ETSI TS 103 194 V1.1.1 (2014-10)

Network Technologies (NTECH);
Autonomic network engineering for
the self-managing Future Internet (AFI);
Scenarios, Use Cases and Requirements for
Autonomic/Self-Managing Future Internet

Reference
DTS/NTECH-AFI-0014-GS01

Keywords
autonomic networking, requirements,
self-management, use case

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Network Technologies (NTECH).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**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 contains a description of scenarios, use cases, and definition of requirements for the autonomic/self-managing future internet. Scenarios and use cases selected in the present document reflect real-world problems which can benefit from the application of autonomic/self-management principles. Two types of high-level requirements are covered:

1) basic requirements that enable to derive an architectural reference model for introducing Autonomic Management & Control (AMC) of networks (resources, protocols, parameters) and services in various reference network architectures; and

2) specific requirements pertaining to aspects requiring "automation" and "behaviour" in a particular network/service management problem.

2 References

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

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] P. Horn. Autonomic Computing: "IBM's perspective on the State of Information Technology" October 2001, IBM Corp.

NOTE: Available at http://people.scs.carleton.ca/~soma/biosec/readings/autonomic_computing.pdf.

[i.2] IBM: "An architectural blueprint for autonomic computing". Technical report, IBM White paper (June 2005).

[i.3] J.L. Crowley, D. Hall, R. Emonet: "Autonomic computer vision systems" in J. Blanc-Talon (Ed.), IEEE Advanced Concepts for Intelligent Vision Systems ICIVS 2007.

[i.4] Recommendation ITU-T M.3060/Y.2401 (03/2006): "Principles for the Management of Next Generation Networks".

[i.5] ETSI TS 188 001 (V1.1.1): "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN management; OSS Architecture Release 1".

[i.6] TeleManagement Forum TR133-REQ V1.2: "NGN Management Strategy: Policy Paper".

[i.7] "White Paper MUSE Business Model in BB Access" Multi Service Access Everywhere FP6 project.

NOTE Available at http://www.ist-muse.org/Deliverables/WhitePapers/White_Paper_Business_roles.pdf.

[i.8] EC funded FP7 EFIPSANS Project: "Exposing the Features in IP version Six protocols".

NOTE: Available at.http://secan-lab.uni.lu/efipsans-web.

[i.9] EC funded FP7 CARMEN Project: "CARrier grade Mesh Networks".

NOTE: Available at http://www.ict-carmen.eu/.

[i.10] A Requirement Specification by the NGMN Alliance NGMN Recommendation on SON and O&M Requirements, NGMN alliance, (2008).

NOTE: Available at http://www.ngmn.org/uploads/media/NGMN_Recommendation_on_SON_and_O_M_Requirements.pdf.

[i.11] EC Funded Autonomic Computing and Networking: "The operators' vision on technologies, opportunities, risks and adoption roadmap" P1855 Eurescom.

[i.12] Next Generation Mobile Networks Use Cases related to Self Organising Network, Overall Description, NGMN alliance, 2007.

[i.13] Autonomic Communication, White Paper, Fraunhofer FOKUS November 2004.

[i.14] IEEE 802.11: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.15] ETSI ETSI ETSI GS AFI 002: "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture (An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management)".

NOTE: Available at http://www.etsi.org/deliver/etsi_gs/AFI/001_099/002/01.01.01_60/gs_AFI002v010101p.pdf.

[i.16] EC funded FP7 FLAVIA Project: "Flexible Architecture for Virtualizable future wireless Internet Access".

NOTE Available at http://www.ict-flavia.eu/.

[i.17] Celtic Authone project: "Autonomic Home Networking" 2006-2008.

[i.18] IETF RFC 2461: "Neighbor Discovery for IP version 6 (IPv6)" 2007.

[i.19] David D. Clark, Craig Partridge, and J. Christopher Ramming: "A knowledge plane for the Internet". In SIGCOMM, pages 3-10, 2003.

