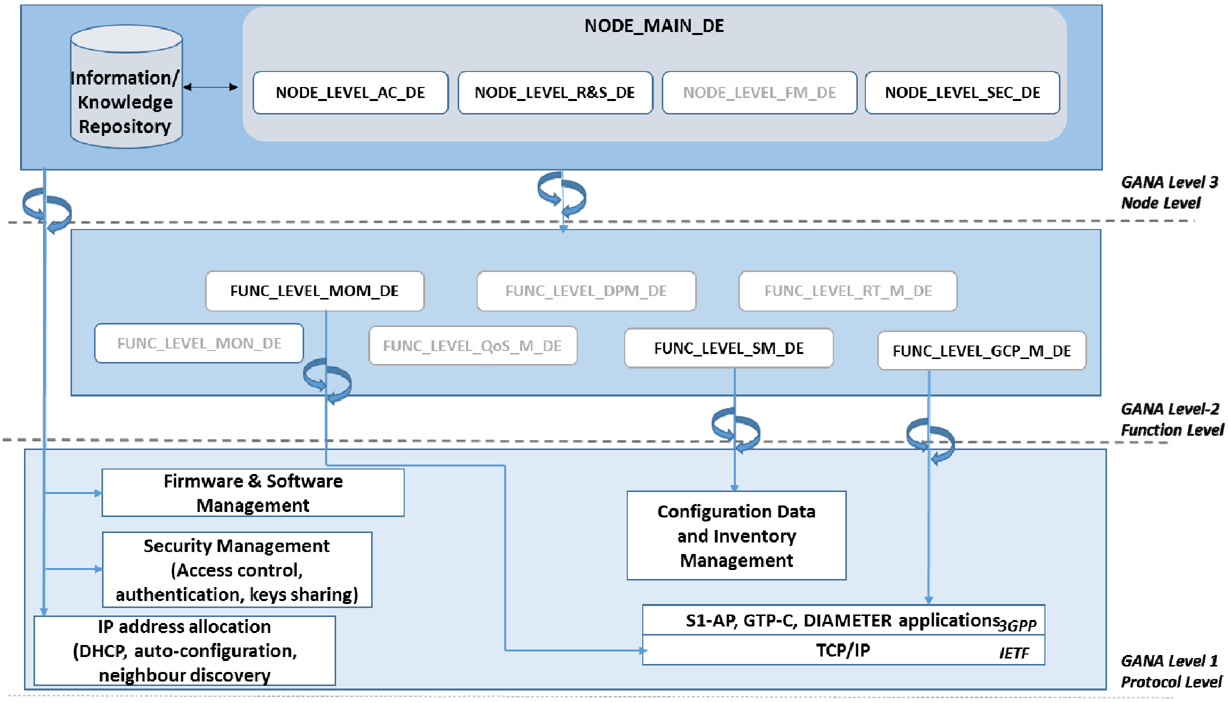

Figure 4: Node level view of self-Configuration case for the MME

6.3.4.2 HSS

Table 7 provides a one to one mapping between the instantiated DEs and the managed protocols and mechanisms for self-Configuration in the case of an HSS NE installed in a pre-configured server. The HSS involves only embedded software functionalities; so in this case, the mapping does not need to address the node configuration mechanisms and protocols.

Table 7 Mapping table for the HSS

9	Node-Level DEs	Function Level DEs	Protocols & Mechanisms	Examples
NET_LEVEL_RS_DE NET_LEVEL_SEC_M_DE NET_LEVEL_AC_DE NET_LEVEL_MOM_DE	NODE_LEVEL_SEC_M_DE		Authentication of HSS entity	Certificate passwords mechanisms,
	NODE_LEVEL_AC_DE		Allocation of port number	TCP/UDP port number discovery and allocation
		FUNC_LEVEL_MOM_DE	Connectivity to management plane entities	OAM sub-system discovery (IP address and port number, network management protocol)
	NODE_LEVEL_RS_DE		Software levels management	software update and dissemination mechanisms, firmware update and dissemination mechanisms
		FUNC_LEVEL_SM_DE	Functional configuration of the CN parameters	Upload of user profiles, Diameter server setup
		FUNC_LEVEL_MOM_DE	Connectivity to neighbouring entities: MME	SCTP
		FUNC_LEVEL_GCP_DE	CN protocols activation	S6a/S6d application initiation
		FUNC_LEVEL_SM_DE	Upload of configuration information in the	Network management configuration data collection

			management plane entities (e.g., MIB)	mechanisms, inventory systems mechanisms

Figure 5 illustrates the mapping in the case of the HSS NE.

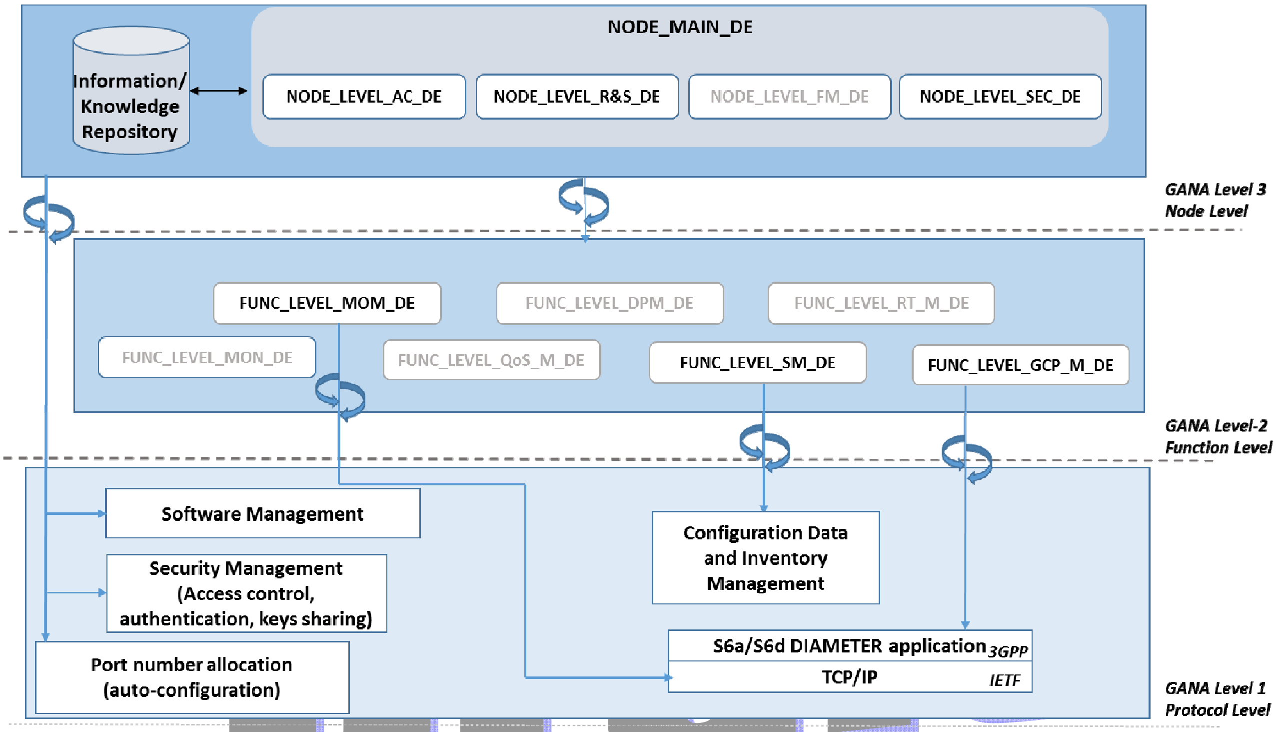

Figure 5 Node level view of self-Configuration case for the HSS

6.3.4.3 IP/MPLS router

Table 8 provides a one to one mapping between the instantiated DEs and the managed protocols and mechanisms for self-Configuration in the case of a backhaul router NE. The specificity in this case lies in the fact that the backhaul router acts only as a transport level node. It is not directly involved in the functional operation of the 3GPP Core Network, which restricts the configuration to be executed to the establishment of the node and of the routing protocols.

Table 8 Mapping table for a router of the backhaul network

Network-Level DEs	Node-Level DEs	Function Level DEs	Protocols & Mechanisms	Examples
NET_LEVEL_RS_DE NET_LEVEL_SEC_M_DE NET_LEVEL_AC_DE		FUNC_LEVEL_RT_M_DE	Configuration of backhaul routers	Subnets definition, configuration of routing protocols, routing table convergence
	NODE_LEVEL_SEC_M_DE		Authentication of entity (CN node/ function)	Access control mechanisms, certificate passwords mechanisms, encryption key dissemination mechanisms
	NODE_LEVEL_AC_DE		Allocation of IP address and/or port number	IP address acquisition
	NODE_LEVEL_RS_DE		Firmware and software levels management	software update and dissemination mechanisms, firmware update and dissemination mechanisms

Figure 6 illustrates the mapping in the case of an IP/MPLS router NE.

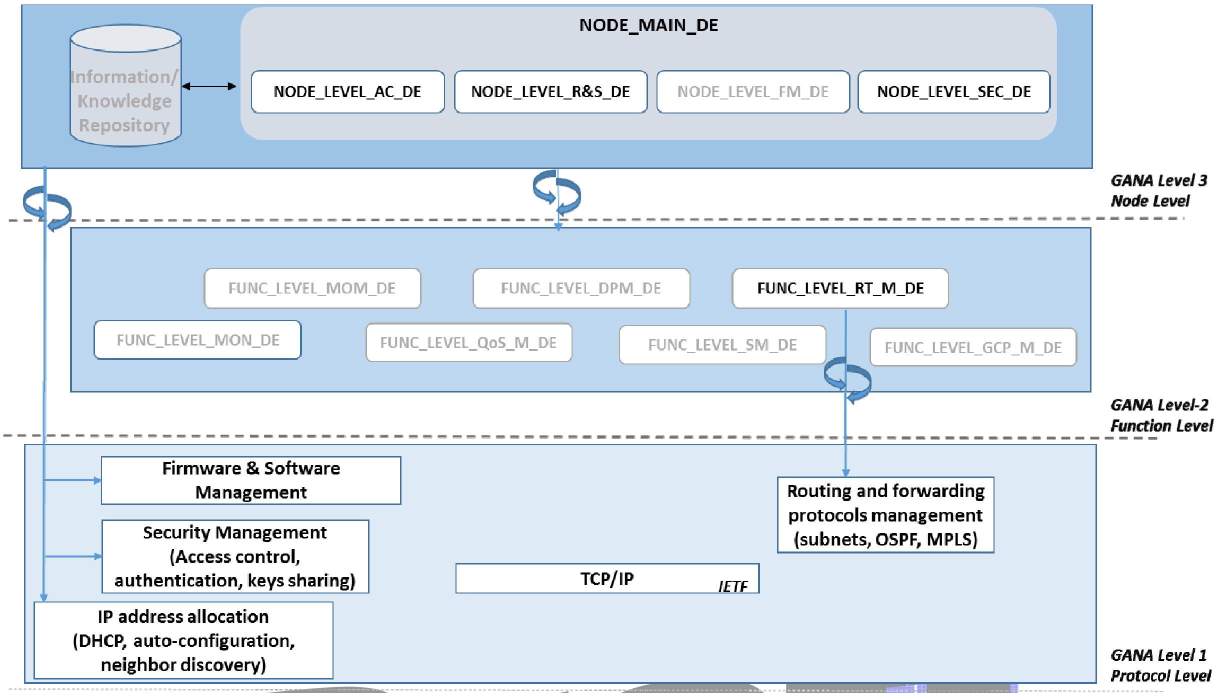

Figure 6: Node level view of self-Configuration case for a router of the backhaul network

6.4 Self-Optimization

6.4.1 General Description and use cases

The initial network configuration is typically made based on assumptions that deviate from the live operation. Changes in traffic volume and behaviour in time and space, newly deployed elements and other environmental variations render the initially configured parameters suboptimal, thus deteriorating network performance. Self-optimization caters for mechanisms that rely on measurements from the operating network in order to provide a much more accurate picture of the real conditions and reveal probable problems, which could not have been predicted under the initial assumptions, whereas they decide for actions that adapt the parameters in order to track those changes and eventually improve the performance of the network.

6.4.2 Protocol-level entities (GANA Level 1) to be managed

The present clause lists examples of mechanisms and protocols that can be seen as protocol-level entities (GANA Level-1 entities) to be managed by GANA DEs for (self-)optimization purposes Examples of these mechanisms are given in the mapping tables of section 6.4.4.

- Mobility Management related:
  - management of Tracking areas and of the reachability of Ues in the mobile service area
  - mechanisms for supporting the mobility (handovers) among eNodeBs and among different 3GPP networks e.g. among 3G and 4G.
- Network Management (O&M) related:
  - Mechanisms are there to support O&M functions related to the EPS such as MME pooling management, Node Load (Re)Balancing, Offloading, Overload control
- Selection related

  - Mechanisms for selection and reselection of the network elements (e.g. MME, P-GW, S-GW, SGSN) that will constitute the network path which can optimally serve the Ues

- QoS related
  - Mechanisms that deal with the management (activation, medication, release) of bearers i.e. the main model for enabling QoS provisioning and differentiated treatment of traffic in the EPC
  - QoS decision policies and QoS enforcement actions taken into elements in terms of filtering, marking, shaping, gating control etc.
  - Charging decision policies and enforcement
- Energy savings
  - Mechanisms for lowering the network element power consumption when for example traffic is lower e.g. by shutting down certain CPUs, interfaces
- Monitoring protocols, mechanisms and tools
  - Mechanisms and tools associated with monitoring of load/traffic behaviour in the network elements
  - Accounting e.g. for charging
  - DPI, analytics

6.4.3 Identification of GANA DEs for self-optimization

The present clause lists the GANA DEs that orchestrate the autonomicity for the self-optimization use case. This list has been built using figure 17 and Table 1 of ETSI GS AFI 002 [***i.8***] as a reference. Each DE is explained with the type of Managed Entities under its control as of the GANA architecture.

