Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomic and Self-Managed Networks Phase 2 (BBF)
Contents

Intellectual Property Rights .......................................................................................................................2

Foreword ....................................................................................................................................................2

Modal verbs terminology ............................................................................................................................2

References ..................................................................................................................................................2

Normative references ................................................................................................................................2

Informative references ..............................................................................................................................2

Definitions, symbols and abbreviations ....................................................................................................2

Definitions ................................................................................................................................................2

Symbols ..................................................................................................................................................2

Abbreviations .........................................................................................................................................2

Background and Introduction to the ETSI GANA Reference Model ........................................................2

Overview ................................................................................................................................................2

Instantiation of the GANA model onto the BBF reference network and management & control architectures .................................................................................................................................2

BBF Reference architectures considered ..................................................................................................2

Instantiation of GANA model concepts onto BBF architecture key functional entities ..................................................2

Introduction ..............................................................................................................................................2

General considerations derived from BBF Specifications ........................................................................2

Requirements for autonomic features in BBF functional entities ................................................................2

Instantiation of GANA DEs onto BBF key architecture Network Elements (NEs) ........................................2

CPE: QoS interworking between fixed and 3GPP networks, marking of tunnels based on user-specific policy, network policy and QoS setting .................................................................2

BNG: BNG termination of PPPoE ................................................................................................................2

AN: Configuration of the xDSL ports ..........................................................................................................2

AN: Buffer configuration ............................................................................................................................2

GANA instantiation onto the virtualised BBF architecture with SDN ........................................................2

Introduction ................................................................................................................................................2

GANA instantiation onto the BBF and ETSI-NFV reference model for infrastructure interworking ........2

BBF Managed Entities (MEs) ..................................................................................................................2

NFV Managed Entities (MEs) ..................................................................................................................2

Overview of the Mapping of GANA model to ETSI NFV MANO ..............................................................2

Overview of the Mapping of GANA model to ETSI NFV MANO ..............................................................2

GANA instantiation onto Network Enhanced Residential Gateway ..........................................................2

GANA instantiation onto Software-Defined Access Network (SDAN) ....................................................2

E2E BBF instantiation ..................................................................................................................................2

Introduction ..............................................................................................................................................2

Conclusion ................................................................................................................................................2

Annex A: ..................................................................................................................................................2

Annex B: Title of annex: The ONIX System and possible ways to implement ONIX ................................2

ONIX architecture ....................................................................................................................................2

First subdivided clause of the annex ........................................................................................................2
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 aims at providing recommendations for the introduction of autonomies (management and control intelligence) into the fixed broadband access and aggregation networks specified in the Broadband Forum (BBF) Architecture specifications. To this effect, it covers the instantiation of the reference model for Autonomic Networking, Cognition and Self-Management, called GANA (Generic Autonomic Networking Architecture), starting from the reference architecture defined in BBF TR 101 [i.9], and considering also TR-178 [i.10] and TR-317 [i.34] reports. It superimposes GANA Decision Elements (DEs) into nodes/devices and the overall BBF 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.

Based on this, the report identifies the requirements for autonomic behaviours (Autonomics Functions/DEs) across the fixed broadband access and aggregation network segments of the BBF reference architecture and provides recommendations on where and how the GANA Functional Blocks (including DEs) should be instantiated. It further extends these recommendations to the virtualized manifestation of these segments considering their virtualized evolution in conjunction with SDN and NFV technologies. Finally, it also provides recommendations on the interworking and coordination between autonomic functions among GANA-BBF and GANA-3GPP (Core Network) domains, as well as recommendations on the Interworking and coordination between virtualised GANA-BBF and virtualised GANA-3GPP (Core Network) domains.

2 References

2.1 Normative references

Not applicable.

2.2 Informative references


[i.2] ETSI TR 103.495: "Network Technologies (NTECH);Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in Wireless Ad-hoc/Mesh Networks".


[i.5] ETSI TS 103 371: " Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Proofs of Concept Framework".

[i.6] ETSI TS 103 194: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet".

[i.7] ETSI TR 103 404: Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in the Backhaul and Core network parts of the 3GPP Architecture", V1.1.1 (2016-10)
[i.8] DSL Forum TR-101 “Migration to Ethernet-Based DSL Aggregation” April 2006

[i.9] BBF TR-101 “Migration to Ethernet-Based Broadband Aggregation” Issue: 2, July 2011

[i.10] BBF TR-178 “Multi-service Broadband Network Architecture and Nodal Requirements” Issue: 1, September 2014


[i.18] Wendong Wang; Xiangyang Gong; Xirong Que: Context-aware autonomic QoS model for future Internet: Published in: GLOBECOM Workshops (GC Wkshps), 2011 IEEE: DOI: 10.1109/GLOCOMW.2011.6162534


ETSI GS AFI 002: Autonomic network engineering for the self-managing Future Internet (AFI): GANA Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management. Note: This GS is now undergoing a transformation to an ETSI TS 103 195-2 that will be published by ETSI in 2017

Software Defined Access Networking (SDAN): Taking NFV and SDN to the “Edge”: White Paper by ASSIA

Heavy Reading & SaS White Paper: Advanced Predictive Analytics: Optimize your Network & Transform Customer Experience


Bruno Cornaglia, Vodafone Group Services, “Fixed Access Network Virtualization”, Broadband Forum Contribution bbf2014.084.00, February 14th, 201

Cornaglia, Bruno; Young, Gavin; Marchetta, Antonio: Fixed Access Network Sharing: Elsevier publication: 10.1016/j.yofte.2015.07.008

BBF TR-358 “Error! Unknown document property name.”, Issue: 1, Issue Date: December 2016.

Appledore Research Group White Paper: Closed Loop Automation and the new role of Assurance: 9/1/201

BBF TR-317 “Network Enhanced Residential Gateway”, Issue 1, Issue Date: July 2016

NETCH AFI TR-Draft – Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI): Impact of Generic Autonomic Network Architecture (GANA) on other paradigms: NFV and SDN How GANA integrates with SDN, NFV, E2E Service Orchestration and Big-Data Analytics for Autonomics

ETSI NETCH AFI TS 103 195 V0.1.1 “Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management
3 Definitions, symbols and abbreviations

3.1 Definitions

Access Network: The Access Network encompasses the elements of the broadband network from the NID at the customer premises to a Broadband Network Gateway. This network typically includes one or more types of Access Node and may include an Ethernet aggregation function.

Access Node: The Access Node (AN) may implement one or more access technologies based on copper, fiber or wireless. It may also aggregate traffic from other access nodes. It can be placed in a variety of locations from climate controlled (central) offices to outside environments that require climate hardening of the equipment to avoid the need for additional cabinets or enclosures. In this specification, this node contains at least one standard Ethernet interface that serves as its uplink interface into which it aggregates traffic from broadband user ports. Access Nodes may be distributed systems, with distributed ONUs, shelves, or modules that attach to one another and present the management view of a single, distributed system.

Aggregation Network: The part of the network stretching from the Access Nodes to the Broadband Network Gateway(s). In the context of this document the aggregation network is considered to be Ethernet based, providing standard Ethernet interfaces at the edges, for connecting the Access Nodes and Broadband Network Gateway(s), and some transport for Ethernet frames (e.g. Ethernet over SONET, MPLS, RPR, etc.) at the core.

Autonomic Behaviour (AB): process which understands how desired Managed Entity (ME) behaviours are learned, influenced or changed, and how, in turn, these affect other elements, groups and network [i.6]

Autonomic networking: networking paradigm that enables network devices or elements (physical or virtual) and the overall network architecture and its management and control architecture to exhibit the so-called self-managing properties, namely: auto-discovery of information and entities, Self-configuration (auto-configuration), Self-diagnosing, Self-repair (Self-healing), Self-optimization, and other self-* properties

NOTE 1: Autonomic Networking can also be interpreted as a discipline involving the design of systems (e.g. network nodes) that are self-managing at the individual system levels and together as a larger system that forms a communication network of systems.

NOTE 2: The term "autonomic" comes from the autonomic nervous system (a closed control loop structure), which controls many organs and muscles in the human body. Usually, human are unaware of its workings because it functions in an involuntary, reflexive manner - for example, human do not notice when their heart beats faster or their blood vessels change size in response to temperature, posture, food intake, stressful experiences and other changes to which human are exposed. And their autonomic nervous system is always working [i.6].

Broadband Network Gateway: IP Edge Router where bandwidth and QoS policies may be applied. This term is used instead of BRAS to denote an Ethernet-centric IP edge node in this document.

Complex Event Processing (CEP): data processing discipline which correlates data from multiple sources to identify patterns of events
context aware: capability of a component or system to be aware of its execution environment, the objectives it is supposed to meet and possibly the consequences of not delivering on the objectives, and be able to react to changes in the environment

Decision Making Element (DME): functional entity designed and assigned to autonomically manage and control its assigned Managed Entities (MEs) by dynamically (re-)configuring the MEs and their configurable and controllable parameters in a closed-control loop fashion.

NOTE 1: Decision Making Elements (DMEs) [Error! Reference source not found.] referred in short as Decision Elements (DEs) fulfill the role of Autonomic Manager Elements.

NOTE 2: In GANA a DE is assigned (by design) to very specific MEs that it is designed to autonomically manage and control (ETSI GS AFI 002 [i.3] provides more details on the notion of ownership of MEs by specific DEs required in a network element architecture and the overall network architecture).

Managed Entities (MEs): physical or logical resource that can be managed by an Autonomic Manager Element (i.e. a Decision Element) in terms of its orchestration, configuration and re-configuration through parameter settings [i.6]

NOTE: MEs and their associated configurable parameters are assigned to be managed and controlled by a concrete DE such that an ME parameter is mapped to one DE. MEs can be protocols, whole protocol stacks, and mechanisms, meaning that they can be fundamental functional and manageable entities at the bottom of the management hierarchy (at the fundamental resources layer in a network element or node) such as individual protocols or stacks, OSI layer 7 or TCP/IP application layer applications and other types of resources or managed mechanisms hosted in a network element (NE) or in the network in general, whereby an ME exposes a management interface through which it can be managed. Mes can also be composite MEs such as whole NEs themselves (i.e. MEs that embed sub-MEs).

non-aggregated scenario: scenario of 3GPP architecture without the aggregation of other types of networks, e.g. previous generations of mobile networks

overlay: logical network that runs on top of another network

NOTE: 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.

self-advertising: capability of a component or system to advertise its self-model, capability description model, or some information signalling message (such as an Ipv6 router advertisement message) to the network in order to enable other entities to discover it and be able to communicate with it, or to enable other entities to know whatever is being advertised

self-awareness: capability of a component or system to "know itself" and be aware of its state and its behaviours. Knowledge about "self" is described by a "self-model"

self-configuration: capability of a component or system to configure and reconfigure itself under varying and unpredictable conditions

self-descriptive: capability of a component or system to provide a description of its self-model, capabilities and internal state

self-healing: capability of a component or system to detect and recover from problems (manifestations of faults, errors, failures, and other forms of degradation) and continue to function smoothly

self-monitoring: capability of a component or system to observe its internal state, for example by monitoring quality-of-service metrics such as reliability, precision, rapidity, or throughput

self-optimization: capability of a component or system to detect suboptimal behaviours and optimize itself to improve its execution

self-organizing function: function that includes processes which require minimum manual intervention

self-protecting: capability of a component or system to be capable of detecting and protecting its resources from both internal and external attack and maintaining overall system security and integrity

self-regulation: capability 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
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
- AN: Access Node
- BBF: Broadband Forum
- BNG: Broadband Network Gateway
- CEP: Complex Event Processing
- CPE: Customer Premises Equipment
- DE: Decision Element
- DHCP: Dynamic Host Configuration Protocol
- DSL: Digital Subscriber Line
- 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
- NFV: Network Function Virtualization
- OSPF: Open Shortest Path First
- P GW: PDN Gateway
- PCRF: Policy and Charging Rules Function
- PPPoE: Point-to-point protocol over Ethernet
- QoS: Quality of Service
- RG: Residential Gateway
- SDN: Software Defined Networks
- S GW: Serving Gateway
- TCP: Transfer Control Protocol
4 Background and Introduction to the ETSI GANA Reference Model

4.1 Overview

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.