[i.20] Stephen Quirolgico, Kevin Mills, and Doug Montgomery: "Deriving Knowledge for the Knowledge Plane". Draft from National Institute of Standards and Technology Advanced Network Technologies Division Gaithersburg, June 2003. MD 20899-8920.

[i.21] J Lu, C Dousson, F Krief: "A self-diagnosis algorithm based on causal graphs" ICAS 2011.

[i.22] A. Mihailovic, I. Chochliouros, A. Kousaridas, G. Nguengang, C. Polychronopoulos, J. Borgel, M. Israel, V. Conan, M. Belesioti, E. Sfakianakis, G. Agapiou, H. Aghvami and N. Alonistioti: "Architectural Principles for Synergy of Self-management and Future Internet Evolution", Proceedings of ICT Mobile Summit, June 2009.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

automated management: automation of the processes involved in the creation of network configuration input using specialized Task Automation Tools, e.g. scripts, network planning tools, policy generators for conflict-free policies

Autonomic Behaviour (AB): process which understands how desired Managed Entity (ME) element's behaviours are learned, influenced or changed, and how, in turn, these affect other elements, groups and network [i.13]

NOTE: Managed Entity can be physical or logical resource.

autonomic manager element: functional entity that drives a control-loop meant to configure and adapt (i.e. regulate) the behaviour of a managed entity

NOTE: E.g. a protocol module or some other type of a managed entity such as a component, processing sensory information from the managed resource and from other types of required information sources and reacting to observed conditions by effecting a change in the behaviour of the managed resource to achieve some goal.

autonomic networking: networking paradigm enabling network devices and the overall network architecture to exhibit the so-called self-managing properties, namely: auto-discovery, self-configuration (auto-configration), self-diagnosing, self-repair (self-healing), self-optimization, etc.

NOTE: The term autonomic comes from the autonomic nervous system, 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.2].

context awareness: property of an autonomic application/system that enables it to be aware of its execution environment and be able to react to changes in the environment [i.1]

Decision Element (DE): functional entity designed and assigned to autonomically manage and control some Managed Entities (Mes)

NOTE 1: Decision-Making-Elements (DMEs) [i.15] referred in short as Decision Elements (Des) that fulfil the role of Autonomic Manager Elements.

NOTE 2: In accordance with note 1, an ME can be a protocol or a mechanism implemented by some functional entity. A Decision Element (DE) in an Autonomic Manager Element implements the logic that drives a control-loop over the management interfaces of its assigned Managed Entities (Mes). Therefore, self-* functionalities are functionalities implemented by Decision Element(s).

NOTE 3: 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.

future internet: framework Interoperating Multi-Service Self-Managing Future Networks that evolve from today's networking models, paradigms and protocols, and will also include newly designed networking models that succeed to be "deployed"

NOTE: The motivation behind Future Internet is to address deficiencies in current networks such as Scalability, and lack of "Network Intelligence (through Autonomics and Cognition)", and also incorporate missing capabilities such as Self-Management Capabilities. Future Internet includes all sorts of Fixed(Wired) / Mobile / Wireless / Sensor Networks. The Future Internet will interconnect and inter-operate IP(v4&v6) and any Post-IP Networks that emerge and get deployed as some other types of "islands" within the global space of the "Future Internet". As the Future Internet evolves, some "islands" identified by old technology will disappear and new "islands" identified by new technology will appear in the picture.

GANA (**Generic Autonomic Network Architecture):** conceptual architectural reference model for autonomic network engineering, cognition and self-management

NOTE 1: GANA purpose is to serve as a "blueprint model" that prescribes design and operational principles of autonomic decision-making manager elements responsible for autonomic and cognitive management and control of resources (e.g. individual protocols, stacks and mechanisms).