Function level DEs

- Mobility-Management-DE [FUNC_LEVEL_MOM_DE] – Typical Mes are mobility management mechanisms and protocols.
- QoS-Management-DE [FUNC_LEVEL_QoS_M_DE] – Typical Mes are mechanisms and protocols associated with the QoS control and provisioning.
- Monitoring-DE [FUNC_LEVEL_MON _DE] – Typical Mes are mechanisms, protocols and tools for monitoring the status of the elements e.g. in terms of signalling/user load, CPU usage etc.

Node level DEs

- AutoDiscoveryAndAutoConfiguration-DE [NODE_LEVEL_AC_DE] – Typical Mes are mechanisms for the selection of other nodes e.g GWs, for OAM related mechanisms such as load balancing, or for saving energy at node level.

Network level DEs

- Mobility-Management-DE [NET_LEVEL_MOM_DE] – Typical Mes are mobility management mechanisms and protocols running at network level.
- QoS-Management-DE [FUNC_LEVEL_QoS_M_DE] – Typical Mes are mechanisms and protocols associated with the QoS control and provisioning at the network level
- Monitoring-DE [FUNC_LEVEL_MON _DE] – Typical Mes are mechanisms, protocols and tools for monitoring the status of the network e.g. in terms of signalling/user load in all the interfaces

6.4.4 Mapping of self-optimization functions

6.4.4.1 MME

Table 9 provides a one to one mapping between the instantiated DEs and the managed protocols and mechanisms for self-optimization in the case of MME NE. As expected, there exist plenty of mechanisms and protocols within MME which are associated with mobility management i.e. the main function that an MME typically offers. Inherently, these could be assigned to FUNC_LEVEL_MOM_DEs, being responsible for Mobility Management. However, decisions such as the ones made e.g. for selection of nodes for achieving load balancing etc. could be also assigned to Node Level DEs (NODE_LEVEL_ AC_DE), since the managed mechanism affects the behaviour of the node (MME) as a whole.

Table 9 Mapping table for MME (control plane)

Network-Level DEs	Node-Level DEs	Function Level DEs	Protocols & Mechanisms	Examples
NET_LEVEL_MOM_DE NET_LEVEL_QoS_M_DE NET_LEVEL_SM_DE NET_LEVEL_MON_DE		FUNC_LEVEL_MOM_DE	Mobility Management protocols & mechanisms	Reachability, Tracking Area list management, Inter CN node signalling for mobility between 3GPP access networks
	NODE_LEVEL_AC_DE	FUNC_LEVEL_MOM_DE	Network Management (O&M) oriented mechanisms	MME pooling management, Load (Re)Balancing, Offloading, Overload control
	NODE_LEVEL_AC_DE	FUNC_LEVEL_MOM_DE	Selection mechanisms	P-GW selection, S-GW selection, MME selection for handovers with MME change, SGSN selection for handovers to 2G or 3G 3GPP access networks
		FUNC_LEVEL_QoS_M_DE	QoS protocols & mechanisms	Bearer management
	NODE_LEVEL_AC_DE		Energy saving mechanisms	Traffic-aware processing power consumption e.g. by shutting down certain CPUs, interfaces
		FUNC_LEVEL_MON_DE	Monitoring protocols, mechanisms and tools	Monitoring of load/traffic, Acccounting, DPI, analytics

6.4.4.2 P-GW

Table 10 Mapping sub-table for P-GW (data plane)

Network-Level DEs	Node-Level DEs	Function Level DEs	Protocols & Mechanisms	Examples
NET_LEVEL_MOM_DE		FUNC_LEVEL_MOM_DE	Mobility	Mobility

NET_LEVEL_QoS_M_DE NET_LEVEL_MON_DE			Management protocols & Mechanisms	anchoring for inter-working with non-3GPP technologies
	NODE_LEVEL_AC_DE		Selection mechanisms	PCRF selection
		FUNC_LEVEL_QoS_M_DE	QoS & Charging Protocols & Mechanisms	Traffic Detection Function, Traffic Shaping, Transport level packet marking in the UL and DL, gating control, Traffic Redirection, Flow based charging support OCS/TDF
		FUNC_LEVEL_MON_DE	Monitoring protocols, mechanisms and tools	Monitoring of load/traffic, Accounting, DPI, Accc analytics
	NODE_LEVEL_AC_DE		Energy saving mechanisms	Traffic-aware processing power consumption e.g. by shutting down certain CPUs, interfaces

6.4.4.3 S-GW

Table 11 Mapping sub-table for S-GW (user plane)

Network-Level DEs	Node-Level DEs	Function Level DEs	Protocols & Mechanisms	Examples
NET_LEVEL_MOM_DE NET_LEVEL_QoS_M_DE NET_LEVEL_MON_DE		FUNC_LEVEL_MOM_DE	Mobility Management protocols & Mechanisms	Mobility anchoring for inter-eNB Handovers (Local), Mobility anchoring for interworking with other 3GPP technologies, packet buffering
		FUNC_LEVEL_QoS_M_DE	QoS & Charging Protocols & Mechanisms	Transport level packet marking in the uplink and the

				downlink, Charging support
		FUNC_LEVEL_MON_DE	Monitoring protocols, mechanisms and tools	Monitoring of load/traffic, DPI, analytics
	NODE_LEVEL_AC_DE		Energy saving mechanisms	Traffic-aware processing power consumption e.g. by shutting down certain CPUs, interfaces

6.4.5 Indicative example of instantiation – MME pooling management

6.4.5.1 General Description

This clause provides an example in order to get into some more details on the instantiation and mapping process described in the previous sub-sections. The example relates to the automated/autonomic management of mobility management entity (MME) pooling in 3GPP EPC networks

6.4.5.2 MME pooling revisiting

The connectivity between Core and Access network part in legacy 2G/3G cellular networks was defined as one to many hierarchical relationship i.e. each core network node connected to its own set of controller in a fixed manner. In Release 5 of 3G/UMTS standard, a feature that allowed for more flexibility in the inter-connection between access and core nodes, thus breaking the usual network hierarchy, was added.

This feature is well known as MME Pooling or S1-Flex (S1 Flexibility). MME pooling defines an MME pool architecture that enables eNBs to access and be served by multiple MMEs, which are grouped in a structure known as a “pool.”

According to TS 23.401[i.2]

- an MME Pool Area is defined as an area within which a UE may be served without need to change the serving MME.
- An MME Pool Area is served by one or more MMEs ("pool of MMEs") in parallel.
- MME Pool Areas are a collection of complete Tracking Areas (Tas).
- MME Pool Areas may overlap each other.

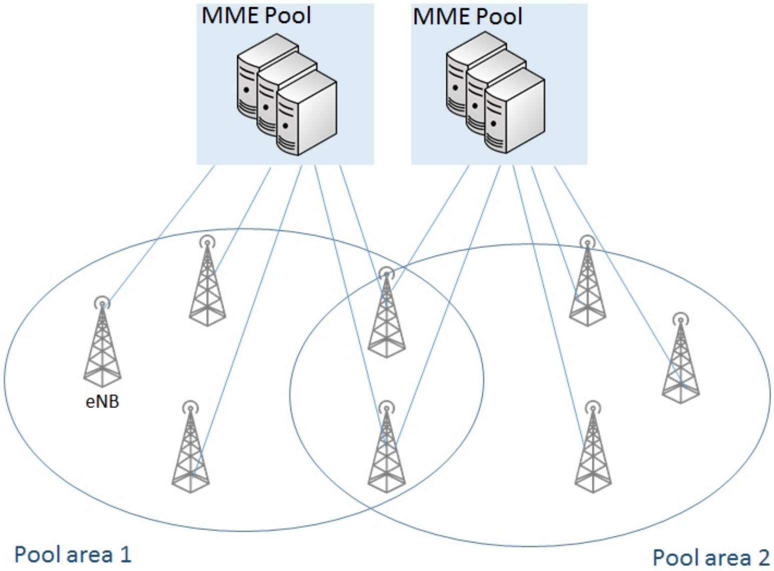

Figure 7. MME pooling concept

MME pooling is actually opening the opportunity to select the most appropriate MMEs (within an MME pool) to serve the Ues in the network based on different context and objectives, with the choice having a great impact on user service latency and general quality of experience. It can take place both while in initial configuration (S1 setup) but also during operation (optimization) and is mainly based on a controllable parameter defined as "weight factor" (e.g. ranging from 1 to 100). Each MME is assigned with such a weight factor that is conveyed to eNB during initial S1 setup. Based on the MME weight factors, an eNB can decide which MME in the pool can serve the calls and to what level. The probability of the eNB selecting an MME is proportional to its weight factor. The weight factor is typically set according to the capacity of an MME node relative to other MME nodes. The weight factor is sent from the MME to the eNodeB via S1-AP messages

A numerical example follows. For instance, assuming that:

- an eNB is communicating with 2 MMEs in a pool
- MME1 has a weight factor of 100
- MME2 has a weight factor of 50
- 3 UE attachments are pending

then, the eNB will forward 2 out of 3 Ues to MME1 and 1 UE to MME2.

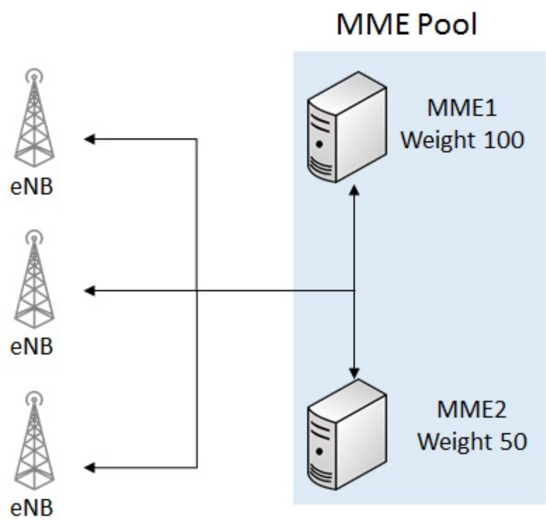

Figure 8. MME weight usage example

The weight factors (a.k.a. relative capacity) can be modified and enhanced by specific algorithms e.g. based on load measurements. These are reported to eNBs and the latter select the MME from the pool based on these updated values per each MME. In this way, the following mechanisms can be supported:

- **Load balancing** i.e. balancing the load among MMEs in the pool during initial configuration or after the introduction of a new MME and/or after removal of a MME from the network
- **Load re-balancing** i.e. balancing the load among MMEs in the pool for instance when an MME enters a maintenance/upgrade state.
- **UE offloading** i.e. moving certain (number of) Ues to less loaded MMEs
- **Overload control** i.e. restricting any new signalling connections by MMEs due to overload conditions.

In general, optimal load distribution of the signalling traffic towards MME nodes can be achieved through autonomic management of the mechanisms above.

In the latter case, proper reconfiguration may be required a) after the introduction of a new MME and/or after removal of a MME from the network, b) for balancing the load among MMEs in the pool, c) for re-balancing the load among MMEs e.g. when there is a need to offload traffic from an MME that may happen for instance when an MME enters a maintenance/upgrade state.

6.4.5.3 Hooks for GANA instantiation

6.4.5.3.1 Instantiation of DEs and indicative parameters

In addition, Load balancing can take place both in a centralized and in a distributed mode.

In the first case, a centralized entity (NMS/EMS) has the knowledge of the whole picture of the network i.e. the MME statuses, and based on this knowledge, it can take decisions for (re)configuring the mechanisms. Network-Level DEs can play the role of enhanced NMS/EMS systems by involving cognitive features e.g. advanced monitoring and predictive models for predicting MME loads in certain periods and location and exploiting this new knowledge for proactively configuring the MME weights an in general for automating the whole process.

More distributed schemes can also apply. In this case, the responsibility of monitoring the MME loads and of accordingly setting weight factors etc. is undertaken solely by each MME node and its DEs, of course by respecting the policies propagated by the operator.

In this case, we could envisage decisions taken at the Node Level DEs e.g. by a NODE_LEVEL_ AC_DE since the managed mechanism affects the behaviour of the node (MME) as a whole.

Alternatively, the mechanisms above (Mes) could be assigned to FUNC_LEVEL_MOM_DE being responsible for Mobility Management which is actually the main function the MME is logically offering, involving also a FUNC_LEVEL_MON_DE for managing monitoring and measurements associated with the mechanisms.

Last but not least, the distributed case requires coordination and interaction among MMEs (their DEs) belonging to the same pool.

By monitoring the MME relative capacities, load status, overload situations etc., the involved DEs should be able to manage the mechanisms and the parameters that each of the mechanisms is actually managing an indicative set of which is listed in Table 12 below.