Though the GANA model was validated in testbeds, a key step towards adoption of autonomies by the industry is to instantiate it onto a set of representative well-known reference architectures in order to enable launching pilot projects on concrete use cases. This is because many network architectures being deployed today do not intrinsically exhibit autonomicity and self-management capabilities, and industry needs to understand the implication of evolving them towards this technology.

The objective of the present work is to develop a Technical Report on the instantiation of the GANA model on the BBF Architecture specifications. More specifically, it is required to perform a mapping on fixed broadband access, aggregation network architectures and the convergence with SDN / NFV.

The work has been divided into several tasks which are reflected in the following clauses. The first task consisted in defining the BBF reference architecture to be addressed. This is reported in Clause 5. In a second step, a mapping of the GANA model to the BBF architecture was defined for the key components of the architecture. This is reported in Clause 6. The final task consists in considering SDN/NFV convergence. This [will be] reported in clause 7.

4.2 ETSI GANA Reference Model in Brief (Nutshell)

To enable the reader to understand the GANA instantiation on the BBF network architectures and their associated management control architectures, the present clause provides a short overview of the GANA reference model specified in [i.36] and described in [i.11].

The ETSI Generic Autonomic Networking Architecture (GANA) reference model specifies the concepts and principles defining the domain of autonomic communication, autonomic networking, autonomic and cognitive management and control-all as part of the “big-picture” of Self-Management. Figure 1 below presents the GANA abstraction levels for self-management functionality at which interworking hierarchical/nested control-loops and their associated DEs can be designed. Figure 1 defines the key GANA Functional Blocks (FBs) for enabling and implementing autonomies in target implementation-oriented architectures, as described in the sub-sections below. A table of a summary of all GANA FB reference points and characteristic information descriptions is given in chapter 13 of ETSI GS AFI 002 [i.25]. The Reference points are further described in this present document.
The GANA is a Reference Model for Autonomic Networking, Cognitive Networking and Self-Management. The aspects of autonomic networking, cognitive networking and self-management of networks and services are covered in GANA collectively as the AMC (Autonomic Management & Control) paradigm. AMC is about Decision-making-Elements (DEs) as autonomic functions (logics that dynamically configure their associated managed entities in respective closed control-loops) with cognition introduced in the management plane as well as in the control plane (whether these planes are distributed or centralized) by virtue of introducing DEs in the planes.

Cognition (learning, analysing and reasoning used to effect advanced adaptation) in DEs, enhances DE logic and enables DEs to manage and handle even the unforeseen situations and events detected in the network.

Control (in “AMC”) refers to the control-loop logic kernel of the DE, capable of dynamically adapting network resources and parameters or services in response to changes in network goals/policies, context changes and challenges in the network environment that affect service availability, reliability and quality.

DEs realize self-* features of a functionality or system (self-configuration, self-optimization, etc.) as a result of the decision-making behaviour of a DE that performs dynamic and adaptive management and control of its associated Managed Entities (MEs) and their configurable and controllable parameters. Such a DE can be embedded in a Network Element (NE) or higher at a specific layer of the outer overall network and services management and control architecture—thereby creating AMC architecture (composed of nested and hierarchically stacked DEs that can also collaborate horizontally across management and control planes). An NE may be physical or virtualized (such as in the case of the NFV (Network Functions Virtualization) paradigm). Network functionality such as routing, forwarding, mobility management, etc. can be made autonomic by embedding a DE. DEs (as software components) are meant to empower the networks and the management and control planes to realize self-* properties: auto-discovery of information/resources/capabilities/services; self-configuration; self-protection; self-diagnosis; self-repair/heal; self-optimization; self-organization behaviours; as well as self-awareness.

Self-manageability in GANA is achieved through the dynamic and context-aware orchestration and management and control of MEs by collaborative Decision-making-Elements (DEs) (see definition of an ME and a DE in the Definitions clause). GANA defines a hierarchy of such DEs in four basic levels: the "protocol", "function", "node", and "network" levels. The levels are described in more detail in ETSI White Paper No.16 [i.24] and in ETSI GS AFI002 [i.25]. At each level, a DE manages one or more lower-level DEs through a control loop. The lower-level DEs are therefore considered as Managed Entities (MEs) by the DE that controls them. Over the control loop, a DE sends commands, objectives, and policies to its lower-level DEs and receives feedback in the form of monitoring information or other type of knowledge. The Protocol Level DEs represent protocols, services, and other fundamental mechanisms running in the target network as MEs that may exhibit intrinsic control-loops (DE logic) and associated DE—as is the case for some of today’s protocols such as OSPF, which can be considered an example of the instantiation of a protocol-level DE (though such autonomic-like feature in OSPF is not cognitive (learning and reasoning) in its operation and by design). As discussed in ETSI White...
Paper No.16, the GANA Specification puts forward a recommendation to primarily focus on the three higher GANA levels of hierarchical control-loops (Level2 to Level4) when introducing autonomics in architectures and considers the protocol level DEs as MEs. The GANA hierarchy emphasizes only the three other levels, which should collaboratively work together. The argument, put forward in the ETSI White Paper No.16 and ETSI GS AFI 002, is that three levels of hierarchical control-loops (GANA level-2 to level-4) demonstrate how AMC can be gracefully (non-disruptively) introduced in today’s existing networks and architectures and even in new network architectures that follow the approach of designing and employing protocols to build protocol stacks in which individual protocols are rather simple and do not embed any intrinsic control-loops.

At the lowest level in the management hierarchy in GANA is the resource layer in the Network Elements (NEs), which can be physical or virtual, that consists of Managed Entities (MEs) such as protocols or stacks, OSI layer 7 or TCP/IP application layer applications and other types of resources or managed mechanisms hosted in a network element (NE). They are managed by Function Level DEs (present in every Network Element, or NE) e.g. Routing Management DE. The orchestration of the Function Level DEs is performed by the Node Main DE. A Node_Main_DE is present in every NE, for example a router. At the highest DE level, the Network Level DEs address similar aspects as the Function Level DEs but on a wider scope. Therefore there is a Network Level Routing Management DE, Network Level Monitoring DE, Network Level QoS Management DE, etc. The GANA Knowledge Plane (KP) is constituted by the Network Level DEs, together with a distributed, scalable Overlay Network system of federated information servers for Information eXchange (ONIX) and a Model-Based-Translation Service (MBTS) for translating information and commands/responses towards NEs. The ONIX is useful for enabling auto-discovery of information/resources of an autonomic network via “publish/subscribe/query&find” protocols. DEs can make use of ONIX to discover information and entities (e.g. other DEs) in the network to enhance their decisions. More details on ONIX are given in the ETSI GS AFI002. The ONIX itself does not have network management & control decision logic (as DEs are the ones that exhibit decision logic for AMC). MBTS (Model-Based Translation Service) is an intermediation layer between the GANA Knowledge Plane (KP) and the NEs (physical or virtual) for translating vendors’ specific and technology specific raw data onto a common data model for use by network level DEs, based on an accepted and shared information model.

The GANA Knowledge Plane (GANA KP) enables advanced management & control intelligence at the Element Management (EM), Network Management (NM) and Operation and Support System (OSS) levels by interworking with them through their northbound interfaces or enhancing and evolving the intelligence of the systems at these levels by way of replaceable and (re)-loadable autonomies modules (DEs) that can be loaded at specific abstraction levels of management and control operations (more details in [i.24] ETSI White Paper No.16, [i.25] ETSI GS AFI002).

Moreover, governance is implemented through the Network Governance Interface. The network administrator uses this interface to manage the operation of the whole autonomic network by authoring, validating and submitting conflict-free policies, high-level network objectives and some configuration data to the KP, all encapsulated together in the form of a “GANA Network Profile” that is generated using automation tools. This GANA Profile is then used by the Network Level DEs to configure themselves and issue commands and lower level policies that are issued to lower level DEs for enforcement (including relaying sub-profiles that are used by lower level DEs to configure themselves and their MEs). More details on the GANA Network Profile creations and use can be found in the ETSI GANA White Paper No. 16 [i.24] and ETSI GS AFI 002 [i.25]. The GANA Profile can be augmented/extended with run-time related information by the Network Level DEs and MBTS and stored/maintained in the ONIX.

4.3 Characterization of the GANA Knowledge Plane

1. The Knowledge Plane (KP) is an integral part of Management & Control Systems that provides for the space to implement complex network analytics functions performed by Decision-making-Elements (DEs) that run as software in the Knowledge Plane and drive self-* operations such as self-adaptation, self-optimization objectives for the network and services by programmatically (re)-configuring Managed Entities (MEs) in the network infrastructure through various means possible: e.g. through the NorthBound Interfaces available at the OSS, Service Orchestrator, Domain Orchestrator, SDN controller, EMS/NMS, NFV Orchestrator, etc. In such interactions the Knowledge Plane DEs may employ the services of an MBTS (Model-Based Translation) set of software libraries as discussed in [i.24] ETSI White Paper No.16, as the MBTS enables management-protocol agnostic, control-protocol agnostic, and vendor-agnostic management and control of physical or virtual Network Elements (NEs) by the GANA Knowledge Plane. An Intent-based language for programming the network through the SDN controller that may provide such a northbound intent-based interface can also be applied by the GANA Knowledge Plane DEs in (re-)programming the network.

2. Various types of GANA Knowledge Plane’s Decision-Elements (DEs) can be designed to perform autonomic management and control operations (the self-* operations) on various types of Managed Entities (MEs) in the network infrastructure’ network elements (virtualized (VNFs) or physical (PNFs)). DEs are representative of cognitive management & control “domains” of reasoning regarding specific management and control aspects. Example DEs that can be designed in the Knowledge Plane are:
• Fault-Management-DE;
• Resilience & Survivability-DE;
• Auto-Configuration-DE;
• QoS & QoE & Performance-Management-DE;
• Security-Management-DE; Monitoring-DE;
• Routing-Management-DE; etc.

A DE monitors Managed Entities (MEs) assigned to it by design, uses the monitoring data and any other input data from other data/information or policy sources in the environment to analyze and compare the state of the MEs against the desired state that is adaptively computed from certain objectives meant to be enforced by the DE (which may change any time based on e.g. context and policy changes, network conditions, manifestations of faults in the network, etc.), and then creates a plan of actions or strategies to dynamically change the state and operations of the MEs, and then executes the actions/plans to effect changes on the MEs. Such DE operations are performed reactively and/or proactively to meet desired objectives regarding the state or behaviours of MEs.