NOTE 2: GANA is a functional architecture and not an implementation architecture [i.15].

knowledge plane: pervasive system within the network that builds and maintains high-level models of what the network is supposed to do, in order to provide services and advice to other elements of the network [i.19]

NOTE: It is a distributed and decentralized construct within the Internet to gather, aggregate and act upon information about network behaviour and operation [i.20]. The subject of the kind of functional entities (mainly GANA Network-Level-DEs) that realize the Knowledge Plane, is covered in clause 9.13 of the GS AFI 002 [i.15]: "Cognition and Knowledge Plane as part of the GANA Decision Plane".

Managed Entity (ME): 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

overlay: logical network that runs on top of another network

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-advertise: ability to advertise its self-model, capability description model, or to send some information signalling message [i.18] to the network in order to allow communication with it or to allow other entities to know whatever is being advertised

self-adaptation: ability of a system or component to change its state of operation e.g. by changing its configuration, in response to context changes that define the service(s) it is supposed to provide to the outside world, or changes in workload, or in response to internal and external challenges (e.g. manifestation of faults, errors and failures)

NOTE: Self-features of a system or component, such as self-optimization and self-healing are special cases of self-* adaptation.

Self awareness: ability to "know itself" and be aware of its state and its behaviours [i.1]

NOTE: Knowledge about "self" is described by a "self-model".

self-care services: ability of a system (e.g. network) to promote and provide an interface for external users to request and consume its services without intervention of the system-administrator, and to update services available to users of such services

self configuration: ability to configure and reconfigure itself under varying and unpredictable conditions [i.1]

self-descriptive: able to provide a description of its self-model, capabilities and internal state [i.3]

self-diagnosis: ability of a system or component to perform fault-diagnosis (also called fault-localization or fault-isolation) procedures by employing various methods to determine the root cause of a failure or malfunction, without external intervention [i.21]

NOTE: Identifying abnormal behaviour (symptom) of a running system or component based on values received by the sensors, by launching some testing (e.g. to discriminate remaining ambiguities), or using the information available in its system or component model and its analysis knowledge-base (e.g. the use of model-based techniques for fault-diagnosis/localization/isolation).

self healing: able to detect and recover from potential problems and continue to function smoothly [i.1]

self-monitoring: able to observe its internal state [i.3]

EXAMPLE: Observation of internal state can be quality-of-service metrics such as reliability, precision, rapidity, or throughput.

self optimization: ability to detect suboptimal behaviours and optimize itself to improve its execution [i.1]

self organizing: able to organize itself with minimum manual intervention **[**i.12**]**

self partioning: introducing level of automation within the partioning process

self protecting: able to detect and protect its resources from both internal and external attacks and maintain overall system security and integrity [i.1]

self-regulation: ability to regulate its internal parameters so as to assure a quality-of-service metric such as reliability, precision, rapidity, or throughput [i.3]

self services: ability to promote and update services available to public

self-testing: ability to test the conformance of its systems

3.2 Abbreviations

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

3GPP	3rd Generation Partnership Project
AB	Autonomic Behaviour
ABGet	Available Bandwidth Get
AC	Admission Control
AC_ME	Admission Control Managed Entity
AF	Autonomic Function
AFI	Autonomic network engineering for the self-managing Future Internet
AMC	Autonomic Management & Control of Networks and Services
AP	Access Point
API	Application Programming Interface
App_DE	Application Decision Element
BBF	Broadband Forum
BS	Base Station
BSS	Business Support System
CaaS	Communication as a Service
CHOP	Configuration-Healing-Optimization-Protection

NOTE: For implying Self-* features of an autonomic system, namely: Self-Configuration; Self-Healing; Self-Optimization and Self-Protection.