Table 12. Mapping table for DEs instantiation in MME

Network Level DE	Node Level DE	Function Level DE	Managed Entity (Mechanism)	Example parameter
NET_LEVEL_MOM_DE NET_LEVEL_MON_DE	NODE_LEVEL_AC_DE	FUNC_LEVEL_MOM_DE	MME Load (Re)Balancing	MME weight factor
		FUNC_LEVEL_MOM_DE	MME Offloading	Percentage of Ues to be offloaded
		FUNC_LEVEL_MOM_DE	MME Offloading	Duration of offloading

		FUNC_LEVEL_MOM_DE	MME Overload control	eNB from which to reject 27rioritiza connections
		FUNC_LEVEL_MOM_DE	MME Overload control	Types of RRC connections to reject (Overload Action)
		FUNC_LEVEL_MOM_DE	MME Overload control	Duration of 27rioritiza rejections
		FUNC_LEVEL_MON_DE	MME Load (Re)Balancing	Measurement parameters e.g. period, Predictions
		FUNC_LEVEL_MON_DE	Offloading	Measurement parameters e.g. period, Predictions
		FUNC_LEVEL_MON_DE	MME Overload control	Measurement parameters e.g. period, Predictions

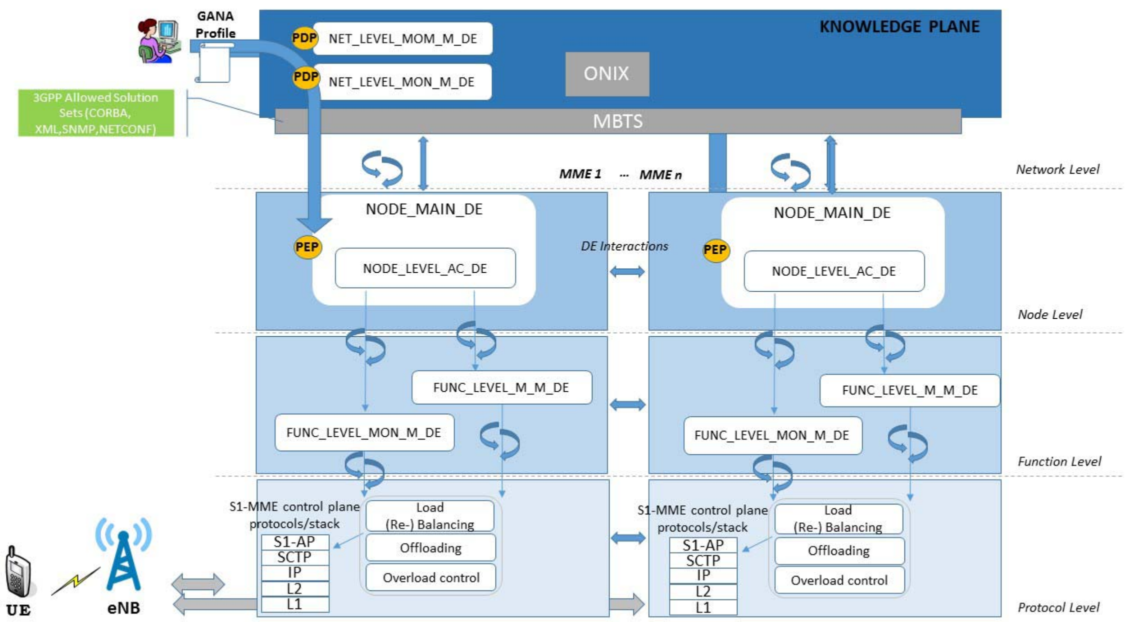

Figure 9: Instantiation of DEs and indicative parameters in the MME pooling management example

6.4.5.3.2 Policies

Different policies may be decided and be enforced based on the operator objectives. The policies can be propagated from the network level (policy decision points) down to the node and /or function-level-DEs (policy enforcement points) and be respected by the decisions being made therein. Examples could be as follows:

- Favouring the use of a specific MME among others belonging in the same pool.

- Controlling the frequency of weight factor changes
- Newly installed MMEs can be assigned with bigger weight factor, thus making them faster to increase their load.
- Offloaded MMEs can be assigned with zero weight factor so as to prohibit new Ues to be allocated to this MME
- The duration of offloading is also configurable and can be managed in an autonomic manner.
- The overload control could only apply to non-emergency and non-high priority mobile originated services.

6.5 Self-Healing

6.5.1 General Description and use cases

Self-healing is the process which detects problems (eg., operational, HW/SW faults etc.) and solves or mitigates these to avoid user impact and to significantly reduce maintenance costs. Self-healing is triggered by alarms generated by the faulty network elements. If it finds alarms that it might be able to correct or minimize the effects of, it gathers more necessary correlated information (e.g., measurements, testing results, and so forth), does deep analysis, and then triggers the appropriate actions. Self-Healing may incorporate SON mechanisms in order to reach its full functional capacity. The two major areas where the self-healing concept could be applied are as follows

A. Self-diagnosis: create a model to diagnose, learning from past experiences.
B. Self-healing: automatically start the corrective actions to solve the problem

The process of self-healing can be divided into four main phases:

1. Detection – Where in the network a problem has appeared.
2. Diagnosis – on the basis of the detection defines what kind of problem has happened and if some healing is required. False alarms are eliminated.
3. Recovery planning – a set of the necessary recovery actions is selected.
4. Recovery execution – phase when the actions are taken to handle the particular type of the detected problem and its outcome is assessed.

The list below consists of the self-healing functions which will be executing when a fault alarm is detected. In section 6.5.5, there is an analytical flow-chart in which all the appropriate steps that will be executed in each case are depicted.

[1]. Self-healing Input Monitoring Function (SH_MON_F): This self-Healing function monitors the TcoSHs (Trigger Condition of Self-Healing) continuously and when a TcoSH is reached, then an appropriate Self-Healing process will be triggered.

[2]. Self-healing Diagnosis Function (SH_DG_F): Based on the TcoSH and gathered information, this Self-healing Function does deep analysis and diagnosis, and gives the result. If the result includes recovery action/s, then go to next step of the healing process part, if not, go to End (termination of process).

[3]. Triggering Recovery Action/s Function (SH_TG_F): If the result from previous functions includes recovery action/s, then this Self-healing Function triggers the executing of the recovery action/s.

[4]. Self-healing Evaluating Function (SH_EV_F): This Self-healing Function evaluates the result of the self-healing recovery action/s. If the fault hasn't been solved and the stop condition/s is not reached, then the self-healing runs again. If the fault has been solved, then this function emits a notification to report the result.

[5]. Self-healing Fallback Function (SH_FB_F): This function is executed when the stop condition of the Self-Healing function is reached. In addition, if necessary, a fall-back situation is executed.

[6]. Self-healing Monitoring and Management Function (SH_MMF): This function monitors the self-healing process and provides the operator with the necessary information of the self-healing process. This function will be able to get information about all other functional blocks. In addition to this, it allows the operator to control the execution of the self-healing process.

[7]. Self-Recovery of NE software Function (SR_NSW_F): This function handles the self-healing function of recovery of NE software.

[8]. Self-healing of Board Fault Function (SH_BF_F): This function handles the self-healing function for board fault.

There are three concrete Use Cases which defined by 3GPP for the scope of the self-healing

A. Self-Recovery of Network Elements
    a. [All the EPC components]
B. Self-Healing of board faults
    a. [All the EPC components]
C. Self-Healing of Cell Outage (out of scope due to the fact that the focused area consists of the EPC, not the E-UTRAN one of LTE.)

6.5.2 Protocol-level entities (GANA Level 1) to be managed

The Self-Healing process affects the HW and SW of a network entity in terms of fault and resilience management when the monitoring process detects TcoSH. This is a condition which is used to judge whether a Self-healing Process needs to be started. In addition, this condition could be an alarm or the detection of a fault. To this end, the respective 3GPP and non-3GPP protocols and mechanisms may be affected and healing actions may be performed on these protocols and mechanisms.

6.5.3 Identification of GANA DEs for self-healing

This section presents the GANA DEs which are part of the self-healing use case. The abovementioned list has been built using figure 19 of ETSI GS AFI 002 as reference point. In addition, each DE is linked with the type of Managed Entities under its control as of the GANA architecture overview.

Function Level DEs

- Monitoring DE: Typical Mes are monitoring protocols/mechanisms which are responsible to monitor the condition of each Network Element (NE).

Network Level DEs

- Fault-Management DE: Typical Mes are mechanisms or protocols which are responsible to action when a fault alarm occurred.
- Resilience and Survivability DE: Typical Mes are proactive and resilience mechanisms or restoration and protection mechanisms.

6.5.4 Mapping of self-healing functions

Table 12 and table 13 provide a one to one mapping between the instantiated DEs and the managed protocols and mechanisms for MME and PGW. These entities have been initially chosen for the instantiation due to the key role they have in the 3GPPP CN.

Table 12 Mapping sub-table for MME

Network-Level DEs	Node-Level DEs	Function Level DEs	Protocols & Mechanisms	Examples
NET_LEVEL_RS_DE			3GPP protocols/mechanisms	Software Failure in the MME entity
NODE_LEVEL_FM_DE			No 3GPP protocols/mechanisms	Hardware Failure in the MME entity
	NODE_LEVEL_FM_DE		3GPP or no 3GPP protocol/mechanism	Software/Hardware Failure in the Node Level of MME
		FUNC_LEVEL_MON_DE	3GPP or no 3GPP protocol/mechanism	Monitoring Component

Table 13 Mapping sub-table for PGW

Network-Level DEs	Node-Level DEs	Function Level DEs	Protocols & Mechanisms	Examples
NET_LEVEL_RS_DE			3GPP protocols/mechanisms	Software Failure in the PGW entity
NODE_LEVEL_FM_DE			No 3GPP protocols/mechanisms	Hardware Failure in the PGW entity
	NODE_LEVEL_FM_DE		3GPP or no 3GPP protocol/mechanism	Software/Hardware Failure in the Node Level of PGW
		FUNC_LEVEL_MON_DE	3GPP or no 3GPP protocol/mechanism	Monitoring Component

6.5.4.1 MME

The figure below illustrates the mapping of GANA functions in the case of an MME network element. As mentioned below in the figure, the bolded “boxes”, which represent the Function Level of the GANA model, are the active components in each GANA Level. The grey-scale components represent the inactive components.

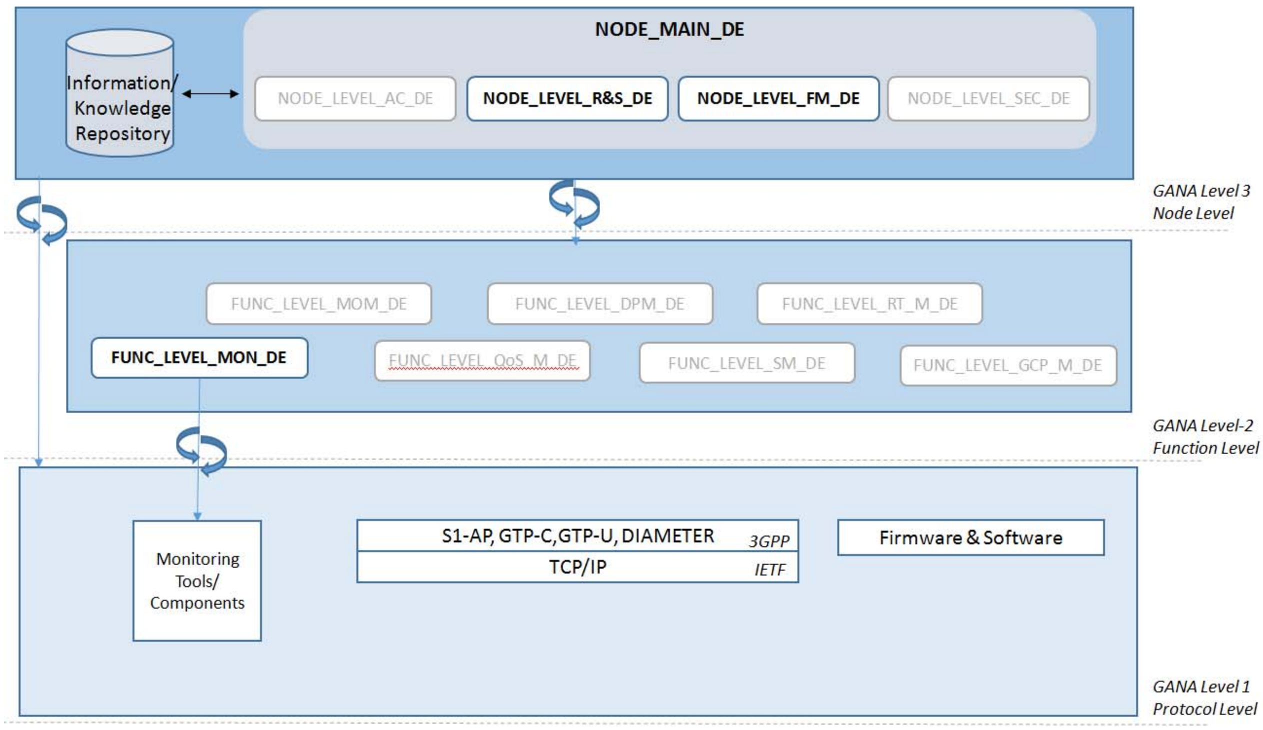

Figure 10: Node level view of self-healing case for the MME

6.5.4.1 P-GW

The figure below illustrates the mapping of GANA functions in the case of an PDN Gateway network element. As mentioned below in the figure, the bolded “boxes”, which represent the Function Level of the GANA model, are the active components in each GANA Level. The grey-scale components represent the inactive components.