Cognitive algorithms of a DE e.g. Machine Learning, Deep Learning, Computational Intelligence and other types of AI (Artificial Intelligence) algorithms, etc., drive the operations of the DE. ETSI GS AFI002 provides insights as to which levels in GANA should the DEs at that level need to have a higher degree of cognitive properties (cognition), as DEs at the Level-1 need to implement fast control-loops possibly with little or zero cognitive properties (cognition); moving higher up the GANA levels—at DEs at Level-2, control-loops are fast in contrast to control-loops at Level-4 (outside of a GANA Node/NE) but slower than those at Level-1, but a certain degree of cognitive properties can be introduced in the Level-2 DEs; moving higher up the GANA levels—at DEs at Level-3, control-loops are fast in contrast to control-loops at Level-4 (outside of a GANA Node/NE) but slower than those at Level-2 to some extent, but a much higher degree of cognitive properties than GANA Level-2 and Level-1 can be introduced in the Level-3 DEs; moving higher up the GANA levels—at DEs at Level-4, control-loops become slower in contrast to control-loops at GANA Levels in the GANA Node/NE level, but the highest degree of cognitive properties than GANA Level-3, Level-2 and Level-1 collectively, can be introduced in the Level-4 DEs. So, in general, control-loops within the NE are fast control-loops (in terms of timescale of reactions to changes) while those outside, at the network-level (GANA Knowledge Plane level), are slower than those at NE level but with much very high degree of cognitive properties and wider (network-wide) views as scope on which the corresponding Network Level DEs operate on. ETSI GS AFI002 provides more insights on such design principles for DEs. GANA, as described in [I.24] ETSI White Paper No.16 and [I.25] ETSI GS AFI 002 and in this present document, provides guidelines on how to design DEs such that they coordinate their operations to avoid conflicts.

3. The GANA Knowledge Plane may perform the functions of traditional management and control systems usually performed by traditional OSS, NMS/EMS if such a scenario is commercially viable such that no such traditional management systems are required anymore, otherwise the Knowledge Plane should interwork with such traditional systems in driving the re-configuration (e.g. to realize Self-Optimization objective or Self-Healing Objective) of the network and services as may be deduced and deemed necessary by DE algorithms during the operation of the network. Another implementation option could involve DEs implemented to run as loadable modules of an OSS, otherwise the Knowledge Plane can integrate with the OSS via an OSS Northbound Interface.

4. The GANA Knowledge Plane should fulfill the combined role of Network Analytics Driven Service Orchestration and Network Analytics Driven Closed-Loop (Autonomic) Service Assurance:

• Network Analytics Driven Service Orchestration should be performed by the Knowledge Plane DEs in response to network or resource capacity demands and resilience targets/objectives.

• Network Analytics Driven Closed-Loop (Autonomic) Service Assurance should be performed by the Knowledge Plane DEs with the target of improving customer experience. Autonomic (Closed-Loop) Service Assurance involves the Knowledge Plane as an Analytics Platform equipped with engines (DEs) that collects and analyses data from various data sources such as traditional Service Assurance Platforms (e.g. Performance management systems), network service functions/nodes, SDN Controllers, etc., and detect any service degradations and SLA violations. The Analytics Platform then closes the loop by communicating monitor results to Orchestrators and triggering remediation and corrective operations via a combination of Service Orchestrators, SDN Controllers, and Service Functions/Nodes.
such as CPE (Customer Premises Equipment), Access Node, BNG in Broadband Forum (BBF) architectures, and other types of service function nodes of other types of architectures. The Knowledge Plane DEs should be able to communicate to a Service Orchestrator Results obtained from Monitoring a Service such as SLA violations and generate Recommendations (actionable insights) on how the problems can be solved (humans could make use of the generated Recommendations, e.g., making use of the Recommendations to perform the actions if the Knowledge Plane DEs are configured to operate in an “Open-Loop” Mode). At the same time in a “Closed-Loop” mode, the DEs should go further on their own accord to trigger operations on the Service Orchestrators (which include orchestrator types like the NFV Orchestrator) in a “Closed-Loop” (autonomic) service assurance goal based on what the DEs determine to trigger on an orchestrator or any other management and control system such as an SDN controller, so as to realize Self-Healing of the Service(s)—thanks to autonomics of the Knowledge Plane operations. While Service Assurance should now evolve towards “Closed-Loop” (Autonomic) Service Assurance, rather that the Service Assurance Function computing Recommendations as actionable insights and operate in an open loop as discussed in [i.27] and in [i.33], the GANA Knowledge Plane is meant to be an implementation of a Service Assurance Function that is autonomic in its operation, acting in a Closed-Loop fashion that drives Self-* behaviours (performed on the Managed Entities (MEs) of the network) such as Self-Healing, Self-Organizing, Self-Optimizing, Self-Protection, Self-Repair, etc., and exhibiting Self-Awareness.

- Offer insights that help the Operator to create and launch new types of services that could be offered to customers based on the Recommendations that the Analytics performed by DEs in the Knowledge Plane can produce with respect to the types of services (e.g. connectivity services) that can be provisioned over the capacity deduced to be available without compromising QoE (Quality of Experience) of end users currently served by the network. The Recommendations should be based on converged and aggregate analytics that are collectively correlated by the various DEs in the Knowledge Plane over historical usage trends of the E2E network capacity and other information such as performance trending data, etc.

5. The GANA Knowledge Plane (KP) is meant to provide the realm in which Decision-making-Elements (DEs), as software, can be designed and implemented to perform and realize the following functions:

- Network Analytics should be performed in the Knowledge Plane (KP) using various types of algorithms for reactive and predictive analytics, including Machine Learning, Deep Learning, Computational Intelligence and others types of cognitive algorithms such as Artificial Intelligence (AI) algorithms, in augmenting any network analytics performed at systems and platforms such as Data Collectors that feed generated knowledge into the Knowledge Plane. Some cognitive algorithms may also run on the ONIX Information Servers for further correlation of information stored in the ONIX, to maintain an updated view on knowledge pertaining to current state of the network and also knowledge pertaining to historical network state and decisions performed by DEs as historical traces. The analytics performed by KP DEs drive maintenance operations and as well as even marketing campaigns (such value is also discussed in [i.26]). Sources such as [i.28][i.29], and many other sources in literature provide insights on data-sources for network analytics that can be performed on analytics platforms such as Data Collectors or at some management systems to generate some knowledge that can be supplied to the Knowledge Plane. The Knowledge Plane DEs can augment the knowledge by consolidating such knowledge and further performing aggregate analytics of information and knowledge from various input sources on a more global level. Cognitive algorithms discussed in [i.28] and many other sources on Knowledge Plane related topics, including results from research projects on autonomics and cognitive network management, and also some real implementations already achieved to some degree in the industry in the areas of Service Assurance and Big-Data Analytics Driven network management can also be applied in implementing the GANA Knowledge Plane and its interfaces described in [i.24].

- Complex Event Processing (CEP) techniques are employed by DEs in the Knowledge Plane, as discussed in [i.24].

- Data collected in the network by probes in the NEs or probes specially instrumented to collect data such as traffic captured through means such as link tapping, should be made available to the Knowledge Plane DEs for the purpose of enabling their algorithms to perform optimization and diagnostics.

6. The ONIX Information Servers and services may be employed for realizing a Real-Time Inventory.

7. The GANA KP should be aware and make of the following items:
- SLAs, for use in determining SLA Violations and autonomically programming the network in order to guarantee and sustain acceptable levels of QoS and QoE for user traffic
- Application policy/Profile profiles
- Network Service Designs/graphs

Other characteristics of the GANA Knowledge Plane: KP Multi-Tenancy may be required for some networking scenarios that require multi-tenancy in the management and control software responsible for portions, slices and administrative domains in the End-to-End network architecture.

5 Instantiation of the GANA model onto the BBF reference network and management & control architectures

5.1 BBF Reference architectures considered

The identification of the reference architecture for the BBF is based on BBF TR101: It provides an architectural/topological model of an Ethernet based aggregation network that supports the business requirements in TR-058. In doing so it describes requirements for protocol translation and interworking, QoS, multicast, security, and OAM for a DSL aggregation network.

The following picture shows the BBF reference architecture:

![Figure 2 Reference BBF architecture](image)

Moreover, TR-145 extends the TR-101 architecture with new technical requirements needed to fulfil the business requirements laid out in TR-144 Broadband Multi-Service Architecture and Framework Requirements. It defines an architectural framework based upon functional modules and the logical interfaces between them, the high-level common network service requirements as well as end-to-end operational functions, such as control and OAM. It focuses on the data plane between the T and A10 reference points and provides the interfaces and connectivity to Policy Control and Management Systems via interfaces across the R and M reference points, respectively. It results to a the generic Functional BBF model depicted in the following figure.
Figure 3: Generic Functional BBF model

6 Instantiation of GANA model concepts onto BBF architecture key functional entities

6.1 Introduction
## 6.2 General considerations derived from BBF Specifications

### 6.2.1 Requirements for autonomic features in BBF functional entities

The key requirements for autonomic features in BBF entities are summarised in the following tables namely, Table 1, Table 2 and Table 3. The tables refer to requirements extracted from BBF TR 101 [i.9], related to CPE, BNG and AN, respectively, and can be addressed/automated through autonomic means by DEs.

**Table 1: Identification of CPE related requirements [i.9]**

<p>| R1 | Bandwidth on Demand and QoS on demand can be supported by leveraging policy at the CPE. |
|    | Multicast upstream IGMP messages to all or a configured subset of the WAN interfaces. |
| R2 | Forward messages to all provisioned interfaces |
| R3 | Configure which ports are allowed to have IGMP hosts. |
| R4 | Configurable Customer maintenance domain level |
| R5 | Auto-configuration of CPE |
| R6 | All the Functional Entities of the node that require that Reactive and Proactive Resilience and Survivability must be reasoned about and handled on the node-level: Software/firmware image management Software module management Dual homing |
| R7 | Security and authentication of CPE with ACS/OSS/Service configuration, subscriber isolation |
| R8 | Diagnostics |
| R9 | Auto-configuration of CPE |
| R10 | Software/firmware image management Software module management Dual homing |
| R11 | Security and authentication of CPE with ACS/OSS/Service configuration, subscriber isolation |
| R12 | Diagnostics |
| R13 | Status and performance monitoring |
| R14 | Session Control - Connection request, Subscriber management function, Scheduling and Traffic Filtering function |
| R15 | Marking on tunnels, QoS Interworking between fixed and 3GPP networks, per customer QoS |
| R16 | VLAN management, multicast resource control, L1/L2 Adaptation and Forwarding |
| R17 | Multicast routing, selection of duplicate streams, separation of customer traffic |
| R18 | Dynamic service provisioning, service integrity, service instance tags used, traffic profiles, service association |</p>
<table>
<thead>
<tr>
<th>R1</th>
<th>Auto-configuration of DHCP relay (makes it possible for DHCP (responsible for broadcasting messages to be sent over routers that do not support forwarding of DHCP messages) on selected interfaces.</th>
</tr>
</thead>
<tbody>
<tr>
<td>R2</td>
<td>QoS support mechanisms: a) Hard partitioning of bandwidth among the Broadband Network Gateways; b) Distributed precedence and scheduling – mark services according to a Layer 2 precedence relationship so lower classes will be dropped under congestion; c) Hierarchical Scheduling (HS) within a BNG-allotted bandwidth partition.</td>
</tr>
<tr>
<td>R3</td>
<td>Policy Management. Configuration of RADIUS server.</td>
</tr>
<tr>
<td>R4</td>
<td>ARP processing. Configuration of “Local Proxy ARP” mode: routing IP packets received from host X on this interface to host Y (X and Y are in subnet Z) back via the same interface.</td>
</tr>
<tr>
<td>R5</td>
<td>Subscriber Session Establishment and Verification.</td>
</tr>
<tr>
<td>R6</td>
<td>Source IP spoofing: only respond to user ARP requests when they originate with the proper IP source address.</td>
</tr>
<tr>
<td>R7</td>
<td>Monitoring Tools and Mechanisms of the device: Status and performance monitoring</td>
</tr>
<tr>
<td>R8</td>
<td>Network Management: define constraints on the range of VLAN, auto-sense PPP/PPPoE as well as IPoE, auto-sense S-VLAN-tagged and C-VLAN-tagged frames Ethernet frames</td>
</tr>
<tr>
<td>R9</td>
<td>Support dynamic adjustment of the user-facing QoS shapers (Multicast)</td>
</tr>
<tr>
<td>R10</td>
<td>802.1.ad support</td>
</tr>
<tr>
<td>R11</td>
<td>multicast resource control , L1/L2 Adaptation and Forwarding</td>
</tr>
<tr>
<td>R12</td>
<td>Policy: ingress policing per: user, VLAN, session/flows</td>
</tr>
<tr>
<td>R1</td>
<td>Auto-configuration of the access nodes</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>R2</td>
<td>Auto-discovery of access nodes and other nodes</td>
</tr>
<tr>
<td>R3</td>
<td>Bulk provisioning (default configuration of customer ports)</td>
</tr>
<tr>
<td>R4</td>
<td>Ethernet interfaces configuration</td>
</tr>
<tr>
<td>R5</td>
<td>PON interfaces (DBA configuration)</td>
</tr>
<tr>
<td>R6</td>
<td>xDSL port (profiles configuration)</td>
</tr>
<tr>
<td>R7</td>
<td>Software upgrade</td>
</tr>
<tr>
<td>R8</td>
<td>Dual-homing</td>
</tr>
<tr>
<td>R9</td>
<td>Link-Aggregation</td>
</tr>
<tr>
<td>R10</td>
<td>ACL configuration &amp; traffic filtering (broadcast, mac address filtering &amp; flooding)</td>
</tr>
<tr>
<td>R12</td>
<td>Control-plane protection</td>
</tr>
<tr>
<td>R13</td>
<td>Diagnostics / Hardware fault detection and report</td>
</tr>
<tr>
<td>R15</td>
<td>Ethernet OAM</td>
</tr>
<tr>
<td>R16</td>
<td>Synchronization</td>
</tr>
<tr>
<td>R17</td>
<td>DHCP/PPPoE relay</td>
</tr>
<tr>
<td>R18</td>
<td>IGMP snooping/proxy for multicast forwarding</td>
</tr>
<tr>
<td>R19</td>
<td>Traffic classification</td>
</tr>
<tr>
<td>R20</td>
<td>Queue configuration (buffer allocation)</td>
</tr>
<tr>
<td>R21</td>
<td>MTU</td>
</tr>
<tr>
<td>R22</td>
<td>Auto-sensing of protocol encapsulation</td>
</tr>
<tr>
<td>R23</td>
<td>VLANs handling &amp; forwarding</td>
</tr>
<tr>
<td>R24</td>
<td>Multicast forwarding</td>
</tr>
<tr>
<td>R25</td>
<td>MPLS adaptation module</td>
</tr>
<tr>
<td>R26</td>
<td>Routing protocols</td>
</tr>
</tbody>
</table>
6.3 GANA instantiation onto BBF architectures