CIM	Common Information Model
CLI	Command-Line Interface
CM	Consistency Manager
DE	Decision Element
DHT	Distributed Hash Tables
DME	Decision Making Element
DMTF	Distributed Management Task Force
E2E	End to End
EMS	Element Management System
EPC	Evolved Packet Core
GANA	Generic Autonomic Network Architecture
GS	Group Specification
GUI	Graphical User Interface
HAN	Home Area Network
IaaS	Infrastructure as a Service
IANA	Implementable Autonomic Network Architecture
IB	Information Base
IDS	Intrusion Detection Systems
IMS	IP Multimedia SubSystem
IP	Internet Protocol
Ipv4/Ipv6	Internet Protocol version 4 or 6
IRP	Integration Reference point
ISP	Internet Service Provider
ISV	Independent Software Vendor

IT	Information Technology
ITU-T	International Telecommunication Union
KPI	Knowledge Plane Information
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Medium Access Control
MANET	Mobile Ad-hoc NETworks
ME	Managed Entity
MM	Monitoring Module
MVNE	Mobile Virtual Network Enabler
MVNO	Mobile Virtual Network Operator
NaaS	Network as a Service
NE	Network Element
NGN	Next Generation Network
NGOSS	New Generation Operations System and Software
NMS	Network Management System
NO	Network Operator
OAM	Operating And Maintenance
OPEX	Operation Expediture
OSS	Operation Support System
OTT	Over The Top
OVN	Overlay Virtual Network
P2P	Peer to Peer
PC	Personal Computer
QoE	Quality of Experience
QoS	Quality of Services
QoS_DE	Quality of Service Decision Element
RAN	Radio Access Network
RFID	Radio-Frequency IDentification
RQ	Requirement
Saas	Service as a service
SDN	Software Defined / Driven Network
SDO	Standardization Organization
SID	Shared Information Data/Model
SLA	Service Level Agreement
SMS	Short Message Service
SOHO	Small Office Home Office
SON	Self Organizing Network
TCP	Transmission Control Protocol
TISPAN	Telecoms and Internet converged Services and Protocols for Advanced Networks
TMF	Tele Management Forum
TSPEC	Traffic Specification
TV	Television
UE	User Equipment
VNO	Virtual Network Operator
WMP	Wireless Media Access Control (MAC) Processors

4 Main drivers towards Autonomic Management and Control (AMC) of Networks and Services

4.1 Global background and general requirements on the need for autonomics

As network operators need to address numerous issues such as deregulated markets, open competition, explosion of digital services, converged fixed-mobile services, converged IT-Network (virtualisation, Clouds) and operation efficiency, they are facing new business and technical challenges. Consequently, they are striving to build a new ecosystem comprising end-to-end solutions, created through strategic alliances within the telecommunications sector including third parties (e.g. Mobile Virtual Network Operator (MVNO) / Mobile Virtual Network Enabler (MVNE), competitors becoming partners (Radio infrastructure sharing or "Radio Access Network (RAN) Sharing" agreement, for instance), Clouds Services Providers, Virtual Network Providers, consumers becoming content producers, outsourcing partners, integrators. For this reason the networks they are operating and the associated 'Operations Support System' (OSS) need to be intelligent, agile, open, secure, flexible and autonomic (i.e. operating with minimum human intervention).

As driving forces from the network evolution perspective, industries can highlight the deployment of key emerging technologies such as IP Multimedia Subsystem (IMS) / Next Generation Network (NGN), Long Term Evolution (LTE)/Evolved Packet Core (EPC), Future Internet, Internet of Things, Machine to Machine (M2M), Infrastructure / Network / Communication as a Service (IaaS/NaaS/CaaS), etc. The underlying network architectures, so called "flat architecture" will increase the amount of equipments required while at the same time the major operators' requirement is to lower operating costs (OPEX).

That means, some level of the notion of being "autonomic" should be embedded into network equipment and OSS at a first phase for the configuration purpose.

Future Network infrastructure should incorporate more and more autonomic features in order to maintain operational costs under control when it comes to a large scale deployment phase.

The same should be also applicable during the "operation phase" and "optimization phase", all lifelong of the network. This needs embedding self-configuration, self-healing, self-optimization, self-protecting (Self CHOP) features.

In this context, requirements aiming at building trust and confidence on these self-functions, in one hand, and the coordination of interaction of various autonomics functions in the other hand, shall be implemented in order to ensure a global optimum while targeting a local optimum per autonomics function activated through the same optimization parameter.