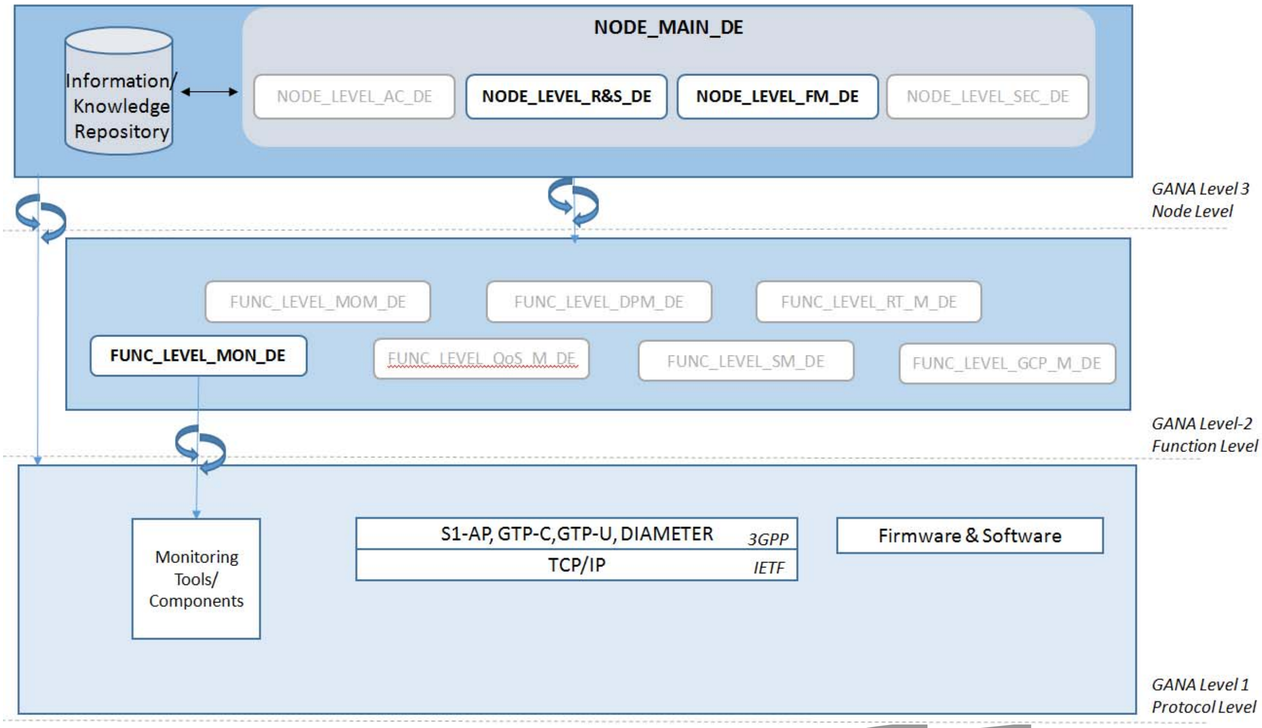

Figure 11: Node level view of self-healing case for the P-GW

6.5.5 Indicative examples of GANA instantiation – MME self-healing

As referred in the TS 32.541, the self-healing process has two parts: the monitoring part and the healing process part. The first one monitors, through a control loop, all the time the network element in order to alarm the appropriate healing process if a TcoSH (Trigger Condition of Self-Healing) is reached. Afterthought, the healing process part, collects the necessary information, 31riorit them and inform the appropriate self-healing processes. Below is listed an initial example of how the GANA and the self-healing functions respond in a fault alert situation, e.g. in the MME entity of the LTE EPC.

1) Monitoring Part:

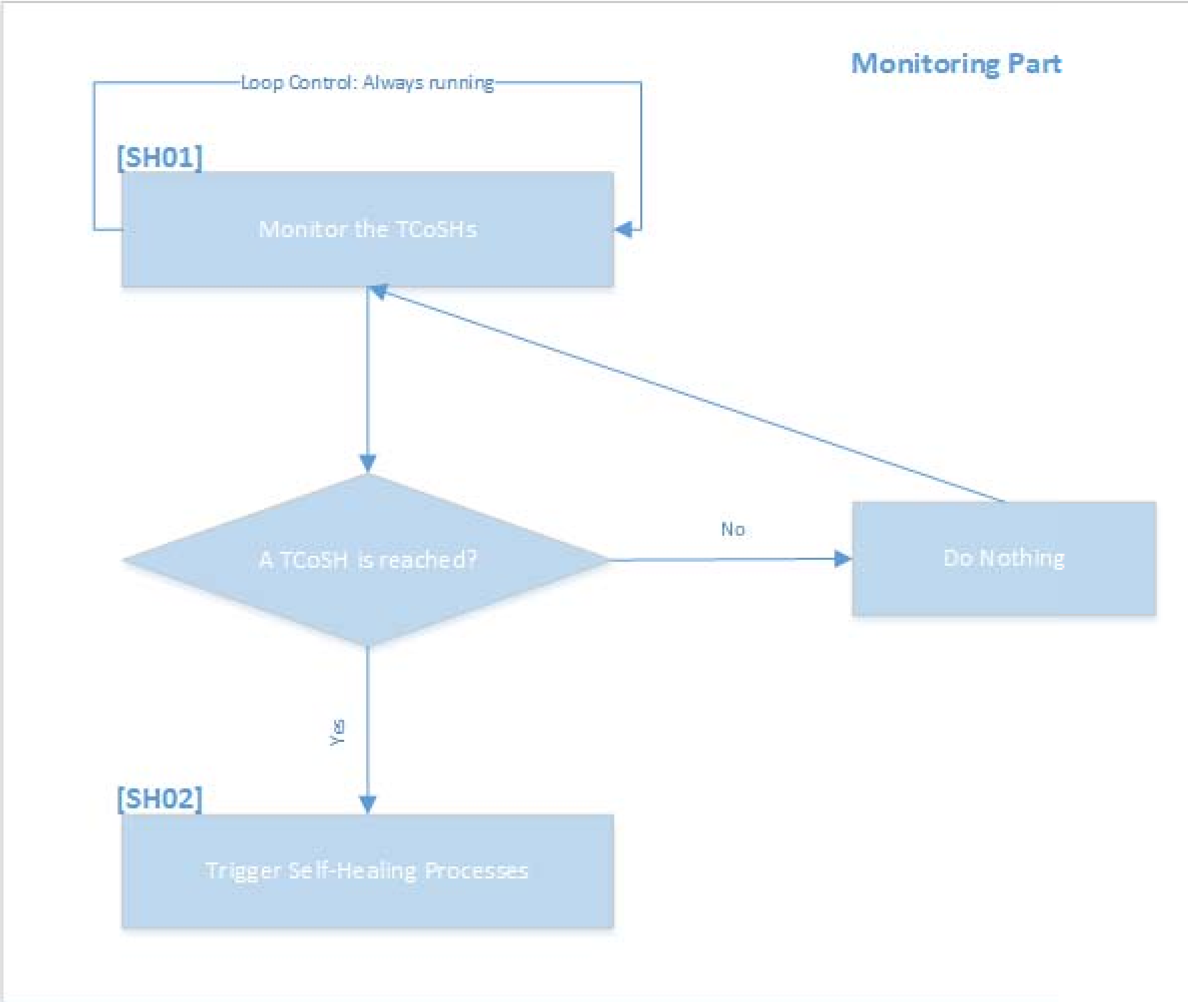

Figure 12: Self-healing monitoring part

[SH01] and [SH02] are corresponding to the Self-Healing functions 01 and 02 respectively. The [SH01] may collaborate with the GANA functions of MME, especially the **Monitoring Tools/Components**, in order to monitor the state of each Nes component.

2) Healing process Part:

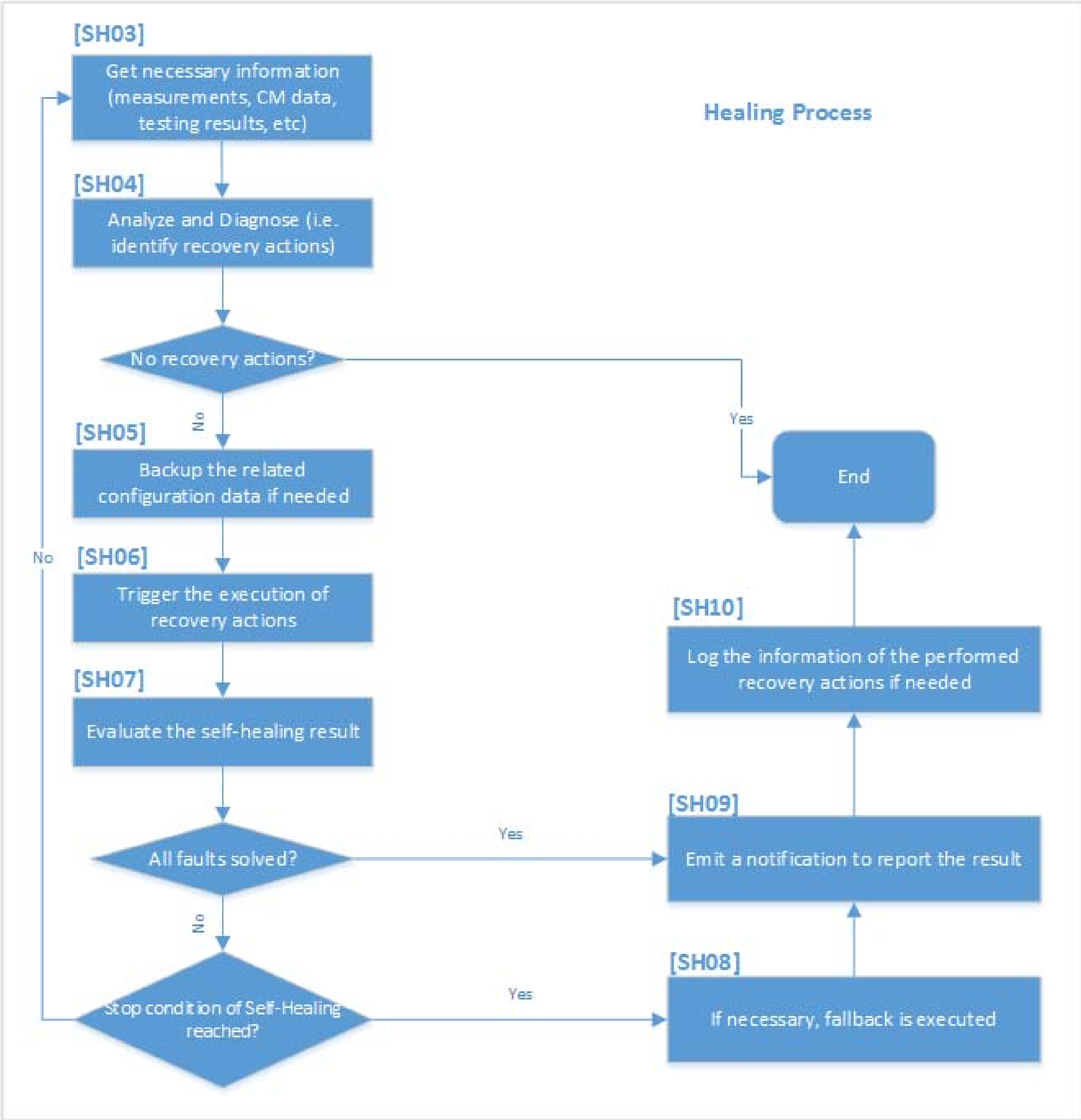

Figure 13 Self-healing processing part

The [SH03] is responsible in collecting all the necessary information, such as measurements, testing results, etc, in order to alert the appropriate self-healing function. The [SH03] may collaborate with the GANA functions of MME, the **FUNC_LEVEL_MOM_DE** and **FUNC_LEVEL_GCP_M_DE**, by collecting all the needed information through these two functions.

6.6 GANA Network Level view with knowledge plane

6.6.1 Characterization of the GANA KP in general, and the Interfaces that are in scope of this work

The Autonomic Management & Control (AMC) comprises a hybrid model that defines the abstraction levels at which interworking control-loops can be designed, while enabling to design nested and distributed control-loops to address complexity in design of autonomic functions. It is quite challenging to continuously analyse and merge raw data streams so that the results make actionable and operational sense. This is the goal of Complex Event Processing or Event Stream

Processing (ESP). Specifically, in the figure below, the main (northbound, southbound and other) interfaces for the GANA KP are depicted.