Following the main approach for the mapping of the GANA model onto BBF architecture, there is a high level view for the instantiation of the GANA Knowledge plane and network level DEs that can be depicted in the following Figure.

![Generic overview for the mapping of GANA to BBF architecture](image)

NOTE: The Reference Points on the diagram are defined in Clause 13 of ETSI GS AFI002 [xxx].

6.3.1 Instantiation (Mapping) of GANA DEs onto BBF key architecture

6.3.2 Enabling Autonomic behaviour of the CPE

In order to enable the CPE to exhibit autonomic capabilities, the mapping (instantiation) of GANA DEs at the node and function levels of abstraction of self-management functionality defined in GANA is required. The mapping follows the requirements analysis and links the GANA DEs to node operations, functions and managed entities (e.g., protocols) for the CPE node. The following table addresses the mapping.

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>The CPE Functions - Managed Entities (MEs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NODE_LEVEL_AC_DE – Node-Level Auto-Configuration Decision-Element</td>
<td>Auto-configuration of CPE</td>
</tr>
</tbody>
</table>
| NODE_LEVEL_R&S_DE – Node-Level Resilience & Survivability Decision-Element | All the Functional Entities of the node that require that Reactive and Proactive Resilience and Survivability must be reasoned about and handled on the node-level:
Software/firmware image management
Software module management
Dual homing |
Diagnostics |
| FUNC_LEVEL_MON_DE – Function-Level Monitoring Decision-Element | Initialization and control of the provisioning session flow. Session Control - Connection request, Subscriber management function, Scheduling and Traffic Filtering function
Marking on tunnels, QoS Interworking between fixed and 3GPP networks, per customer QoS |
| FUNC_LEVEL_GCP_M_DE – Function-Level provisioning decision-Element | VLAN management, multicast resource control , L1/L2 Adaptation and Forwarding |
| FUNC_LEVEL_QoS_M_DE – Function-Level Quality of Service-Management Decision-Element | Multicast routing, selection of duplicate streams , separation of customer traffic |
| FUNC_LEVEL_DP&FWD_M_DE – Function-Level DataPlane&Forwarding-Management Decision-Element | Dynamic service provisioning , service integrity , service instance tags used, traffic profiles , service association |
| FUNC_LEVEL_RT_M_DE – Function-Level Routing-Management Decision-Element | |
| FUNC_LEVEL_SM_DE – Function-Level Service-Management Decision-Element | |

The Autonomic CPE is depicted in the figure below.
6.3.4 Enabling the BNG to exhibit autonomic behaviours

In order to enable autonomic capabilities to the BNG the mapping of GANA DEs for node and functional level is required. The mapping follows the requirements analysis and links the GANA DEs to node operations, functions and managed entities (e.g., protocols) for the BNG node. The following table addresses the mapping.

Table 5: Mapping of GANA DEs to BNG node functions and managed entities

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>The BNG Functions - Managed Entities (MEs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NODE_LEVEL_AC_DE – Node-Level Auto-Configuration Decision-Element</td>
<td>Auto-configuration of BNG:</td>
</tr>
<tr>
<td></td>
<td>- DHCP Relay on/off</td>
</tr>
<tr>
<td></td>
<td>- ARP processing</td>
</tr>
<tr>
<td></td>
<td>- OAM messaging</td>
</tr>
<tr>
<td></td>
<td>- Configuring RADIUS Server</td>
</tr>
<tr>
<td></td>
<td>- Activating Control Policy</td>
</tr>
<tr>
<td></td>
<td>- Establishing Subscriber Sessions</td>
</tr>
<tr>
<td></td>
<td>- Deploying QoS</td>
</tr>
<tr>
<td></td>
<td>- Configuring Subscriber Features</td>
</tr>
<tr>
<td></td>
<td>- Verifying Session Establishment</td>
</tr>
<tr>
<td>NODE_LEVEL_R&amp;S_DE – Node-Level Resilience &amp; Survivability Decision-Element</td>
<td>Source IP spoofing: only respond to user ARP requests when they originate with the proper IP source address.</td>
</tr>
<tr>
<td>NODE_LEVEL_SEC_DE – Node-Level Security Decision-Element</td>
<td></td>
</tr>
</tbody>
</table>
### 6.3.5 Enabling the AN to exhibit autonomic behaviours

In order to enable autonomic capabilities to the access node (AN) the mapping of GANA DEs for node and functional level is required. The mapping follows the requirements analysis and links the GANA DEs to node operations, functions and managed entities (e.g., protocols) for the access node. The following table addresses the mapping.

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>The AN Functions - Managed Entities (MEs)</th>
</tr>
</thead>
</table>
| NODE_LEVEL_AC_DE – Node-Level Auto-Configuration Decision-Element | Auto-configuration of Access Nodes  
Auto-discovery of Access Nodes and others nodes  
Bulk provisioning  
Ethernet interfaces  
PON interfaces (DBA configuration)  
xDSL ports (profiles configuration) |
<table>
<thead>
<tr>
<th>Decision-Element</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NODE_LEVEL_R&amp;S_DE – Node-Level Resilience &amp; Survivability Decision-Element</strong></td>
<td>Software upgrade, Dual-Homing, Link Aggregation, RSTP/MSTP</td>
</tr>
<tr>
<td><strong>NODE_LEVEL_SEC_DE – Node-Level Resilience &amp; Survivability</strong></td>
<td>ACL configuration, Traffic filtering (broadcast, mac address filtering &amp; flooding), Control-plan protection</td>
</tr>
<tr>
<td><strong>NODE_LEVEL_FM_DE – Node-Level Fault-Management Decision-Element</strong></td>
<td>Diagnostic tools, Hardware faults detection and report</td>
</tr>
<tr>
<td><strong>FUNC_LEVEL_MON_DE – Function-Level Monitoring Decision-Element</strong></td>
<td>OAM, Synchronization</td>
</tr>
<tr>
<td><strong>FUNC_LEVEL_GCP_M_DE – Function-Level Generalized Control Plane-Management Decision-Element</strong></td>
<td>DHCP relay, PPPoE Relay, IGMP snooping/ proxy</td>
</tr>
<tr>
<td><strong>FUNC_LEVEL_QoS_M_DE – Function-Level Quality of Service-Management Decision-Element</strong></td>
<td>Traffic classification, Queue configuration (buffer allocation), MTU</td>
</tr>
<tr>
<td><strong>FUNC_LEVEL_DP&amp;FWD_M_DE – Function-Level DataPlane&amp;Forwarding-Management Decision-Element</strong></td>
<td>Auto-sensing of protocol encapsulation, VLANs handling, VLAN forwarding (1:1 or 1:N), MPLS Adaptation Module, Multicast forwarding, Routing protocols</td>
</tr>
<tr>
<td><strong>FUNC_LEVEL_RT_M_DE – Function-Level Routing-Management Decision-Element</strong></td>
<td></td>
</tr>
<tr>
<td><strong>FUNC_LEVEL_SM_DE – Function-Level Routing-Management Decision-Element</strong></td>
<td></td>
</tr>
</tbody>
</table>

The Autonomic AN is depicted in the figure below.
6.3.6 Use Cases for illustrating the value of autonomic features in BBF network elements

6.3.6.1 CPE: QoS interworking between fixed and 3GPP networks, marking of tunnels based on user-specific policy, network policy and QoS setting

A subscriber may want to use an application on his mobile device, while outside the Home Network, and then wishes to change the device he is using to a fixed Home Network attached device. A multimedia call is handed over from the mobility macro network to a home network, but instead of remaining on the same device, the user chooses to transfer the multimedia call to a Media Device connected to a large screen TV display and resumes the call on that device. Bandwidth and QoS is maintained for the large screen experience to be meaningful. Accounting and settlement is supported between the application and network service providers.

It is assumed that the IMS system will initially perform the necessary transfer of the initial UE session from the mobile access network to the Home Network (e.g., WIFI). The IMS Service Continuity procedures will be initiated.

In order to transfer the multimedia call to the Media device, Inter-UE Transfer procedures will be executed. In this case, the whole IMS multi-media session is transferred from one UE to the other UE with the support of CPE which will have to reallocate the flow to the new device.

CPE will have to:

- Consider the service profile and QoS requirements,
- Enable dynamic service provisioning, service integrity, by using service instance tags
- Correlate traffic profiles with service association
- Perform Session Control, Subscriber management, Scheduling and Traffic Filtering
- Perform Marking on tunnels, QoS Interworking between fixed and 3GPP networks, per customer QoS
6.3.6.2 BNG: BNG termination of PPPoE

The BNG allows hosts with private IP addresses to access the Internet. It mainly includes the following functions:

- Maintains the mapping from the private IP address to the public IP address (auto-configuration).
- Terminates PPPoE subscriber sessions with private IP address to public IP address to access Internet.