Without this coordination, the operator could not prevent the fact that some parameters can lead to the optimization of one autonomics function while at the same time, it negatively impacts another autonomics function. This results in an unstable behaviour of the network.

That means, the coordination of interaction of autonomics functions deployed in a network is a major requirement as well from operators' perspective.

In case of failure of an Autonomics function, a process shall be specified and designed to allow the operator to keep control of the management of the network through its OSS and related tools by desactivating a given autonomics function as long as a solid trust and confidence has not being built.

Currently, there is a lot of work being carried out on autonomics, mostly conducted by the research community but from the operational point of view there is little common understanding on how autonomic technologies can help and how they will impact current operation models of the operators. There is a need to build a new management environment that can definitely contribute to the efficiency of business units and reduce OPEX. Autonomics and Self-Management related technologies are envisioned as the solution for a player to control its own environment and at the same time assuring the end to end view, which emerges from the individual behaviours of all the players.

The present document focuses on the set of requirements for Autonomic and Self-Managing Future Networks to efficiently help the operator to face new market realities and on the definition of the operational requirements for operators to take advantage of such advanced infrastructure. The operational model is far beyond the classical centralized management approaches, looking for innovative methods for controlling and managing distributed decision making functions embedded in an autonomous and intelligent infrastructures.

The present document establishes a framework for "Scenarios, Use Cases and Requirements for the Self-Managing Future Networks" contributed by network operators and other players such as content providers, etc.

The starting point is capturing autonomic issues and global context from operators' requirements in order to shape the current and Future network vision. This serves as input to formulate operators' requirements from operation view point. The result is shaping AFI high level requirements.

4.2 Future network vision and expected further requirements for Autonomics and its interworking with other emerging paradigms

This clause is simply meant to provide useful insights into emerging trends in networking, in which autonomics, as a paradigm, is expected to play a role while also complementing other emerging networking paradigms such as Virtualization and Software-Driven/Defined Networking (SDN).

In the future, processing, storage and communication services will be highly pervasive, intertwined and strongly related to each other. What the future network vision expects is that people, smart objects, machines and the surrounding space will all be embedded with devices such as sensors, RFID tags, etc., defining highly decentralized dynamic network environments of virtual resources interconnected by wired and wireless connectivity. Overlay networks will be the major means to organize and aggregate these highly dynamic communication environments.

Virtualization of resources (from networking to processing to storage, etc.) will be a key characteristic of Future Networks. As a consequence:

- autonomic features should support functions such as the creation and maintenance of overlay networks of virtual resources.

For instance autonomic features might be integrated with hypervisors' capabilities.

Therefore, networks will evolve towards a broader perspective to include not only connectivity resources but also other types of resources such as processing, storage and things (e.g. terminals, sensors, actuators, probes, etc.). This is a more holistic and future proof vision of the network environment (useful for analysing various scenarios/use-cases: from zero-configuration Home to Cloud Computing, to Content Delivery Networks, etc.).

Besides, programmability and flexibility through SDN (Software Defined / Driven Network) are key enablers for networks (fixed and mobile) as well for data centres. (Reader may refer to SDN-oriented enablers are also mapped to GANA reference model [i.15]). It allows a close interaction of applications to networks which leads to delivering network services in an efficient manner via standardized and open Application Programming Interfaces (APIs).

4.3 Operator's requirements that enable derivation of a reference model for introducing AMC in networks

The scope in this clause is mainly focused on end to end services management from user perspective within an evolved network. Besides, some operators have to deal with the legacy network that is why an autonomic management and control specification needs to seek how to adapt Fixed (e.g. BBF), Mobile (e.g. 3GPP) and services (e.g. IMS) architectures in order to make the introduction of autonomic functions easier and smoother in physical, virtualized, distributed centralized resources. Therefore, in addition to user's requirements, a set of technical and management requirements for operators to deal with an autonomic network have also been captured.