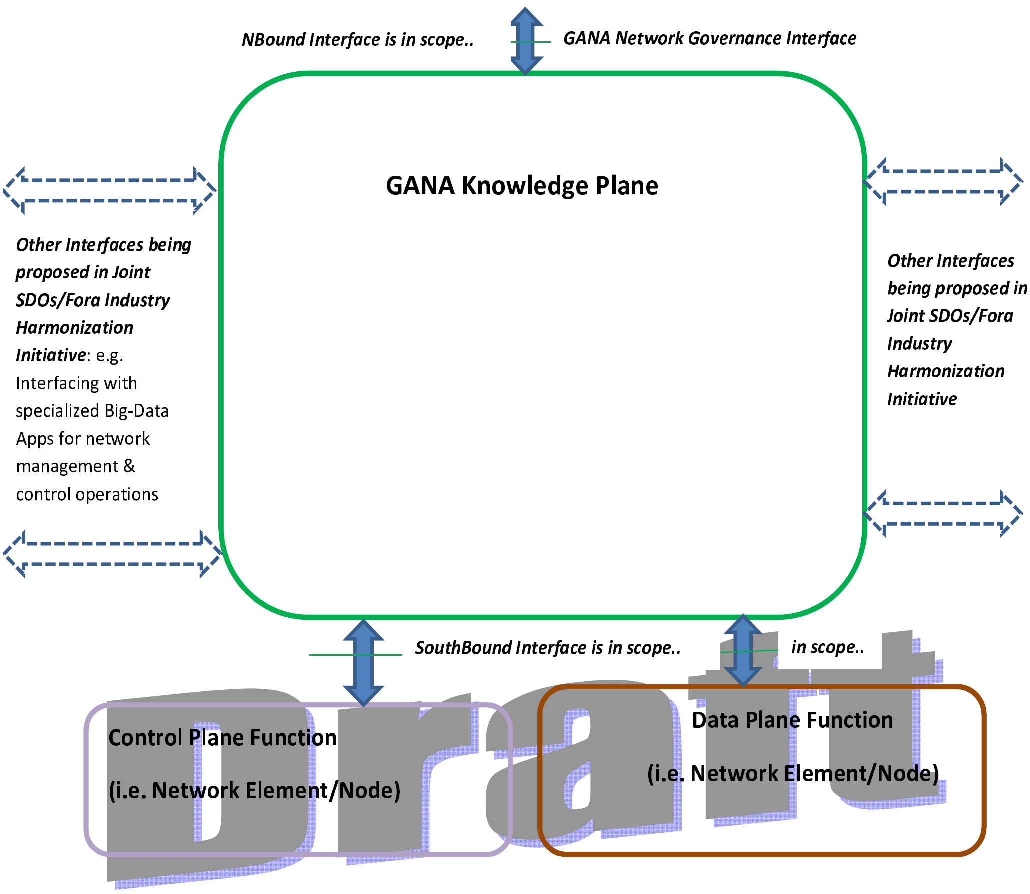

Figure 14 Interfaces of the GANA Knowledge Plane

The GANA KP and abstraction model can be viewed as a Modularized Analytics Engine, where each of the DEs (Decision Elements) may perform analytics and based on these analytics, the decisions and respective policies may be updated in the DEs. This is the part that incorporates the feedback loops and this may incorporate CEP, in order to harmonize the respective updates in policies and decision making. Examples of real-time and predictive analytics by specific DEs, may be addressed especially in Network Level Decision Elements (DEs) for the GANA Knowledge Plane like:

1. *QoS and QoE Management DE*
2. *Mobility Management DE*
3. *Fault Management DE*
4. *Resilience & Survivability DE*

For example fault analytics may be gathered by Fault Management DE. After performing and evaluating the data analysis, Complex Event Processing (CEP) for Decision-Making in individual DEs can be realized in two ways, either at each DE, or an instance of a CEP Module undertakes the assessment overhead and feeds all the relevant DEs. This implies the update of the policies in order to enable updated decision making based on the feedback loop.

6.6.2 Relationship between Analytics for management & control and Autonomics

As mentioned also in the previous section, there can be a strong link between data analytics and decision making based on a feedback loop. [i.11] discusses the relationship between analytics engines/processes designed specifically for management and control of network resources, parameters and services, and the broader paradigm of autonomics. In that regard such analytics is seen as part of the broader picture of Autonomic Management & Control (AMC) of networks and services, i.e. it is only a part of autonomics. Therefore following the discussion also from the previous section:

1. The GANA Knowledge Plane can be viewed as a Modularized Analytics Engine
2. DEs (Decision Elements) perform analytics
3. Examples of input to real-time and predictive analytics by specific DEs (including example Use Cases for Decision-making) can be found in the paper [i.10]

The data analytics can be based on Monitoring tools gathering various measurements and data from the network operations and services. The data can be of big volume or it can also history and real time data. In any case, the respective application of data analytics can have influence on the update of policies and decision making capabilities of the DEs, resulting in changing network or node behaviour.

6.6.3 Relationship between C-SON and GANA KP, and KP Southbound Interfaces Instantiations for 3GPP Core

In Figure 15, the Network level view for the mapping of relevant functionalities is depicted (here, showing the self-healing functions), with an emphasis to the GANA knowledge plane (KP).

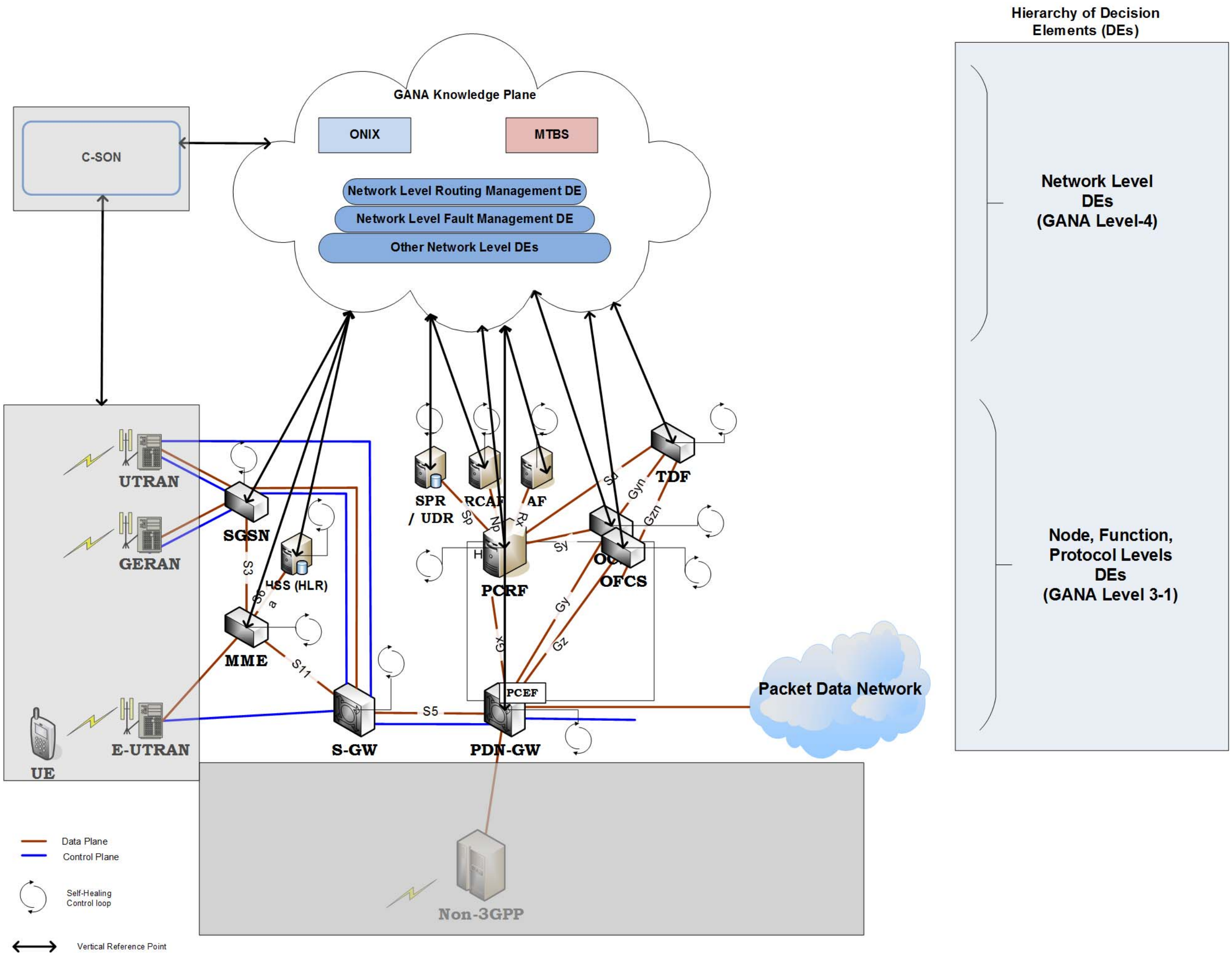

Figure 15 Instantiation of the GANA Knowledge Plane for the 3GPP Core Network

6.6.4 Instantiation of the GANA Network Governance Interface of the KP for the 3GPP Core Network

The GANA Network Governance Framework provides for coherence of policies and synchronisation between and across operator and administration domains. This is schematically depicted in Figure 16.

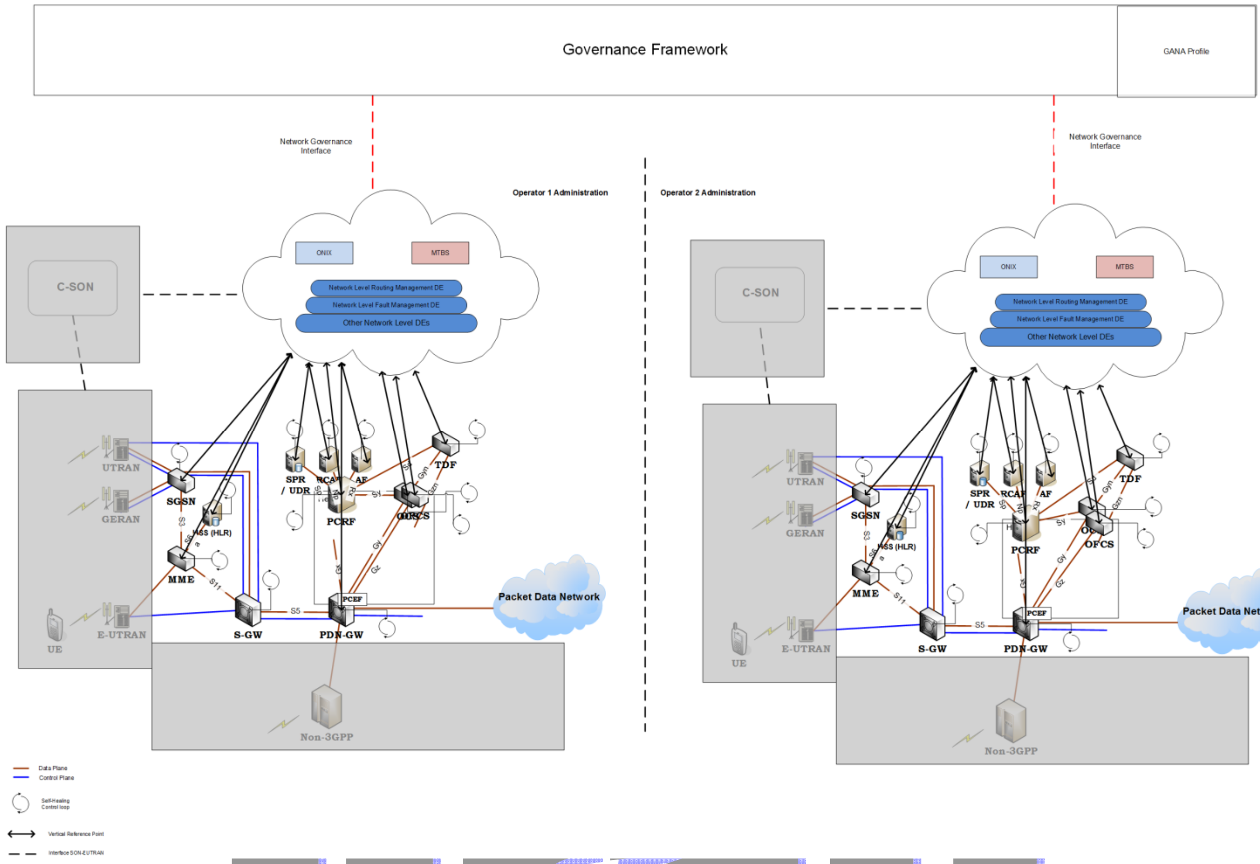

Figure 16 Instantiation of the GANA Network Governance Interface of the KP for the 3GPP Core Networks

An important issue for the governance framework and for the GANA Knowledge Plane is the policy management for enabling the autonomic network behaviour. In general Policies are very important for the operation and configuration of autonomic networks, since the policy is the rule defining a choice of the network behaviour. Policies have been widely used for the introduction of some level of automation in the control and configuration of network equipment operational behaviour. Usually they are based on predefined event-condition-action rules. They provide a deliberate plan of action for the decision enforcement and for the achievement of desired behaviours. Policy based behaviour of a network can be either static, or dynamic, depending on whether the policies can be updated automatically by the network systems, based on the evolution of network knowledge base. The application of either static or dynamic policies in autonomic systems may affect different decision levels. Conflict resolution mechanisms may be required as well.

Policies can be addressed as higher level policies (more abstract network view or business level) and low level policies (can be derived from system transformations). Moreover, policies can be also adaptive to new situations that demand changes in the network operation or configuration in order to accomplish its goals or to have a better performance. Policies also play a big role in interacting self-governing networks, for example for trust management between networks an domain and for achieving better operation between these networks from a wider network level perspective.

7 Autonomic behaviours across multiple segments

7.1 Introduction

The second phase of the GANA instantiation on the 3GPP EPC consists in devising the information exchanges and interactions between the entities identified in the mapping, i.e. the entities inside the KP, the DEs at the three higher levels of GANA, and the MEs. Interactions also take place across the different domains involved in the end-to-end operation of the mobile network, spanning RAN, backhaul and EPC NEs. At network level, this study defines how objectives and policies are transferred from PDPs to PEPs, how knowledge is shared and stored, which decisions are taken and where they are enforced. It also covers interactions among GANA nodes instantiated in NEs located in backhaul and EPC segments, but when needed it expands to RAN, as well e.g. autonomic decisions that are taken for the EPC segment, yet taking into account information retrieved from management functions responsible for RAN, primarily referring to C-SON. These interactions are summarized in Figure 17 below.