PPPoE has two phases, the discovery phase and the session phase:

- Discovery: The client identifies the servers which are available. To complete the phase the client and server must communicate a session-id. During the discovery phase all packets are delivered to the PPPoE control plane (FUNC_LEVEL_GCP_M_DE).
  - PPPoE Active Discovery Initiation (PADI). This packet is broadcasted and used by the client to search for an Access Concentrator (access server), providing access to a service.
  - PPPoE Active Discovery Offer (PADO): If the access server is able to provide the service it should respond with a unicast PADO message to signal the client. Multiple servers may respond and the client may choose a server to connect to.
  - PPPoE Active Discovery Request (PADR): After the client receives a PADO, this unicast packet will be used to connect to a server and request service.
  - PPPoE Active Discovery Session-confirmation (PADS) A server may respond to the client with this unicast packet to establish the session and provide the session-id. Once the PADS was provided the PPP phase begins.
- Session: Once the session ID is established connectivity is available for the duration of the session. Either client or server can terminate a session. During the life of the session the packets may be uniquely identified by the client’s MAC address and session-id. The session can terminate either by PADT sent by the client or server or by an LCP Terminate-Request packet.

6.3.6.3 AN: Configuration of the xDSL ports

DSL technologies are widely used to provide triple-play services including high-speed Internet, voice over IP and television over IP. These services are requiring more and more bandwidth and copper technology is pushed to its limits.

At the same time, quality of service (QoS) is one of the main concerns of telecom operators that must find a compromise between line performances and line stability knowing that copper line characteristics may change over time. This comprise is part of a global QoS policy that is defined by each operator and that may also change over time.

As a consequence, DSL profiles applied to each DSL port of access nodes may have to be changed from time to time. This action may be done automatically by access nodes according to both line characteristic and global QoS policies.

NB: Changing DSL profiles leads to a desynchronization and resynchronization of the DSL modem. During this time, triple-play services are not available for the customers. As a consequence, this modification must be done at the most appropriate moment of the day.

AN should perform the following in an autonomic fashion:

- Analyse the stability of each xDSL line
- Choose the best profiles according to global QoS policies (stability vs performances)
- Analyse port traffic statistics in order to determine the most appropriate moment for the modifications.
- Apply the new policy at the most appropriate moment for the modification to be transparent for the customers

6.3.6.4 AN: Buffer configuration

Quality of service (QoS) is one of the main concerns of telecom operators and latency, throughput and packet loss are key performance indicators. Some services require low latencies and can support packets loss. Other services can support bigger latencies but throughput can decrease dramatically in case of packet loss.

In order to ensure a good quality of service, QoS policies (including buffer configuration) must be enforced in the network in an end-to-end approach depending on each service requirements.

AN should perform the following in an autonomic fashion:

- Determine the type of traffic that goes into each queue on each interface
- Communicate with other devices in the network in order to have an end-to-end buffer configuration policy
- Configure buffer size per queue depending on services requirements and global network QoS policy

7 GANA instantiation onto the virtualised BBF architecture with SDN

7.1 Introduction

The BBF SDN enabled architecture and the BBF and ETSI NFV architectures are addressed in the context of instantiating the GANA model features into the respective virtualized component architectures. The concepts are aligned with the Unified Architecture for the ETSI GANA Model, SDN, NFV, E2E Service Orchestration, Network Analytics, and Big-Data Analytics for Autonomics that is discussed in the ETSI White Paper No.16, which offers insights on the integration of the GANA with these paradigms (readers are encouraged to learn more details on this subject in the more elaborate work being done in ETSI NTECH AFI on this subject). The following diagram is one of the diagrams that show how GANA integrates with the other emerging paradigms, but the focus here is on depiction of where Autonomic Functions (Decision Elements) can be introduced in the ETSI NFV Architectural Framework.
Figure 7 Introduction of GANA Autonomic Functions (Decision Elements) in the ETSI NFV Architectural Framework
7.2 GANA instantiation onto the BBF and ETSI-NFV reference model for infrastructure interworking

Figure 8 BBF and ETSI-NFV reference model for infrastructure interworking

Figure 8 illustrates a combination of the BBF and ETSI-NFV architectures where the services are hosted in NFVI that has deployed a BBF specified multiservice broadband network. On this scenario, the infrastructure layer(s) will typically be a combination of MPLS and Ethernet augmented with datacenter overlay protocols (e.g., VxLAN) in the services infrastructure domain (e.g., NFVI). The network function view of the network service layer is assumed to be IP based with the selection of the corresponding forwarding graph of the network service layer. As TR-359 indicates, the diagram does not account for when NFVI deployments span BBF reference points (i.e., A10, V, U, T). In addition, a NFVI-PoP can exist between reference points (e.g., between U and V).

Figure 9 shows an example of Network Enhanced Residential Gateway (NERG) architecture deployed on top of ETSI NFV architecture.

Figure 9 NERG Example (Home Virtualization)

The reference models of the BBF and ETSI NFV can be combined such that the functional components and reference points of the BBF TR-145 and TR-134 reference models and ETSI NFV reference model are depicted for the
management and control of Services along with the interworking of the user/data plane of the BBF reference models with the infrastructure (NFVI) layer of the ETSI NFV reference model.

With the intention of GANA instantiation, in Figure 10, the Managed Entities (MEs) of both BBF and NFV architectures are identified and GANA Network Level and GANA Node Levels MEs are illustrated.

![Figure 10 BBF and ETSI-NFV reference model for service management and control](image)

### 7.2.1 BBF Managed Entities (MEs)

In this section, we will describe the BBF MEs and their being assigned to specific GANA DEs to enable DE developers to identify DE to MEs mappings in order to innovate and develop DE algorithms that dynamically and collaboratively manage and control MEs.

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>Auto configuration server (ACS) Managed Entities (MEs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACS NODE <em>LEVEL</em> AC DE</td>
<td>The first time a BRG contacts the operator’s network, not all of the functions associated with the NERG may be activated on the BRG and within the vG. As such, when the BRG contacts the ACS for the first time, the ACS informs the NERG management system which then may activate additional functions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>Authentication Authorization and Accounting (AAA) Managed Entities (MEs)</th>
</tr>
</thead>
</table>
AAA NODE_LEVEL_SEC_M_DE

AAA is used in NERG architecture at different nodes and for different purposes:

- At the MS-BNG:
  - in the case of the Flat Ethernet LSL, to extend the subscriber’s access VLAN to the vG_MUX, by dynamically cross-connecting the Access-VLAN to an L2 network resource such as a VxLAN, an MPLS pseudo-wire or an Ethernet over GRE tunnel,
  - in the case of the Overlay Ethernet LSL, to provide the BRG with the necessary tunneling information via DHCP to allow the BRG to connect to vG_MUX. In this case, the tunneling information is encoded in a set of new RADIUS Attributes and translated into a set of DHCP options.

- At the vG_MUX:
  - to extend the LSL from the vG_MUX to the subscriber’s vG, the LSL being either a Flat Ethernet LSL or an Overlay LSL.

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>Policy Managed Entities (MEs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy NODE_LEVEL_SEC_M_DE</td>
<td>For the offering of per device services and policy management (e.g. per device QoS or steering). Out of scope in TR-317.</td>
</tr>
</tbody>
</table>

7.2.2 NFV Managed Entities (MEs)

In this section, we will describe the NFV ME and their relationship with GANA DEs.

7.2.2.1 Overview of the Mapping of GANA model to ETSI NFV MANO

Figure 11 depicts this mapping. The DEs of the GANA Knowledge Plane are autonomic functions (AF) that are supposed to autonomically manage and control the Managed Entities (MEs) that determine the services of a network node (e.g. a VNF or PNF), e.g. its protocols/stacks instances and/or other functional entities and their configurable parameters. That means GANA Knowledge Plane DEs can be loaded or integrated as modules of an EMS or implemented as part of EMS or OSS in general. EMS and OSS vendors may offer an interface through which GANA Knowledge DEs (as customized or second party control logics that embed autonomics-enabling algorithms) can be loaded or integrated to introduce/enhance autonomies capabilities of the EMS or OSS. Other than DEs, the other GANA Knowledge Functional (FBs) such as ONIX and MBTS, may also be implemented and integrated in order to take advantage of the functions they offer in an autonomic network. Autonomics (AMC) on the Orchestrator Level, VNFMaanger level, VIM Level [i.35].
Table 8 provides a global picture of GANA mapping to ETSI NFV MANO architecture with the instantiation of autonomic functions (AF). It includes the following four perspectives:

- Autonomies at ETSI MANO level
- GANA DE role in terms of performing analytics, creating and executing plans of actions wrt Managed Entities (ME)
- ETSI MANO lower level Components involved (Managed Entities)
- Autonomic Control-loop’s operating region (decision making coverage)
### Table 8: Diagram of the Mapping of GANA model to ETSI NFV MANO

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>NFV-O Managed Entities (MEs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data_Plane_and_Forwarding_Management_DE</td>
<td>Service Function Chaining, across multiple network applications</td>
</tr>
<tr>
<td>Security_Management_DE</td>
<td>Tenant session management.</td>
</tr>
<tr>
<td>QoS_Management_DE</td>
<td>Generates, maintains and tears down network services of VNF themselves. If there are multiple VNFs, orchestrator will enable creation of end to end service over multiple VNFs.</td>
</tr>
</tbody>
</table>

---

### 7.2.2.2 Overview of the Mapping of GANA model to ETSI NFV MANO

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>VIM Managed Entities (MEs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSS</td>
<td>GANA Knowledge Plane (KP) Decision Elements (DEs) are modules that perform the analytics</td>
</tr>
<tr>
<td>EMS</td>
<td>GANA Knowledge Plane (KP) Decision Elements (DEs) are modules that perform the analytics</td>
</tr>
<tr>
<td>VNF</td>
<td>GANA-Level-2 and Level-3 Decision Elements (DEs) instrumented in the VNF</td>
</tr>
<tr>
<td>NFVO</td>
<td>GANA-Network-Level Decision Element (DE) (NFVO-DE as module that is part of Orchestrator SW and is controlled and augmented by GANA KP DEs’ algorithms)</td>
</tr>
<tr>
<td>VNFM</td>
<td>GANA-Network-Level Decision Element (DE) (VNFM-Manager-DE as module that is part of VNFMManager SW)</td>
</tr>
<tr>
<td>VIM</td>
<td>GANA-Network-Level Decision Element (DE) (VIM-DE as module that is part of VIM SW)</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>GANA-Network-level Decision Element (DE) (Hypervisor-DE as module, part of Hypervisor SW)</td>
</tr>
</tbody>
</table>
7.3 GANA instantiation onto Network Enhanced Residential Gateway

In TR-317 and TR-359, the residential or customer related node is addressed by the respective SDN and NFV enhanced node, thus called Network Enhanced Residential Gateway or virtual (Business) Gateway.

BBF architectures have typically focused on nodal requirements and geographically sensitive deployments. This is a consequence of the physics of broadband access transmission media. As such, although virtualization is driving both nodal and geographic deployment independence, specific nodes do not go away on the overall architecture, hence the inclusion of the access node and residential gateway/CPE.

The NERG concept involves moving some of the networking and service-related functions from the RG to the NSP’s network. The distribution of functions effectively splits the RG into 2 sets of connected functional components as depicted in figure 6.

In this context, the physical node BRG: Bridged Residential Gateway – this is the CPE still located at the residential customer premises, configured as a managed bridge connecting its LAN interfaces and the BRG-LSL interface. The separation of logical functions which are operational in the virtualized part provide the main alternative deployments for the vG. The main alternative deployments – use cases are addressing the placement of the vG either “closer” to the BRG in the network nodes (e.g., close to the AN), or further to the network e.g., a cloud infrastructure.