First, a "knowledge plane" shall be introduced in the network taking into account the legacy network on the one hand, and services (e.g. IMS), access (e.g. Fixed and Mobile) and home access networks (e.g. Broadband Forum reference architecture, "Authone: Autonomic Home Networking" project [i.17], for instance), on the other hand.

- This knowledge plane shall take into account the constraints of all the actors and security concerns.

- Data in the knowledge plane shall be up to date and granted. Information from different actors could be shared by context defined by an ontology.

Autonomic features would decide locally based on knowledge retrieved from analysed information of the global network. Based on such knowledge, local decisions would be taken in respect of end to end or global views, e.g. configuration of network elements from end to end constraints actors view point, mobility control between different heterogeneous access network with different radio access technologies (e.g. WiFi, Wimax, 2G/3G/LTE), services adapted to user context.

The clause defines a set of operational requirements for an operator to control an Autonomic and Self-Managing Future Network. The requirements have implications on the operational principles of autonomic components of an autonomic network e.g. federation requirements, information sharing, and other types of desired behaviours in networks (as described later with figure 2) which illustrate a Policy Management framework.

In this context two views need to be highlighted: "cross layers autonomic views" within an operator's network in one hand, and "cross domain autonomic view" through various domains in the other hand. Domains mean here "players" as described later with figure 14.4.2 requirement framework for a policy- based management as input towards derivation of a reference model for introducing amc in networks. Indeed, from "cross layers autonomic views", an upper layer "cognition function" is able to retrieve from local views a situated view of its environment. At a lower layer which embeds an Autonomic Function it becomes possible to retrieve objectives from upper layers in order to make a decision locally with a global objective, to different layers (as described later with figure 3).

Regarding "cross domain autonomic view", the cognition functions are used here with the goal to disseminate the knowledge through various domains (as described later with fgure 4). Indeed, each "Autonomic Function" will use this "cognition function" to react locally with a *common* objective, to different domains.

- In order to manage end to end services autonomously if needed (players' agreements, regulation constraints, etc.) an horizontal autonomics architecture shall be defined.

4.4 Management requirements input to derivation to automated management workflow and architectural aspects of an autonomic network

This clause gathers the set of operational and management requirements for an operator to deal with an autonomic network. Starting from users' requirements, a set of operational and maintenance requirements are captured for an operator to fulfil the quality expectations of users. This work is aligned with the NGN management requirements that can be found in [i.6] and [i.5] where a first level of requirements (level 0) is composed by:

- Customer centric requirements.
- Business vision requirements.
- Technology requirements.
- Operational requirements.
- Regulatory requirements, only the Technology and Operational requirements are covered here.

The first set of requirements in Table 2 is user oriented. Users want to have access to adapted services that they choose with a guarantee of security and quality. This implies requirements from operators' perspective: Operating and Maintenance (OAM) requirements.

4.4.1 Identifying players that drive network management aspects as basis for capturing requirements for automated management and autonomic behaviours

In order to translate end user requirements ("user" meaning the intended or perceived user of autonomics related technology for management of networks and services) into technical requirements within the operators' networks, the following template is used as a guideline. It contains the following fields:

- Players.
- Network environment.
- Scenario.
- What is the requirement.
- What need to be automated (this field is more linked to Generic Autonomic Network Architecture [i.16]. It is here only to better understand the technical requirement).

In order to better capture operators' requirements and map them to the relevant scenarios, the methodology used here is the partioning of the operator' network in various "Network Environments".

Following is an instantiation of this Network environment concept:

- Home Area Network (Small office Home Office SOHO network).
- Access network.
- Regional network.
- Service platform.
- Content platform.
- Ad hoc network.
- IT platform.
- User Network.
- Other, etc.

Following is an instantiation of the "Player" concept:

- User Network.
- User Service.
- Subscriber [i.7].
- Application service provider [i.7].
- Multimedia content provider [i.7].
- Multimedia service provider.
- Network connectivity provider [i.7].
- Access network provider [i.7].
- Regional network provider [i.7].
- Network service provider [i.7].
- Internet service provider [i.7].