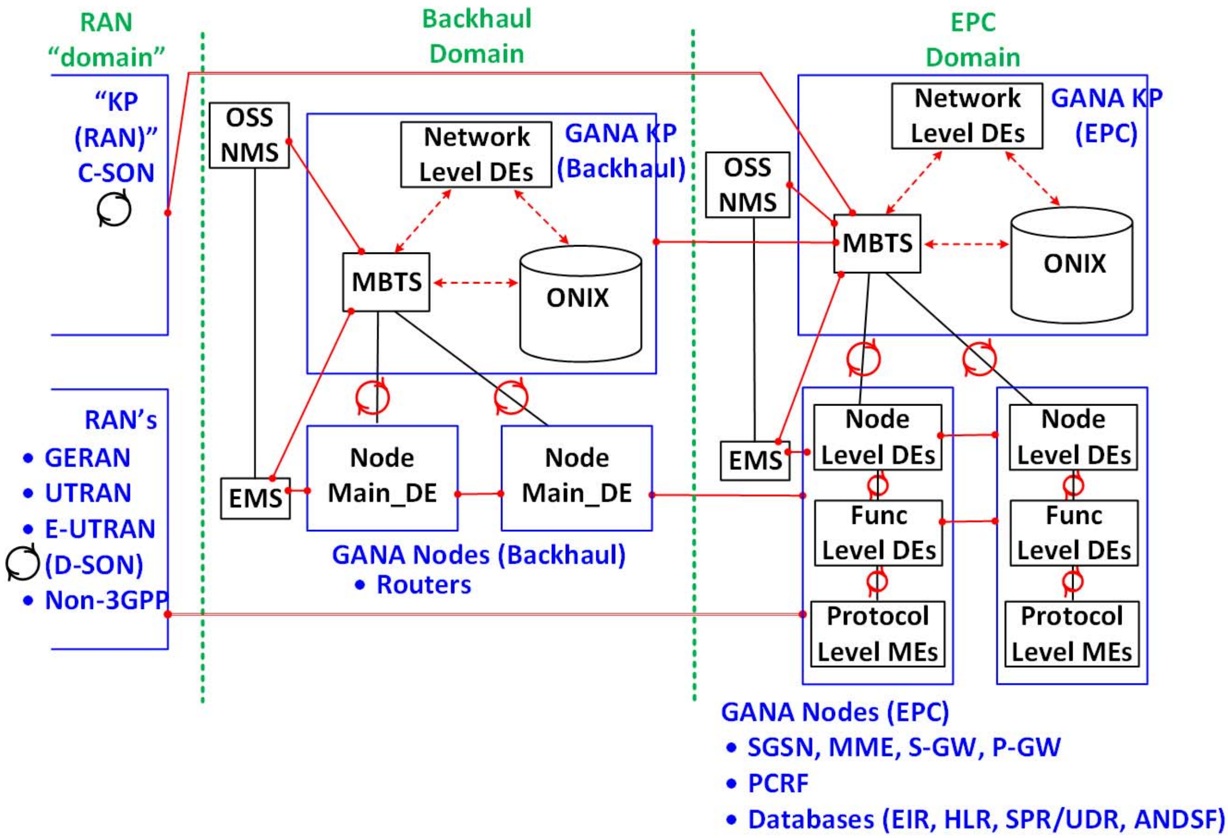

Figure 17 Interactions involving GANA entities for 3GPP Core Network mapping

Thus, this clause describes the transfer of policies, characteristic information and knowledge among that happens as part of the interactions among entities both horizontally (among different nodes and entities in the nodes) and vertically (among centralised management systems/knowledge plane and nodes) so as to support the decision taking and eventually the enforcement of autonomic decisions. This is shown using a set of exemplary use cases for each of which the following elements are identified and analysed: a) the objective of the use case, b) reference points at which information needs to be exchanged, c) the information, in terms of parameters/groups of parameters, that is to be exchanged and d) the candidate messages and associated protocols that can be used to exchange this information

7.2 Instantiation of the Governance interface for 3GPP core – Policy continuum

In 3GPP, the main network management reference model is the one depicted in the figure below. It covers the main structure of the management system and the respective processes, the reference points for information and policy exchange and the policies that will be implemented in node and network level.

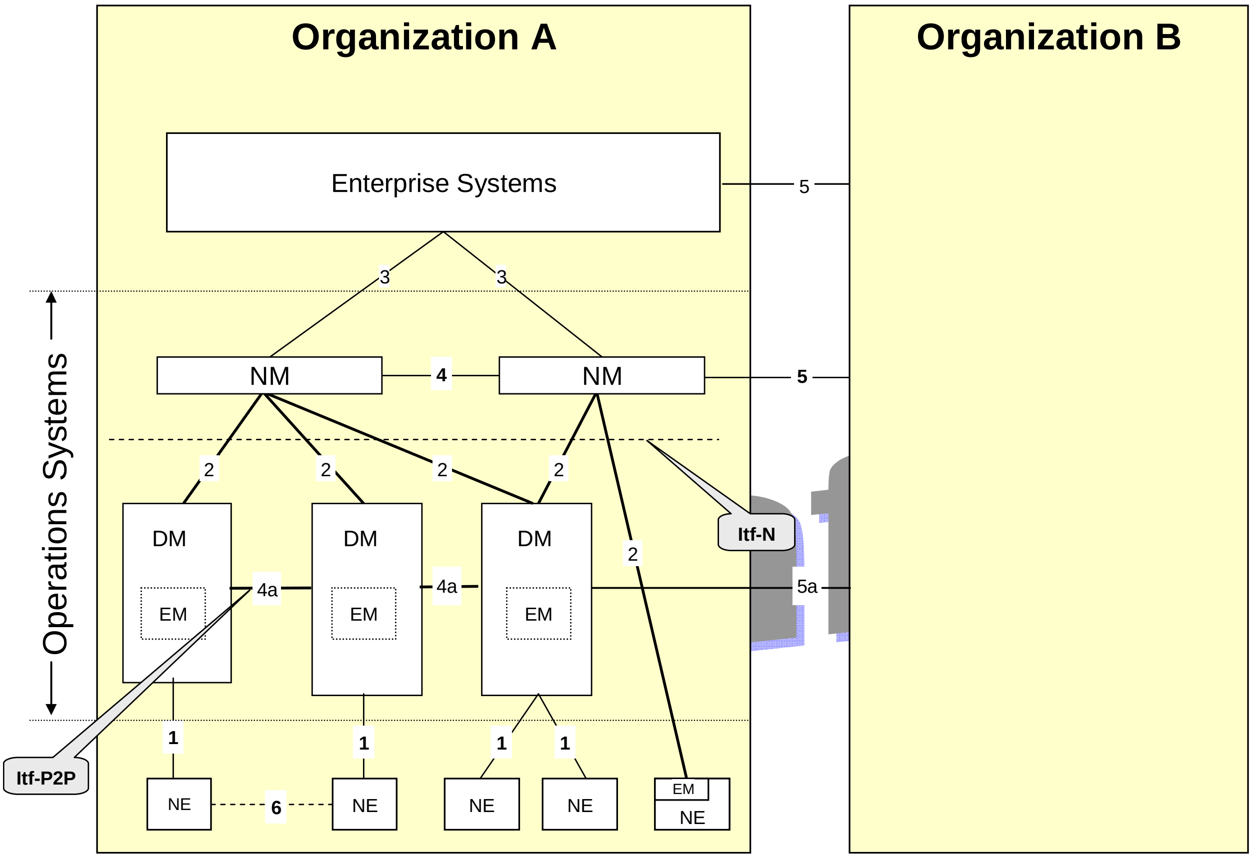

Figure 18 Management reference model (reproduced from 3GPP TS32.101)

In this model the interfaces that are most relevant for the mapping with the GANA model entities are the Itf-N, i.e. the Type 2 management interface and Itf-P2P, i.e. theType 4a management interface, since they can be associated with the interfaces and reference points between node level DEs and network level DEs, depending also on the implementation choices. In this context, the association of policy exchange and the respective protocols need to be addressed.

On the other hand in a 3GPP network architecture the functions that are primary related to policies and policy exchange are PCEF and PCRF. The Gx reference point is located between the Policy Control and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF). The Gx reference point is used for provisioning and removal of Policy and Charging Control (PCC) rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control or both by applying AVPs relevant to the application.

An example instantiation of a Policy-based QoS Management System for 3GPP networks is the following:

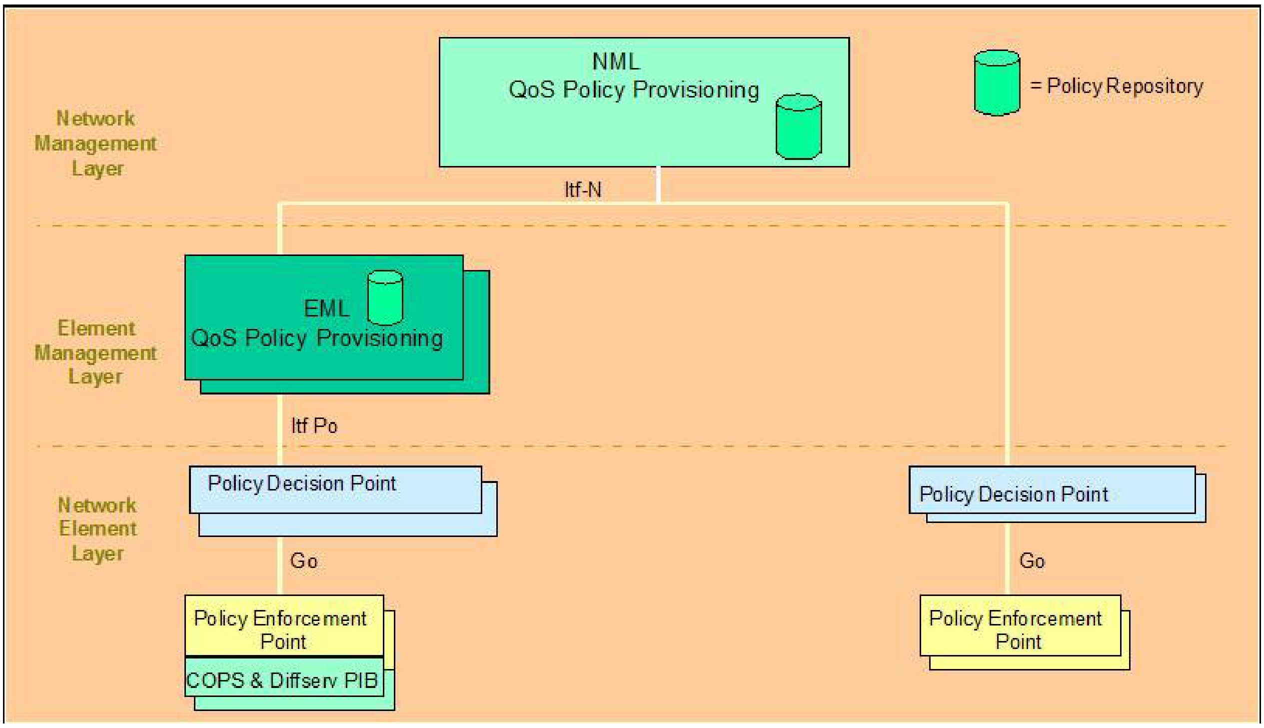

Figure 19 Conceptual architecture for a policy-based QoS Management System (reproduced from 3GPP TS32.101)

In this Figure it is apparent how the policy continuum can be addressed, between Policy Decision Points and Policy Enforcement Points. In the several levels of policy exchange, there are currently several protocols used, some of them are of more general purpose than others but all contribute to the enablement of different implementations for the policy exchange. The main protocols are:

- COPS (Common Open Policy Service) protocol
- BGP (Border Gateway Protocol)
- Diameter
    - Diameter interfaces in **LTE**

      S6a - Authentication, more in TS 29.272
      Gy - Prepaid charging, more in TS 23.203, TS 32.299;
      Gz - Postpaid charging;
      Gx - QoS/Policy, more in TS 29.211, TS 29.212;
      Rf - Charging, more in TS 32.299;
      Ro - Charging, more in TS 32.299;
      Rx - QoS/Policy, more in TS 29.214;
      S6d - Authentication;
      S9 - QoS/Policy;
      Sh - Subscriber Profile;
      Cx - Subscriber Profile;
      e2 - Location.
- Valid management application layer protocols for 3GPP
    - SNMP
    - CORBA IIOP
    - SOAP (WS)
    - REST

Taking all these into consideration, the next step is to address the instantiation of the Governance interface (based on the GANA model) for 3GPP core supporting the policy continuum aspect.

7.3 Reference points and associated protocols

Reference points:

- Reference points are illustrated in Figure 17. Unless otherwise specified, they enable bi-directional interactions. The data exchanged are described in the next paragraph.
- Network level reference points
    - From CN OSS i.e. the NMS at network level, or the EMS entities inside the nodes to MBTS;
    - Between RAN C-SON and MBTS;
    - For building the EPC KP: from MBTS to ONIX, between the Net_level DEs and ONIX, between the Net_level DEs and the MBTS, between the different Net_level DEs;
    - From the EPC KP to the Backhaul KP.
- Node level reference points
    - Between the different entities of the KP EPC and Node_Main_DE, targeting the orchestration of the Func_level DEs;
    - Between the KP EPC and the Node level DEs;
    - Between the Node-Main DE and the involved Func_level DEs;
    - Between Node level DE and respective Functional level DE;
    - Between each of the Node_level DE and its corresponding MEs;
    - Between each of the Func_level DE and its corresponding MEs;
    - Between the peer Node_level_DEs, across the GANA nodes,
    - Between the peer Func_level_DEs, across the GANA nodes,
    - Between the different Node_level DEs, inside the GANA node
    - Between the different Func_level DEs, inside the GANA node.