These alternative use cases are shown in Figure 13.
The main BRG capabilities are depicted in the Figure 14.

![Figure 14: BRG NERG capabilities](image)

The main vG capabilities are depicted in Figure 15.
For the GANA instantiation onto the NERG components, the main autonomic capabilities are split between the BRG and vG. The split is depicted in Table 9.

**Table 9: Separation of autonomic features and capabilities between BRG and vG**

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>The NERG Functions - Managed Entities (MEs)</th>
<th>vG</th>
<th>BRG</th>
</tr>
</thead>
<tbody>
<tr>
<td>NODE_LEVEL_AC_DE – Node-Level Auto-Configuration Decision-Element</td>
<td>Auto-configuration of CPE</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>NODE_LEVEL_R&amp;S_DE – Node-Level Resilience &amp; Survivability Decision-Element</td>
<td>All the Functional Entities of the node that require that Reactive and Proactive Resilience and Survivability must be reasoned about and handled on the node-level: Software/firmware image management, Software module management, Dual homing</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Decision-Element</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NODE_LEVEL_FM_DE – Node-Level Fault-Management Decision-Element</td>
<td>Diagnostics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUNC_LEVEL_MON_DE – Function-Level Monitoring Decision-Element</td>
<td>Monitoring Tools and Mechanisms of the device - Status and performance monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUNC_LEVEL_GCP_M_DE – Function-Level Generalized Control Plane-Management Decision-Element</td>
<td>Initialization and control of the provisioning session flow, Session Control - Connection request, Subscriber management function, Scheduling and Traffic Filtering function</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUNC_LEVEL_QoS_M_DE – Function-Level Quality of Service-Management Decision-Element</td>
<td>Marking on tunnels, QoS Interworking between fixed and 3GPP networks, per customer QoS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUNC_LEVEL_DP&amp;FWD_M_DE – Function-Level DataPlane&amp;Forwarding-Management Decision-Element</td>
<td>VLAN management, multicast resource control, L1/L2 Adaptation and Forwarding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUNC_LEVEL_RT_M_DE – Function-Level Routing-Management Decision-Element</td>
<td>Multicast routing, selection of duplicate streams, separation of customer traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUNC_LEVEL_SM_DE – Function-Level Service-Management Decision-Element</td>
<td>Dynamic service provisioning, service integrity, service instance tags used, traffic profiles, service association</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Finally, Figure 16 and Figure 17 depict the mapping of the GANA DEs to NERG (BRG – vG). The figures illustrate the GANA Level-3 and Level-2 DEs that add value in the depicted NEs. The two figures correspond to two different options regarding the role of the GANA Knowledge Plane in the Management and Control Systems, namely:

Option 1: Knowledge Plane external to the legacy management and control systems EMS/NMS/OSS (Figure 16)

Option 2: Knowledge Plane as integrated within the management and control systems (Figure 17).
Figure 16: GANA instantiation on SDN/NFV architecture for NERG – Option 1 (KP external to the legacy management and control systems)
Following the main alternative use case deployments for NERG, the mapping of the GANA knowledge plane is addressed. The main GANA Knowledge Plane covers all the network segments operated by the operator. In this case the Knowledge Plane can access all the infrastructure network elements (VNFs or PNFs) without any administrative constraints and can also policy lower level GANA DEs instrumented in the network elements. In this case the knowledge plane interoperates with the vG on the cloud. The other alternative deployment encompasses the instantiation of relevant knowledge closer to the customer premises, e.g., interacting with the vG deployed at the AN.
7.4 GANA instantiation onto Software-Defined Access Network (SDAN)

7.4.1 Towards Autonomic SDAN

NOTE: The operations of the DEs should be seen as some degree of self-management intelligence delegated to the SDAN network element (data plane network node) that should complementarily and harmoniously interwork with the logically centralized management & Control Programmatic Operations and Policy control operations performed by either the GANA Knowledge Plane’s Decision Elements (DEs) and/or by an SDN Controller towards the network infrastructure element(s). The logically centralized GANA Network-Level DEs in the GANA Knowledge Plane complementarily interwork with DEs instantiated on the node-level in the infrastructure elements as described in [i.24] and [i.25]. For example the Network-Level Fault-Management-DE in the Knowledge Plane complements the Node-Level Fault-Management, as discussed in [i.13][i.14][i.15][i.16]. But DE algorithm developers have a choice on whether an algorithm is better implemented using “in-network DE-to-DE” collaborations through the horizontal peer DE-to-DE reference points defined in the GANA Model or solely through a combination of centralized algorithm implemented by the collaboration of a DE in the Knowledge Plane and one embedded in network element(s). The Knowledge Plane DEs should have the freedom to drive management & control systems such as the SDN controller, for some operations that program the Network Element, while also being able to dynamically perform policy-control of the lower level DEs in the Network Element using a policy control protocol (NOTE: ETSI NTECH AFI WG is still looking into candidate protocols that can be used for this purpose).

Software Defined Networking (SDN) separates the control and data planes to enable coordinated, intelligent control of network resources.

WT-358 introduces SDN concept into existing access nodes equipment by specifying the SDN-based nodal requirements necessary to satisfy existing requirements documented within BBF TRs including TR-101i2, TR-178, and TR-301. This will enable the implementation and deployment of more flexible and less complex access nodes and increase the rapidity of the introduction of new feature.

Based on one of SDN principles of separation of the forwarding plane and control plane, WT-358 illustrates SDAN as shown on Figure 19.

![Figure 19: SDAN High Level design](image)

Control plan of the access node is implemented into a SDN controller whereas forwarding plane remains into the access node. Control and Management interfaces are defined to communicate between both planes. The Openflow protocol
specified by ONF can be used for the control interface between the access nodes and the SDN controller. The Netconf described in IETF RFC 6241 can be used for the management interface between the access nodes and the SDN controller.

WT-358 illustrates more precisely the implementation of SDAN by defining a set of components that can be localized in the SDN controller or externalized into the physical access node:

- SDN Agents, including an OpenFlow agent for the forwarding plane provisioning and performance management (counters), and a NETCONF agent for other provisioning including FCAPS.
- ANLC functions. An SDN controller may delegate control functions to an SDAN network element, those functions may include STP, LACP, ERPS, OAM, etc.
- ANEC functions. An SDN controller also has the option to run control protocols itself. For example, IGMP processing, DHCP relay, 802.1X Authenticator, etc.
- Forwarding Plane. It filters and forwards packets. Traffic classification, VLAN tagging and QoS are part of the forwarding plane functions.
- Non-traffic related FCAPS. It includes classic functions such as equipment inventory, software upgrade, etc.

Based on this detailed design and the mapping of GANA DEs to AN node functions and managed entities, the main autonomic capabilities can be split between the SDN controller and the SDAN Network Element as follows.

**Table 10: Separation of autonomic features and capabilities between SDAN Network Element and SDN Controller**

<table>
<thead>
<tr>
<th>Decision Element (DEs)</th>
<th>The AN Functions - Managed Entities (MEs)</th>
<th>SDAN Network Element</th>
<th>SDN Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>NODE_LEVEL_AC_DE – Node-Level Auto-Configuration Decision-Element</td>
<td>Auto-configuration of Access Nodes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Auto-discovery of Access Nodes and others nodes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bulk provisioning</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Ethernet interfaces</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PON interfaces (DBA configuration)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The mapping of the GANA DEs to SDAN can be done in two different ways:

The first solution is depicted on Figure 21 and show the mapping of GANA DE to SDAN according to Table 10: . This approach can be seen as a first option for implementing GANA model into SDN-based architecture.
The second option is depicted on Figure 22 and shows the mapping of GANA “ANEC-related” DE on top of the SDN controller. This second approach introduces no impact on the SDN controller. “ANEC-related” DE are implemented in the knowledge plane and interact with the SDN controller through its northbound interface.
7.4.3 Further Complementary Details on Autonomic SDAN Network Element: DEs and MEs Mappings and Characterization

Table 11: DEs and their mappings to Self-* operations and the DE mappings to Managed Entities (MEs) autonomically orchestrated or managed by their corresponding DEs

<table>
<thead>
<tr>
<th>Decision Element (DE)</th>
<th>Self-* realized by the DE</th>
<th>Category of Management aspect addressed by the DE via autonomic means</th>
<th>Managed Entities (MEs) autonomically orchestrated or managed by the DE</th>
<th>Example Data Sources for the DE(s)</th>
<th>Remarks and additional aspects for consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node-Level Fault-Management-DE</strong></td>
<td>Self-Diagnosis, Self-Repair and Self-Healing on Component, Module or System Level during the long term operation of the Network Element (NE) as described in Fault Management part of FCAPS</td>
<td>Mechanisms or Tools dynamically applicable for Fault-Detection, Fault-Localization (Diagnosis) and Fault-Removal</td>
<td>Tools (e.g. monitoring tools) and all entities in the node that can communicate events related to manifestations of faults, errors, failures in the node or in the network</td>
<td>Interworks with the Network-Level Fault-Management-DE implemented in the Knowledge Plane</td>
<td></td>
</tr>
<tr>
<td><strong>Node-Level Resilience &amp; Survivability-DE</strong></td>
<td><strong>Fault Management part of FCAPS</strong></td>
<td><strong>Configuration Management part of FCAPS</strong></td>
<td><strong>Knowledge Plane</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto-Remediation and Reactive &amp; Proactive Self-Healing on Service Level by applying protection and restoration techniques and strategies, while at the same time interworking with the Fault-Management DE to implement Self-healing strategies on the node level as described in [i.13][i.14][i.15][i.16].</td>
<td>Mechanisms and Tools dynamically applicable for remediation or self-healing of services and for global node resilience to faults/Errors/Failure manifestations in the node or the network</td>
<td>Function-Level DEs and any other entities in the network element that need to be bootstrapped or (re)-configured in response to policy changes and workload changes. Function-Level DEs receive policies from the Knowledge Plane via the Auto-Configuration-DE.</td>
<td>Knowledge Plane DEs, MBTS, ONIX, local DEs; Agents such as SDN Agents (OpenFlow Agents, NETCONF Agents, Legacy Management Agents) may export operational state information such that it is accessible to the DE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To ensure policy consistent network resources configuration, the Auto-Configuration-DE needs to be aware of all configuration agents (e.g. SDN Agents, Legacy Management Agent, etc.) operating in the network element. The Auto-Configuration-DE should have access to configuration event that is to occur or has occurred on the network element through a local agent, and may need to access the configuration.
<table>
<thead>
<tr>
<th><strong>Node-Level Security Management-DE</strong></th>
<th><strong>Self-Protection of the node/element.</strong></th>
<th><strong>Security Management part of FCAPS</strong></th>
<th><strong>Knowledge Plane's Security Management DE may dynamically policy control the Node-Level Security Management-DE.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> Principles for designing autonomic Security management based on the GANA as described in [i.17]/[i.18] can be applied to designing the Security Management-DE(s), while taking into account various security aspects in SDN (e.g. using sources such as [i.23]).</td>
<td>Mechanisms and Tools dynamically applicable for Security Threats-Detection and Self-Protection of the node and possibly for network wide self-protection via the collaboration of Node-Level Security-Management DEs. Traffic Filtering Mechanisms may be employed by the DE during it attempts to block suspicious traffic, and also some security mechanisms such as tunneling mechanisms may be dynamically employed by the DE the security enforcement of the node.</td>
<td>The Security Management-DE may require intercepting (or acting proxy for) certain communications with the outside world (and this may include from the SDN controller) when self-protection and self-defending algorithms of the DE require it to do so. The DE may apply traffic filtering rules on the interfaces of the network element upon security threat detection and re-adjust traffic filtering rules accordingly. This behavior may be enforced by Security-Management-DE in the Knowledge Plane. The DE may be required to...</td>
<td></td>
</tr>
<tr>
<td><strong>Function-Level QoS &amp; Performance Management-DE</strong></td>
<td><strong>Self-Configuration of QoS guaranteeing mechanisms:</strong> Self-Optimization of QoS guaranteeing mechanisms taking into consideration workloads, traffic volume and state of the node and the service impacting factors derived from network conditions.</td>
<td><strong>Performance Management part of FCAPS</strong></td>
<td>QoS guaranteeing mechanisms such as Traffic Classifiers, Traffic shaping, Queuing, DiffServ Packet (Re-)Marking, bandwidth allocation adjustments, etc.</td>
</tr>
<tr>
<td>Management-DE(s)</td>
<td>Performance</td>
<td>Knowledge Plane’s Monitoring DE as it may supply new policies that guide the way the DE should operate</td>
<td>Interworks with the Network-Level Monitoring-DE implemented in the Knowledge Plane</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Function-Level Monitoring-DE** | **Self-Configuration of monitoring mechanisms and mechanisms or tools for monitoring data formatting and dissemination to consumer entities such as (local or remote);**  
**Self-Optimization of monitoring behaviors and tools, and data dissemination methods, frequency, etc.** | **Principles for designing autonomic monitoring based on the GANA as described in [i.19][i.20][i.21] can be applied to designing the Monitoring DE(s).** |                                                                 |
| **Function-Level Data Plane & Forwarding Management-DE** | **Self-Configuration and Adaptive Re-Configuration of Access Node Localized Control (ANLC) functions based on operator policies or management and control inputs supplied by the external management and control systems (e.g. SDN Controller)** | **Management of the Access Node Localized Control (ANLC) functions that may be delegated by the SDN controller to run in the SDAN network element, and such functions may include STP, LACP, ERPS, OAM, etc. [i.32].** | **Interworks with the Network-Level Generalized-Control-Plane Management-DE implemented in the Knowledge Plane** |
| **Performance Management part of FCAPS** | | **Various data sources (including local data sources within the SDAN network element) that the DE algorithm developer/innovator may want to use** | |
Dynamic (Autonomic) Management and Control aspects addressed by the DataPlane & Forwarding Management-DE:

- **Dynamic (Autonomic) Management of LACP** forwarding based on local and/or network events and at the same time in respect of the external governing policies enforced by a management and control system such as the SDN-Controller or the Knowledge Plane. The DE algorithm developer may use any Managed Objects (MOs) defined for the LACP to determine what could be dynamically (autonomically) configured/adjusted for LACP’s operation to achieve a certain goal by virtue of the DE algorithm innovation. Such dynamic management performed by the DE may be based on various data sources (including local data sources within the SDAN network element). The MOs that the DE designer may consider in designing the DE may come from the corresponding MIBs (Management Information Bases) available for LACP.

- **Dynamic (Autonomic) Management of STP** based on local and/or network events and at the same time in respect of the external governing policies enforced by a management and control system such as the SDN-Controller or the Knowledge Plane. The DE algorithm developer may use any Managed Objects (MOs) defined for the STP to determine what could be dynamically (autonomically) configured/adjusted for STP’s operation to achieve a certain goal by virtue of the DE algorithm innovation. Such dynamic management performed by the DE may be based on various data sources (including local data sources within the SDAN network element). The MOs that the DE designer may consider in designing the DE may come from the corresponding MIBs (Management Information Bases) available for STP.

- **Dynamic (Autonomic) Management of ERPS** based on local and/or network events and at the same time in respect of the external governing policies enforced by a management and control system such as the SDN-Controller or the Knowledge Plane. The DE algorithm developer may use any Managed Objects (MOs) defined for the ERPS to determine what could be dynamically (autonomically) configured/adjusted for ERPS’s operation to achieve a certain goal by virtue of the DE algorithm innovation. Such dynamic management performed by the DE may be based on various data sources (including local data sources within the SDAN network element). The MOs that the DE designer may consider in designing the DE may come from the corresponding MIBs (Management Information Bases) available for ERPS.

7.4.2 Characterization of the GANA Knowledge Plane instantiated for SDAN

1. Example Autonomic Management & Control (AMC) Use Cases that can be implemented by DE algorithms in the Knowledge Plane in dynamic management operation performed adaptively by the responsible DEs during the network operation phase, after the initial configuration of the aspects (Managed Entities) by either the Knowledge Plane or by other types of management and control systems in place to interwork with the Knowledge Plane:

   - Dynamic (Self-) Optimization of the physical layer configuration of the broadband connection, for example by changing parameters such as data rates and power levels

   - Dynamic Access network control by the Knowledge Plane DEs in collaboration with any management and control systems in place to interwork with the Knowledge Plane by being driven by the Knowledge Plane layer involves dynamic (self-adaptive) configuration of e.g. Network Elements (NEs) access nodes, thereby adapting the physical layer configuration parameters such as data rates, transmitted power and spectrum, coding schemes, resilience to noise, and latency, based on various factors such as challenges in the network environment and policy changes by the Operator, etc. ([i.26] ASSIA SDAN White Paper provides insights on this subject of examples of configurable parameters).
• Dynamic application of maintenance profiles (see in [i.26]) in adherence to operator's policy should be automated by DEs in the Knowledge Plane. Knowledge Plane DEs can perform profile optimization relying on historical and current data about a subscriber line, and taking into account for the line’s service profile as discussed in [i.26].

• Access Network Diagnostics (discussed in sources such as [i.26]) should be performed by the Fault-Management-DE in the Knowledge Plane, and the Knowledge Plane should help resolve service issues and compute remedial strategies and apply them for self-healing of services automatically, and other automations should also be performed by the Knowledge Plane DE algorithms, e.g., automated maintenance and upgrades of the access nodes. The Fault-Management-DE performs Root-Cause Analysis (RCA) and computes self-healing and self-repair strategies that it then applies to the Managed Entities (MEs) in the Network Elements (NEs) that should be effected ((re-)orchestrated or (re-) configured) to help eradicate the problem/fault or reduce its impact on services by invoking remediation strategies in collaboration with other DEs.

• SDAN Diagnostics and Producing Recommendations as discussed in [i.26] should also be performed by the Fault-Management-DE in the Knowledge Plane. The types of Recommendations discussed in [i.26], should be produced by the Knowledge Plane DEs, and may “include the identification of upsell opportunities” as discussed in [i.26].

NOTE/Remark: The Knowledge Plane DEs should also dynamically policy (perform policy control of) the lower level GANA DEs instrumented in the network elements (VNFs or PNFs), e.g., CPE, AN, BNG, to complement and tune the autonomic behaviors realized at the lower GANA levels (within the network elements).

2. Impact of some SDAN Scenarios on the nature, multiplicity and responsibilities desired of the GANA Knowledge Plane (KP) instances that should be operated in the various scenarios, and the relationships of the specific Knowledge Plane instances with the Network Elements (NEs) that should be under the control of a specific Knowledge Plane instance. The following scenarios are taken from [i.26][i.30][i.31], and more scenarios and more details are expected to be published by BroadBand Forum (BBF) in Access Virtualization and Fixed Access Network Sharing (FANS) related documents:

• Scenario 1: Single Operator SDAN

Knowledge Plane (KP) characterization: Only a single Knowledge Plane instance may be required to cover all the network segments operated by the operator. In this case the Knowledge Plane can access all the infrastructure network elements (VNFs or PNFs) without any administrative constraints and can also policy lower level GANA DEs instrumented in the network elements. The Data Sources for the Knowledge Plane are for example VNF’s data, VNFM, VIM, SDN controller, Service Orchestrators, OSS, Performance Management Systems, Data Collectors, Probes, Information shared through ONIX, etc.; if such data sources can be available to the Knowledge Plane. ONIX, a distributed scalable overlay system of information servers and being a part of the Knowledge Plane, should also be instantiated to serve as Real-Time Inventory for various types of information. The ONIX would be useful for enabling auto-discovery of information/resources of an autonomic network via its “publish/subscribe/query&find” protocols. Databases in the Broadband network can be treated as members of ONIX if their information they store could be desirable to have it consumed through the “publish/subscribe/query&find” paradigm and protocols employed by ONIX. DEs can make use of ONIX to discover information and entities (e.g., other DEs) in the network to enhance their decision making capability.

• Scenario 2: Multiple Operator SDAN

Knowledge Plane (KP) characterization: Sub-Scenario (a): The Knowledge Plane can be implemented as an integral part of a multi-tenant management & control system that serves the needs for all the operators involved (including the Virtual Network Operators) and caters for configuration, diagnostics and remediation functions of all connections in the access network as discussed in [i.26], a scenario in which management functions are implemented by the Multi-tenant Management System. In such a scenario the Knowledge Plane may have to rely only on the management and control mechanisms available in the multi-tenant management system and not available through an OSS owned by a Virtual Network Operator, to dynamically adapt the configuration of the network services and connections
Whenever it determines to do so. The multi-tenant management & control system may be made to run
in a virtualized environment. The Knowledge Plane may run as multiple instances and as independent
owners for specific Virtual Network Operators operating in the shared access network. A means to
enable the Knowledge Plane (integrated as part of a multi-tenant management and control system) to
access all the infrastructure network elements (VNFs or PNFs) without any administrative constraints
should be put in place, as the Knowledge Plane DEs may also dynamically policy the lower level GANA
DEs instrumented in the network elements. The Data Sources for the Knowledge Plane are for example
VNF’s data, VNFManager, VIM, SDN controller, Service Orchestrators, Performance Management
Systems, Data Collectors, Probes, Information shared through ONIX, etc., if such data sources can be
available to the Knowledge Plane. The ONIX part of the Knowledge Plane should also be instantiated
to serve as Real-Time Inventory for various types of information and should complement any databases
that may be used.

**Sub-Scenario (b):** Multiple Knowledge Plane instances, whereby a Virtual Network Operator (VNO)
has a Knowledge Plane instance (VNO Knowledge Plane) associated and attached to the management
and control systems (including the OSS) dedicated to the VNO, and the Physical Infrastructure Provider
has a Knowledge Plane instance (Physical Infrastructure Provider Knowledge Plane) associated and
attached to the management and control systems (including the OSS) dedicated to the Physical
Infrastructure Provider. Such management and control systems may be implemented outside an Access
Virtualization System as discussed in [i.26]. A means to enable the individual Knowledge Plane
instances to access the infrastructure network elements (VNFs or PNFs) that should be under their
control without any administrative constraints should be put in place, as Knowledge Plane DEs may
also dynamically policy the lower level GANA DEs instrumented in the network elements. The VNO
Knowledge Plane and Physical Infrastructure Provider Knowledge Plane may need to be federated
such that they coordinate their operations if their collaborative behaviors can effect a global self-
optimization of network resources. The ONIX part of the Knowledge Plane should also be instantiated
to serve as Real-Time Inventory for various types of information and should complement any databases
that may be used. The ONIX Information servers owned by the different players may also need to be
federated to form a global ONIX system. The Data Sources for the Knowledge Plane are for example
VNF’s data, VNFManager, VIM, SDN controller, Service Orchestrators, OSS, Performance
Management Systems, Data Collectors, Probes, Information shared through ONIX, etc., if such data
sources can be available to the Knowledge Plane.