- Packager [i.7] (operators with different players or make the link with different players (VNO)).
- Third party.
- Identity provider.
- Government (regulator).
- Application developer.
- OTT: Over The Top (e.g. Google, Apple, Microsoft, etc.).
- Network outsource actor.
- Service outsource actor.
- User content provider.
- Community service provider.
- Network community stakeholder.
- Social network stakeholder, etc.

Figure 1 shows player dependencies from a network environment point of view. Network environment management is driven by the different players of the network. There is no longer one operator that owns the whole network, but a web of players that offer services and network interfaces to others [i.7]. As a consequence:

- autonomic technologies shall guarantee that a player control their own environment and at the same time assure the end to end view, which emerges from the individual behaviours of all the players.

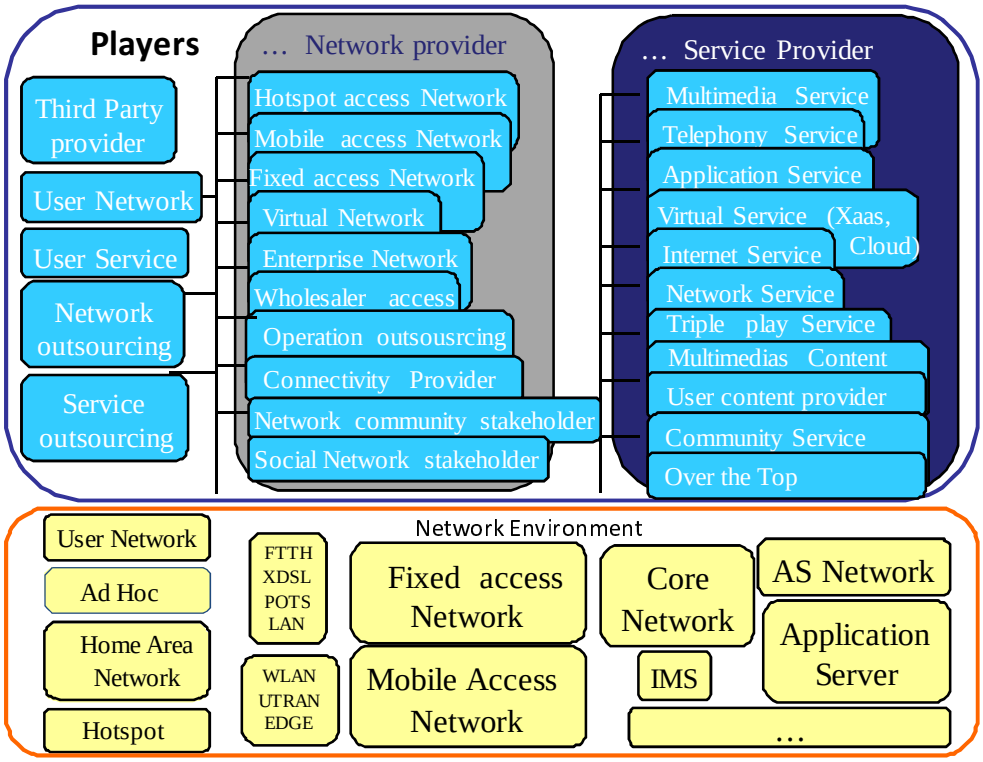

Figure 1: Network environment management driven by players

4.4.2 Requirement framework for a Policy- based management as input towards derivation of a reference model for introducing AMC in networks

This framework illustrates the evolution of the network management in order to become intelligent, open, flexible, autonomous/Autonomic, secure, context-aware, policy-based, business-driven and SLA-driven. It is structured through the 4 following requirements from an operator perspective. In order to better understand the description of this requirement, alongside describing these requirements themselves, they have been mapped with regards to a high level operator's network.