Candidate Protocols to be used at the reference points:

- The main protocols used are listed in Clause 7.2. The type of protocol to be used for each of the reference points is listed below.
- Network level reference points
    - From CN OSS (NMS, EMS) to MBTS: the protocols used are mainly COPS, SOA, Flume, SNMP;
    - Between RAN C-SON and MBTS: the protocols used are mainly Flume, SNMP;
    - From MBTS to ONIX: the schemes used are mainly publish/subscribe, secure query/search, data mining and find mechanisms;
    - Between the Net_level DEs and ONIX: the schemes used are mainly publish/subscribe, secure query/search, data mining and find mechanisms;
    - Between the Net_level DEs and the MBTS: the protocols used are mainly COPS, SOA, SNMP, CMIP, Flume …
    - From the EPC KP to the Backhaul KP: the protocols used are mainly COPS, SOA, BGP.
- Node level reference points
    - Between the EPC KP and the Node_Main_DE/ Node level DEs: COPS, CMIP, SOA, Diameter, Netconf, SNMP;
    - Between the Node-Main DE and the Func_level DEs: Node internal secure communication mechanisms;
    - Between each of the Func_level DE and its corresponding MEs in the EPC node: Diameter, SNMP, Netconf, RestConf, Netflow, OpenFlow;
    - Between the peer Func_level_DEs / Node_level_DEs, across the GANA nodes: GTP-C, ANIMA control plane protocol (GRASP, RPL), legacy protocols such as BGP, COPS, Diameter. SNMP, CMIP, SOA;
    - Between the different Func_level DEs, inside the GANA node: Node internal secure communication mechanisms.

7.4 Load Control

This sub-clause defines the objectives, entities and interactions at network level for the Load control example described in Clause 6.4.5.

Load Balancing and in general load control refers to the process whereby the load of the traffic that is going to be shared by more than one similar network elements is equally shared or generally controlled so as to serve specific network /operator needs. The similar network elements can be anything from P-GW, S-GWs, MMEs but also RAN elements such as base stations. As a matter of fact, the procedure is much intertwined with the selection functions described in 3GPP TS 23.401, in the sense that each time a decision is to be made that involves the selection of an MME/P-GW or S-GW etc., respectively, it is important to take into account load information among the multiple candidate elements to be chosen. Accordingly and in order to increase system capacity, MME pools may share user traffic load across different MMEs, P-GW may be selected to serve PDN connections according to their load and capacity, while at the same time base stations may share/offload traffic to neighboring cells etc. As a result, different DEs (algorithms) per segment or even per node, can simultaneously take load balancing decisions as per need.

Objective:

Thus the objective of the sub-clause is to propose an assignment of the load control/balancing and gateway selection decisions taken by EPC Nes into GANA specified DEs, while at the same time to drill into the details with respect to the involved reference points, as well as the policies to be injected, the load specific parameters to be delivered and the protocols to be used for delivering these parameters in order to support such load control decisions.

Involved DEs:

- In the KP, Network level Des that include: the Net_Level_MON_DE, for tuning the monitoring behaviours and tools of lower level monitoring DEs and the Net_Level_MOM_DE for taking decisions on the balancing and control of the load in the NEs and eventually in the network as a whole.
- In the GANA nodes, the equivalent Function level DEs are involved i.e. Func_Level_MON_DE and Func_Level_MOM_DE.
- Net_Level_MON_DE coordinate and inject policies to lower level monitoring DEs in nodes/devices to guide them on load related information that needs to be disseminated to external data collectors and requesting DEs like the Net_Level_MOM_DE
- Net_Level_MOM_DEs essentially take decisions on the load assignment per NE, based on high level operator policies, but also based on load information collected from the involved nodes, typically representing the mid and longer term traffic behavior of each node.
- Analogous decisions can be taken at the node level, based on short term measurements of load and distributed exchange of load information at node level or among the respective Function level DEs

Parameters or groups of parameters exchanged at the reference points

- Network level reference points
    - From OSS (NMS, EMS) to MBTS. The MBTS translates the policies and KPIs received from the OSS into GANA profiles and processed KPIs. This acquired knowledge is transferred and stored into the ONIX
    - Between RAN C-SON and MBTS. This interface allows to retrieve RAN related information, parameters, streams of KPIs and/or decisions made at RAN level by C-SON algorithms. The real-time data are directly consumed by the network level DEs to run the decision and data processing algorithms related to the desired network objectives, while aggregated data are stored in the ONIX. In the other direction, the network level DEs may either provide their decisions to the C-SON or collaborate with the C-SON functions, e.g. the load balancing or handover optimization, to coordinate the decisions made in order to achieve an e2e load balancing. This interface also transfers the control for the KPIs flow to be received, i.e. which parameters and with what periodicity.
    - Between the Net_level DEs and ONIX. This interface is used to transfer history of decisions, predicted network behaviour and traces. The ONIX provides GANA profiles to the Net_level DEs. Updated GANA profiles are exchanged in the other direction to be stored in the ONIX
    - Between the Net_level DEs and MBTS. The Net_level DEs use the node level views, retrieved from the GANA nodes through the MBTS, to complement the ONIX knowledge. In the case

where a decision impacts one or several entities in the network, the actuator part of the control loop triggers the corresponding commands, which are translated by the MBTS and forwarded to the related entities in the GANA nodes.

  - From the EPC KP to the Backhaul KP. The decisions made by the Net_level DEs may also require an adaptation of the routes or resource provisioning in the backhaul transport network. Policies and decision data are then provided to the backhaul KP, which triggers its own network level DEs.

- Node level reference points
  - Between the different entities of the KP EPC and Node_Main_DE as the highest level entity in the GANA hierarchy at node level. In the upwards direction, the Node_Main_DE provides the node level view of the network, e.g., monitoring information and measurement results regarding the load in the node. In the downwards direction, it receives and forwards policies and commands regarding node weight factors, load thresholds, variant load estimation algorithms. This interface is also used to push the node configuration and parameters into the KP, and more specifically the ONIX, through the MBTS.
  - Between the Node-Main DE and the involved Func_Level DEs: The Node-Main DE orchestrates the Func_level DEs, forwarding in both directions the information exchanged with the KP, and more specifically the MBTS, to retrieve the required parameters or apply the decisions made at network level.
  - Mon_DE –ME: measurement commands (what (load), when, periodicity, duration), measurement reports
  - Between the Func_Level_MON_DE and its corresponding MEs in the EPC node. The Func_Level_MON_DE uses the information it receives to run its own control loops. It communicates with the MEs it manages (monitoring mechanisms) to provide commands on how to measure the load, at which time, with what periodicity, with what granularity, for how long etc.
  - Between the Func_level_MOM_DE and its corresponding MEs in the EPC node: The Func_Level_MOM_DE uses the load information it receives to run its own control loops. It communicates with its related MEs, i.e. 3GPP nodes, mainly for updating the weight factors based on which the traffic load is appropriately shared, directed, or offloaded among the involved nodes.
  - Between the peer Func_Level_DEs, across the GANA nodes. These DEs exchange local policies from network level, load information/weight factors at node level, or streams of Func_Level load related decisions or types of load estimation algorithms used.
  - Between the different Func_level DEs, inside the GANA node. These DEs collaborate internally to exchange decisions and parameters request / parameters report (values). The MOM_DE may request the MON_DE to configure data sources that could feed such data back to the MOM_DE

7.5 Congestion resolution

Load balancing allows to transfer load from capacity restricted resource to others which have available capacity. This capability is also very important in the case where the congestion of one node occurs in the network. Using autonomicity to measure network quality and detect and resolve congestion situations would allow MNOs to react in a very short time frame to this type of events, improve the efficiency of their network operation and planning, maximize network utilisation, avoid over-provisioning, and thus reduce their CAPEX in a way not possible manually. Considering the LTE network deployments, congestion affects mostly the user plane, in the RAN, or in extreme cases, in the S-GW. However, for completeness, this report also considers it may occur in the P-GW and in the MME for the control plane. Existing mitigation techniques consist in disrupting the traffic in excess, which causes inconvenience to the MNO customer. Using autonomicity and GANA architecture, it is possible to resolve these situations by automatically offload part or whole of the UE traffic, or moving it between NEs, while maintaining the enforcement of the operator policies and authorizations.

Objective:

- The congestion resolution example covers the detection of congestion situations and their resolution by traffic offloading or UE mobility.
- The effect of the decision is to apply policies to execute the triggering of the resolution mechanisms, to control the monitoring behaviour, to define off-loading policies and mobility policies in the target nodes.
- In this example, the information collection also takes into account the reporting from the RCAF in the PCC and the UE subscription data from one of the databases installed in the EPC: HSS, HLR, UDC, User equipment information (EIR), or the User location information in the GMLC. Non-3GPP policies from the Access Network Discovery and Selection Function (ANDSF) may be considered as well.
- The impacted MEs are functions in the MME, the S-GW, and the P-GW, with some potential effect on the PCC entities as well.

Involved DEs:

- In the KP, this use case requires the Net_Level_MON_DE for monitoring and the Net_Level_MOM_DE for managing the offloading and the UE mobility. The Net_Level_QoS_M_DE may be involved as well to provide functionalities like Self-optimization and Self-adaptation.
- In the GANA nodes, the equivalent Function level DEs are involved: Func_Level_MON_DE, Func_Level_MOM_DE and potentially Func_Level_ QoS_M_DE.
- At network level, the DEs take decisions such as: retrieve monitoring information, trigger congestion resolution, selectively offload part of the traffic from one or more Ues, relocate some PDN connections, start UE mobility to a new NE with available resources.

Parameters or groups of parameters exchanged at the reference points:

- Network level reference points
    - From OSS (NMS, EMS) to MBTS. The MBTS translates the policies and KPIs received from the OSS into GANA profiles and processed KPIs. This acquired knowledge is transferred and stored into the ONIX.
    - Between RAN C-SON and MBTS. This interface allows to retrieve RAN parameters and steams of KPIs. The real-time data are directly consumed by the network level DEs to run the decision and data processing algorithms related to the desired network objectives, while aggregated data are stored in the ONIX (see more details in clause 7.7). In the other direction, the network level DEs may either provide their decisions to the C-SON or collaborate with the C-SON functions, e.g. the load balancing or handover optimization, to coordinate the decisions to be performed in order to mitigate the issue. This interface also transfers the control for the KPIs flow to be received, i.e. which parameters and with what periodicity.
    - Between the Net_level DEs and ONIX. This interface is used to transfer history of decisions, predicted network behaviour and traces. The ONIX provides GANA profiles to the Net_level DEs. Updated GANA profiles are exchanged in the other direction to be stored in the ONIX.
    - Between the Net_level DEs and ONIX. The Net_level DEs use the node level views, retrieved from the GANA nodes through the MBTS, to complement the ONIX knowledge. In the case where a decision impacts one or several entities in the network, the actuator part of the control loop triggers the corresponding commands, which are translated by the MBTS and forwarded to the related entities in the GANA nodes.
    - From the EPC KP to the Backhaul KP. The decisions made by the Net_level DEs may also require an adaptation of the routes or resource provisioning in the backhaul transport network. Policies and decision data are then provided to the backhaul KP, which triggers its own network level DEs.
- Node level reference points
    - Between the different entities of the KP EPC and Node_Main_DE as the highest level entity in the GANA hierarchy at node level. In the upwards direction, the Node_Main_DE provides the node level view of the network, e.g., monitoring information and measurement results (see "List

of parameters" below), while in the downwards direction, it receives traffic steering or UE mobility commands, duration of offloading, updated parameters, updated algorithms and policies. This interface is also used to push the node configuration and parameters into the KP, and more specifically the ONIX, through the MBTS.

- between the Node-Main DE and the involved Func_level DEs: The Node-Main DE orchestrates the Func_level DEs, forwarding in both directions the information exchanged with the KP, and more specifically the MBTS, to retrieve the required parameters or apply the decisions made at network level.
- Between the Func_Level_MON_DE and its corresponding MEs in the EPC node. The Func_Level_MON_DE uses the information it receives to run its own control loops. It communicates with the MEs it manages to provide commands and their parameters (e.g., measurement commands: what (load, UE location information), when, periodicity, duration), or receive corresponding answers and measurement reports.
- Between the Func_level_MOM_DE and its corresponding MEs in the EPC node: The Func_level_MOM_DE uses the information it receives to run its own control loops. It communicates with its related MEs, i.e. 3GPP nodes, to provide commands and parameters related to offloading or UE mobility, e.g., parameters for traffic steering, overload control parameters, candidate routes for offloading, candidate anchors for UE mobility, or receive corresponding answers or reports.
- Between the peer Func_level_DEs, across the GANA nodes (e.g., Func_Level_MON_DE in the MME and Func_Level_MON_DE in the S-GW). These DEs exchange local policies from network level, node-level monitoring information, or streams of Func_level decisions such as offloading decisions.
- Between the different Func_level DEs, inside the GANA node e.g., between the Func_Level_MON_DE and the Func_Level_MOM_DE. These DEs collaborate internally to exchange decisions and parameters request / parameters report (values).

List of parameters

The detailed list of C-SON KPIs parameters is not standardized. Therefore, it depends on the vendor implementations and is often considered as confidential information. On the other hand, the functions performed by the different products available on the market are well-known: automatic neighbour relations, load balancing, interference control, coverage and capacity optimization, or handover optimization [ref]. Service assurance platforms may be programmed to export the whole stream of KPIs or process them with their internal algorithms, while defining specific events where an aggregated view of the KPIs is exported to the KP. This corresponds to a flow of parameters or specific knowledge information with a time interval lower than with raw data.