**Scenario 3: SDAN to the Home**

**Knowledge Plane (KP) characterization.** In having to management that is extended into the home
network and is made to include end-user customer experience involving user access to OTT services as
discussed in [i.26], the characterization of the Knowledge Plane may take similar nature to the KP in
the scenario involving Multiple Operator SDAN. In such a scenario, the Knowledge Plane can be
implemented as an integral part of a multi-tenant management & control system that serves the needs
for all the operators involved (including the Virtual Network Operators) and caters for configuration,
diagnostics and remediation functions of all connections in the access network as discussed in [i.26], a
scenario in which management functions are implemented by the Multi-tenant Management System. In
the case of extending management into the home network, probes instrumented in the home network
should disseminate performance data collected across networking devices owned or controlled by
multiple service providers as discussed in [i.26]. The Knowledge Plane DEs as an integral part of the
multi-tenant management system can either produce recommendations that enable VNOs to control and
optimally configure the access network, while at the same time the Knowledge Plane DEs, in a “closed
loop” fashion autonomically apply the recommendations to realize self-optimization as autonomic
objective. Data fusion that spans CPEs and Wi-Fi access points that may have been deployed by
different service providers should enable the Knowledge Plane DEs (a process orchestrated and driven
by the Fault-Management-DE) to perform Root Cause Analysis (fault correlation/diagnosis/localization) to resolve the faults (root causes) that commonly affect multiple end
users serviced by the different access points. The ONIX part of the Knowledge Plane should also be
instantiated to serve as Real-Time Inventory for various types of information and should complement
any databases that may be used.

The Data Sources for the Knowledge Plane are for example End-user management systems that gather
data exported by monitoring probes/agents instrumented in the home network and OTT service data
and export such data to the Knowledge Plane part of the multi-tenant management system, as we well
as VNF’s data, VNF Manager, VIM, SDN controller, Service Orchestrators, OSS, Performance
Management Systems, Data Collectors, Probes (e.g. passive probes) gathering network traffic data, etc., if such data sources can be available to the Knowledge Plane.

8 E2E Value of Federated Autonomics across Multiple BBF Network Segments

8.1 Introduction on Use Cases for E2E Business value of Autonomics/AMC

Whereas sections 6 and 7 elaborate on the instantiation of GANA model concepts (such as DEs) on each of the (physical and virtualised manifestations) main nodes of the BBF architecture, this section looks at this instantiation from an end-to-end (e2e) perspective while seeking to show the value of E2E business value of autonomies. This means that the focus is placed on the cooperation and interaction among the instantiated GANA DEs in each of the (physical and virtualised) nodes of the BBF architecture, as well as among the instantiated GANA DEs in the BBF architecture and the ones instantiated on the 3GPP architecture (physical and virtualised), capitalizing in part on the work published in [i.27].

The goal is to realize holistic use cases which highlight the importance of introducing autonomies both in terms of business value for network operators/service providers and in terms of improved experience for the end-user (customer). One such use case is described in Table 12 below.

Table 12: Example Use Case on the value of autonomies for Network Operators in improving customer Quality of Experience (QoE)

<table>
<thead>
<tr>
<th>Title</th>
<th>Proactive identification and resolution of customer’s network experience incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description/Storyline</strong> Use Case</td>
<td>Analytics and autonomic management and control are applied in this case in order to a) understand customer network experience, incidents in a holistic manner and from different perspectives, b) plan remediation actions and c) apply remediation actions, thus preventing the customer from contacting the call center to complain.</td>
</tr>
<tr>
<td><strong>Insights and predictions</strong></td>
<td>Location type e.g. home, work etc.</td>
</tr>
<tr>
<td></td>
<td>Time of the day, week, month</td>
</tr>
<tr>
<td></td>
<td>Type of service usage e.g. voice calls, email, browsing, video etc.</td>
</tr>
<tr>
<td></td>
<td>Type of application e.g. YouTube etc.</td>
</tr>
<tr>
<td></td>
<td>Relevant posts on social media</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Broadband, fixed-access networks (can be extended to cellular network in case of hybrid mode operation)</td>
</tr>
</tbody>
</table>

Apart from information about network capabilities and line characteristics, and current install base of equipment/services, insights and predictions derive based on a customer network experience profile created from a multitude of different perspectives, including:

- Dynamic increase of bandwidth offered for specific service and application type and time. This applies for instance in cases that a high increase in Video or IPTV traffic is expected in certain locations at night and during the weekend.
- Optimization and dynamic application of flexible maintenance profiles
- Software/Firmware updates and/or equipment upgrades

but also opportunities for

- Upselling to customers. For example, identifying frequent dropped calls happening while the customer is at home location or her enterprise can trigger the recommendation for a small cell or a license for a new product upsell.
Operators are investing a lot in order to intensify their customer retention efforts for maintaining their market share and profitability. Nevertheless, resources are limited and should be properly targeted. The network incidents that will be perceptible by the customer and therefore impact the customer experience, constitute a main frustration factor that creates the need for the customer to interact with an assisted channel. It is noted that the interaction with the call center is very expensive. According to McKinsey/IBM “1M calls are received per month by a mid-size SP’s call center at an average cost of 10$ per call”. In addition, repeated deterioration in experience and subsequent complaints can potentially lead to churn.

Accordingly, there is an imminent need to leverage (predictive) analytics and autonomic management and control in order to identify/predict incidents, which can then be fixed proactively to prevent the customer from calling the call center to complain.

### Functions Impacted
- Self-optimization, self-healing

### Systems Involved
- CPE, Access Nodes, Aggregation nodes, BNG

### Indicators/Data
- Network data (including layer 3 and above)
- Customer Demographics
- Social Data

### Evaluation criteria/Metrics
- Decrease or even nullify number of (repeated) contacts
- Decrease or even nullify complaints
- Increase net promoter score (NPS)

### Players
- Customer
- Network operator/Service provider
- Equipment vendor
- Service Provider

### Beneficiaries, and the Benefits
- Customer experience is improved.
- Costs are reduced as calls to centers and complaints are reduced or nullified, thus resulting in increased customer loyalty and lifetime value.
- which in effect solidifies existing revenue streams.
- New revenue streams may be opened for the SP through the derived proactive upsell/marketing opportunities.

---

8.2 How the E2E instantiation of the GANA onto the various BBF network segments and their management and control architectures can realize such E2E Autonomics Use Cases

**Work in Progress ….. We are still working on this part** and we seek to describe how the above use case can be addressed by GANA FBs across multiple network segments and domains (e.g. those outlined for the SDAN scenarios or Mobile/Fixed Convergence scenarios) in a federated fashion

9 Conclusion
Annex A:

Annex B:
Title of annex: The ONIX System and possible ways to implement ONIX

B.1 ONIX architecture

ONIX is characterized by:

- **ONIX Internal Protocols** for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques

- **ONIX External Protocols** (e.g. DHCPv6++, gRPC, or any other protocols that can be used for communicating information in formats that ONIX can be made to support) for supporting the following operations by ONIX users:
  
  1. *Publish Information into ONIX*
  
  2. *Subscribe to receive Information from ONIX, including “on-behalf” subscriptions*
  
  3. *Query & Find Operation to retrieve Info from ONIX*

In terms of Information Servers as members of ONIX, we can distinguish the following:

- Information Server that stores Info purely in ONIX Native Format such as XML, YANG, and other types that could be supported as ONIX native formats for information communicated to ONIX users (consumers of the Information such as GANA Decision Elements (DEs) or Network Elements (NEs—Physical or Virtual)) or stored by ONIX users intending to store information into the ONIX

- Traditional Relational Databases that can be made to support ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques, and can convert some data they store into ONIX native formats for information exchange with ONIX users

- Other Types of Data Storage that can be made to support ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques, and can convert some data they store into ONIX native formats for information exchange with ONIX users

- Shared Common Repository (R) for State Data (e.g. VNFs (Virtual Network Functions State Data) that is made to support ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques, and can convert some data they store into ONIX native formats for information exchange with ONIX users. Such a Shared Common Repository can still be directly accessible via a Native Data/Info Access Interface it should still expose. Such a Direct Data Access Interface exposed by the Server may support access methods such as LDAP, SPML, Diameter, API, or other methods.

- Some Information Servers that are members of ONIX and also exposing their Server-Native Interfaces for use by some “Non-ONIX Native” Data/Information Repository User. As such server-native Data/Info Access Interface may be exposed by e.g. a Repository or Database that is also a member of ONIX at the same time.
NOTE: Data/Information Servers ("N", "X", R") on the Figure 23 below support ONIX Internal Protocols for Federation of Information Servers (i.e. they can be made to operate as ONIX members) and can convert some data they store into ONIX native formats for information exchange with ONIX users.

Figure 23: ONIX architecture

Table: ONIX Interfaces and Services, Internal and External Protocols

The table below provides illustrations of External Interfaces and Services of ONIX, External Protocols and Internal Protocols of ONIX.

<table>
<thead>
<tr>
<th>External Interfaces and Services of ONIX</th>
<th>External Protocols</th>
<th>Internal Protocols of ONIX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

KEY:
- ONIX-EX-Proto(s) = ONIX’s External Protocol(s)
- NE = Network Element (Physical or Virtual)
- VNF = Virtual Network Function
- Direct-Data-Access = Direct Data Access Interface exposed by the Server, supporting access methods such as LDAP, SPML, Diameter, API, etc.
<table>
<thead>
<tr>
<th>ONIX-EX-Proto(s) Interface ENABLES</th>
<th>Various external protocols may be supported by ONIX for providing such services, e.g. extended DHCPv6 (DHCPv6++[refxxx]), gRPC [refxxx], or any other protocols that can be used for communicating information in formats that ONIX can be made to support.</th>
<th>Various external protocols may be supported by ONIX for ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques</th>
</tr>
</thead>
</table>
| enables “ONIX native” users such as **GANA DE, MBTS, or a GANA Node (NE)** to use the following services of ONIX: | • *Publish Information into ONIX*  
• *Subscribe to receive Information from ONIX*  
• *Query & Find Operation to retrieve Info from ONIX* | |
| | | |
| ONIX-EX-Proto(s) Interface ENABLES | Various external protocols may be supported by ONIX for providing such services, e.g. extended DHCPv6 (DHCPv6++[refxxx]), gRPC [refxxx], or any other protocols that can be used for communicating information in formats that ONIX can be made to support. | Various external protocols may be supported by ONIX for ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques |
| enables ONIX native users such as **“ONIX-External” Data Collector** that stores Monitoring Data from the network infrastructure to use the following services of ONIX: | • *Publish/Update Information into the ONIX via any accessible ONIX server* (Cognitive Algorithms operate on raw data on the Data Collector and create Knowledge stored into ONIX and also streamed to DEs in the GANA Knowledge Plane) | |
| ONIX-EX-Proto(s) Interface ENABLES | Various external protocols may be supported by ONIX for providing such services, e.g. extended DHCPv6 (DHCPv6++[refxxx]), gRPC [refxxx], or any other protocols that can be used for communicating information in formats that ONIX can be made to support. | Various external protocols may be supported by ONIX for ONIX Internal Protocols for Federation of Information Servers, e.g. using DHTs (Distributed Hash Tables) and other techniques |
| enables ONIX native users such as **“ONIX-External” DataBase** to use the following services of ONIX: | • *Publish/Update Information into the ONIX via any accessible ONIX server* | |

*Draft ETSI TR 103 473 V0.0.3 (2017-05)*
B.1.1 First subdivided clause of the annex

<Text>.

---

Annex E:
Bibliography

/Publication>: "<Title>".

OR

• /Publication>: "<Title>".

---

Annex F:
Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Information about changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2016</td>
<td>0.0.1</td>
<td>First publication of the TR for TC NTECH #17</td>
</tr>
</tbody>
</table>


### History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Milestone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>