On the EPC side, 3GPP TS 32.426 [ref] specifies the performance measurements to be performed in the different nodes: MME, P-GW, S-GW, but also MBMS-GW and PCRF. For example, the following measurements are relevant in the congestion resolution example:

- MME
  - Failed EPS attach procedures
  - MME control of overload related measurements for EPC (Start procedure, Stop procedure)
  - EMM-Registered subscribers (Mean number, Maximum number)
  - Handover related measurements (Inter RAT handover)
  - Number of dedicated EPS bearers in active mode (Mean, Maximum)
  - Failed dedicated bearer activation procedures by MME
  - MME Processor usage (Mean, Peak)
- P-GW
  - Failed number of PDN-GW initiated Dedicated Bearer Creation
  - Failed PDN-GW initiated Dedicated Bearer Modification with QoS update
  - Active EPS Bearers related measurements for EPC (Mean Number, Max Number)
  - Number of EPS bearers (Mean number, Maximum number)
  - SGi related measurements
- S-GW
  - GTP related measurements (GTP data/signalling packets, data volume on S4 and S12 interfaces)
  - S1-U data volume related measurements (GTP data packets on the S1-U interface)
  - Bearer resource Usage related measurements

- PCRF
  - IP-CAN session establishment related measurements

7.6 S-GW failure (without restart)

Following the capabilities that GANA model enables in Autonomic networks, the autonomic behaviours of the nodes can provide several solutions in cases of nodes restoration. An interesting example is when a PGW/MME/SGSN detects that a peer SGW has failure, it shall delete all PDN connection table data/MM bearer contexts associated with the peer node that fails as well as freeing any internal PGW/MME/SGSN resources associated with those PDN connections. Since there are no bearer/MM contexts in the PGW, the mobile terminated service cannot be delivered to the UE for long time. If the MME/SGSN performs implementation specific action to cleanup external resources, including at eNodeB/RNC and UE, the UE will be reattached to the network and the EPS services will be restored. Incorporating the GANA model and extending the autonomic behaviour of the nodes, in the abovementioned case, an autonomic approach could be adopted for the restoration of the resources and the connections. The general approach would encompass the Autonomic Fault-Management activities in a GANA network. These are executed by a set of node level Decision Elements and a network level DE on top of them. These DEs, together with the Resilience and Survivability DE on node/network level, and additional supporting components (e.g. incident dissemination mechanisms), form the Unified Architecture for Autonomic Fault-Management, Resilience, and Survivability (UAFAReS). The Network-Level-Fault-Management DE (NET_LEVEL_FM_DE) is responsible for self-configuration of diverse aspects of the NODE_LEVEL_FM_DEs in a certain network scope (e.g. OSPF area). Furthermore, the NET_LEVEL_FM_DE is the instance that keeps the global knowledge with respect to incidents and alarms for the network. This enables the NET_LEVEL_FM_DE to react to network wide erroneous states in case the NODE_LEVEL_FM_DEs are not capable of resolving the occurred faults and to escalate faulty conditions to the network operation personnel in case they are not resolvable by means of Autonomic Fault-Management.

Objective:

- Address the autonomic behaviour of nodes in cases of failures and recovery attempts. The self-healing actions should be driven by policies, decision taking and knowledge sharing. The failures can be partial or total, can involve the SW or the HW or both and can have varying recovery delays and remedies. Depending on the policies that are fed in the node or network level, in combination with the Knowledge building performed in KP, the policies that apply in each case create also a feedback loop in order to produce new policies based on history and dependency of events and on system knowledge.

- Consider examples like Node Failures, e.g., S-GW failure.

  - Policies relevant to S-GW failure: S-GW selection, UE services consumed (SPR), re-allocation of the paths from/to eNb + P-GW.

- Processes and tasks that can benefit from autonomicity:

  - Perform self-healing and recovery either at node level or network level, using policies and knowledge from previous situations in order to tackle the healing and recovery process more efficiently.

  - In case of node failures, to automate the transfer of the traffic over to new connections/tunnels and/or allocate flows, users, tasks etc to other nodes seamlessly.

Involved DEs:

- **The GANA model enables Self-healing/self-repair functionality.** The Autonomic Fault-Management control loop realized in the network devices is complemented by a control loop on the network level. The network level control loop facilitates the self-* features of self-healing and self-repair in case that the control loops inside the devices fail to introduce a successful self-healing/repair behaviour. The main functionalities involved in these processes are the **Fault-Detection and Incident Dissemination and Fault-Isolation.** The generic approach for these operations is the following:
  - The main processes of Fault-Detection and Incident Sharing, are carried out by the NET_LEVEL_FM_DE which is supported by a set of repositories and an Incident Dissemination Engine (IDE) that facilitate the sharing of alarm/incident events in a network scope. The NET_LEVEL_FM_DE keeps all incident events (across the network) in its

repositories, i.e. it has the global view regarding faults. On the other hand, the NODE_LEVEL_FM_DEs get informed only about information that they are concerned with.

- The NET_LEVEL_FM_DE runs a Fault-Isolation process on the global view of incident events stored in its repositories. This enables the NET_LEVEL_FM_DE to identify network wide faults and initiate the required process of Fault-Removal.

- Therefore, the main DEs involved in the S-GW failure are:
    - In the Network level : The Fault-Management DE is used for the identification of failures, while Resilience and Survivability DE is used for the application of network wide repair schemes that will allow seamless fault removal and network operation
    - The respective Node level DEs involved are: Fault Mngt ,for the identification, repair and removal of faults, based on the parameters that are monitored by the Mon_DE
    - The main Function level DE is the : Mon_DE, providing parameter monitoring

Parameters or groups of parameters, policies exchanged at the reference points:

- Reference Points
    - From OSS (NMS, EMS) to MBTS, mainly business level and network wide operational level policies and KPIs are exchanged. C-SON – MBTS = C-SON to MBTS: parameters and RAN KPIs from C-SON for recovery and self-healing , load balancing etc. if necessary – MBTS to CSON: alarms to C-SON Self-Healing function for fault incidents, like e.g., S-GW failure:
        - S-GW performs per-bearer user plane tunnelling and inter-eNodeB path switching during handover. S1-U is the interface between EUTRAN and S-GW. The transport protocol over this interface is GPRS Tunnelling Protocol-User plane (GTPv1-U). In case of S-GW failure, the C-SON should receive an alarm. Then, depending on the recovery policies adopted, the e-NodeBs may be prompted to establish a connection to another anchor S-GW. Relevant parameters can be: dedicated bearer identity, Linked Bearer Identity to identify the associated default bearer, the traffic flow template, and the associated QoS parameters
    - Between MBTS – ONIX, mainly GANA profiles, translated KPIs and knowledge are exchanged. The MBTS translates the policies and KPIs received from the OSS into GANA profiles and processed KPIs. This acquired knowledge is transferred and stored into the ONIX.

- Between the Net_level DEs and ONIX:history of decisions, healing and recovery schemes and optimizations at network level, traces , network resilience schemes. This interface is used to transfer history of decisions, predicted network behaviour, , healing and recovery schemes, network resilience schemes and traces. The ONIX provides GANA profiles to the Net_level DEs. Updated GANA profiles are exchanged in the other direction to be stored in the ONIX. Between Net level DEs-ONIX: The Net_level DEs use the node level views, retrieved from the GANA nodes through the MBTS, to complement the ONIX knowledge. In the case where a decision impacts one or several entities in the network, the actuator part of the control loop triggers the corresponding commands, which are translated by the MBTS and forwarded to the related entities in the GANA nodes by updated GANA profiles

    - Between Net-level DEs – MBTS : The Net_level DEs use the node level views, retrieved from the GANA nodes through the MBTS, to complement the ONIX knowledge. In the case where a decision impacts one or several entities in the network, the actuator part of the control loop triggers the corresponding commands, which are translated by the MBTS and forwarded to the related entities in the GANA nodes

- EPC KP – Backhaul KP exchange policies, decisions. The decisions made by the Net_level DEs may also require an adaptation of e.g., the routes or resource provisioning in the backhaul transport network. Policies and decision data are then provided to the backhaul KP, which triggers its own network level DEs. The MON_DE (node or network level) and the Fault-Management_DE (node or network level) exchange mainly TCoSH (Trigger Condition of Self-Healing)
- Fault Management DE and Resilience & Survivability DE exchange mainly data analytics and policies for decisions related to network robustness and fault tolerance and resolution, as well as schemes for self-Healing and recovery
- Fault Management DE (network level) and Fault Management DE(node level) exchange mainly policies for self-Healing and recovery and TCoSH (Trigger Condition of Self-Healing)
- Peer Node level DEs exchange mainly monitoring data, as well as policies for recovery

7.7 Recommendations

The main outcome of the study in this report is that it is possible to introduce autonomics (management and control intelligence) in the Core and the Backhaul without impacting the existing reference points and architecture. Existing protocols and management mechanisms can be leveraged to execute the necessary interactions between the Core Network standardized nodes and functionalities and the overlay of atomic autonomic components (software) entities introduced by the GANA framework mapping. The autonomic components may be launched in the network as intelligence-enhancing management and control software. There is no impact on the user plane or the control plane. However the work identified the need for a reference point in the management plane to be placed between the C-SON and GANA Knowledge Plane for the Core network. This would enable information (e.g. some KPIs) or decision sharing between the two entities so as to implement collaborative end-to-end self-optimization by C-SON and GANA Knowledge Plane for the Core network.

More specific recommendations regarding implementation alternatives of the GANA model can be derived as follows:

Dynamic PDP and PEP

Because of the dynamic nature of the GANA model, the attribution of PDP vs. PEP functions may vary over time, mainly for the entities related to the KP and for the DEs in the GANA nodes. From a general point of view, a DE acts as a PDP for its lower level DE and as PEP for its upper level DE. In the 3GPP CN mapping, the network level DEs may act as PEP or PDP for the OSS and the RAN C-SON, depending on the target function and the status of the network. In this case, the notion of cascading PDP is introduced, when OSS acts as PDP for the network level DEs which, in their turn, are PDPs for the DEs in the GANA nodes.

MBTS and ONIX

The role of the MBTS is not to store knowledge, but rather to process ontologies from different vendors in order to translate the data received at its interfaces into GAN profiles and aggregated data sets. On the other hand, ONIX is a distributed system providing secures services for storing, retrieving and disseminating information. It does not contain any decision logic.

In the 3GPP CN mapping, the ONIX stores information with a larger time scale, e.g., [TBD]:

- Profiles from OSS translated into cleaned GANA profiles (as an xml structure)
- updated GANA profiles after DE algorithm execution
- history of DE commands and their context
- Information pushed from GANA nodes at the EPC nodes (MME, S-GW, P-GW, PCRF): capabilities, resources, configuration
- configuration information pushed by 3GPP databases (HSS, HLR, EIR, UDC,ANDSF, …) when relevant
- aggregated KPIs from RAN and measurement from EPC nodes
- predicted network behavior

Minimum DEs in each EPC node: Monitoring

Monitoring is an important aspect of the management of 3GPP CN. Thus all EPC nodes should at least host a GANA node including the Node-Main DE and the Func_Level_MON_DE to be able to report the node level view of the network to the network level DEs through the MBTS and potentially stored in the ONIX.

GANA MBTS and C-SON interactions in Self-Healing – S-GW failure

The C-SON Self-Healing function and the GANA self-Healing related functions have similarities and complementarities. A harmonisation of the detailed alarm/s which a self-healing function monitors should be performed during the implementation phase. For example C-SON should be able to monitor alarms from the GANA Network level DEs. The recovery actions can be different, although a harmonisation of these actions between core and access is also preferable. So, it is recommended that the solutions of self-healing would be implemented in a harmonised way in terms of monitoring and recovery schemes between C-SON and GANA self-healing functions. Following this, it is recommended to define by vendors a general framework for the self-healing function, including the monitored faults that a self-healing function may resolve and the general method of the self-healing function. The alarms monitored by the self-healing functions would benefit from a harmonised framework and the recovery actions of the self-healing function may not be specified for all self-healing use cases.

The knowledge plane and the feedback loops in order to update the policies in Self-Healing – S-GW failure

The knowledge plane and the policies have a strong interdependence. In self-healing functions, the respective business level policies will be incorporated in network level and node level DEs, in order to enable the identification and prioritization of Faults/Failures as well as the appropriate recovery schemes. Following the actions taken in each case, then this input will be fed back to the knowledge plane along with the results of the actions, e.g., whether the failure was repaired, whether the issue has been escalated to the administrators and required human intervention etc. In this case the feedback loop is able to generate new policies that depend to the situation awareness knowledge enriched by the results of the actions triggered by the default policies. So, it is recommended that the policies and respective solutions of self-healing should be implemented in case by case manner.

8 Conclusion

Annex A:

Annex B:
Title of annex

B.1 First clause of the annex

B.1.1 First subdivided clause of the annex

<Text>.

Annex E:
Bibliography

<Publication>: "<Title>".

OR

- <Publication>: "<Title>".

Annex F:
Change History

Date	Version	Information about changes
December 2015	0.0.1	First publication of the TR for TC NTECH #13
February 2015	0.0.2	STF Internal version including new Chapter 7
February 2015	0.0.3	Improvements to be submitted to steering committee on 03/03/2016
March 2015	0.0.4	Update for TC NTECH #14
March 2015	0.0.5	Update for LS to 3GPP

History

Document history		
<Version>	<Date>	<Milestone>