Strategic requirements

This requirement is focusing on business intelligence and associated partnerships necessary to implement this strategy.

- Minimize OPEX/CAPEX
- Maximize user satisfaction
- Minimize carbon footprint
- Maximize revenues

In this context, the present document illustrates this partnership from stakeholders and partners' viewpoint by a high level (abstraction) layered architecture composed of two main domains, operator's domain and vendors' domain.

At the top level, the present document depicts the operator's domain which includes 3 layers: business policy, service objective, operator's OSS. At the bottom level, it depicts vendors' domain which includes the network and its associated management system.

Governance requirements

For the purpose of this network governance, an interface is needed to allow the operator to adjust the features of the demanded service/infrastructure. The reason why, a business level language is required to help the operator to express what it is needed from the network:

- such business language shall be semantics-oriented; and
- shall be modelled by the use of ontology to add semantics and enable machine reasoning on the goals.

Indeed, the operators and services providers are expecting benefits and usability of ontologies in their service strategies within highly competitive and fast moving Internet market environment with strong Time-To-Market constraints. Ontologies capture the semantics of information from various sources and are a powerful tool in services design, service composition (service logic) and service personalization through specific user profiles in a dynamic way. At the same time, current oriented-object information models specified by various SDOs (SID from TMF and CIM from DMTF or IRP from 3GPP, etc.) are less flexible to meet this objective. This requirement has a direct impact on existing BSS/OSS information models.

Such a Business Policy level description eases the automation of "Edition – Translation – Execution" of Policies. This leads to the translation into "Service Profiles" at Service level and into "Network Profiles" at Network level.

Finally, after translation phase, the distribution process of Service Profiles and Network Profiles is performed in order to prepare the execution and enforcement. The last phase of this process is the "Policy and Rule Enforcement and Execution" by the Network part (Nes) in the vendor's domain as depicted in figure 2.

This approach for network governance gives the operator a mechanism for controlling the network.

Operational requirements

This requirement aims at improving operation efficiency (reduce OPEX). One way to achieve this goal is to harmonize Business Support System (BSS) and Operation Support System (OSS), Data Models and to deploy a standardized northbound management interface. Such a harmonization is vital in the context of converged fixed-Mobile network and services management.

From management architecture perspective, figure 2 maps these "Operational requirements" to the real operator architecture which will handle the implementation. The network environment (Vendors' domain in the figure) will be managed by business objective which will drive the service objective. The service objective will be then translated into policy rules which will be enforced in the operator's network through the operator's Network Management System (NMS). The policy enforcement will be then executed by the different vendor's Element Management System (EMS) and the Network Elements (NE) forming the operator's network. Each layer of the whole architecture will take into account its intrinsic constraints.

Autonomous and Cognition requirements

This requirement aims at taking advantage from introducing Self-Awareness, Analysing, Learning, and Reasoning capabilities and mechanisms. It also includes gathering information, transforming it into knowledge and distributing it to various needs. There is also a need to building and ensuring Trust and Confidence as well as Stability in Autonomics loops and in the network.

From management architecture perspective, figure 2 maps these "Autonomous and Cognition requirements" to the real management architecture.

The cognition aspect is shown by "cognition module" (purple boxes) in the right part of the figure. These cognition modules are used to retrieve relevant knowledge from data/information and it allows the cross-control loop interactions accordingly. These cognition modules can also be seen as "brokers" where various knowledge sources store the knowledge in a controlled and secured way, while, the users of these knowledge retrieve required and relevant knowledge through a subscription model. In this context, a dissemination plane is used to disseminate knowledge and decision.

NOTE: The indicated Cognition Modules can all be implemented within the Knowledge Plane's DEs.

The Autonomic capabilities are introduced in this management architecture thanks to Autonomic Functions (AF) (pink boxes) which includes the Decision Making Element (DME) at different layers. This implementation of these AFs in the autonomic network architecture is driven by operator's policy. Ian this perspective, the figure 2 represented the 3 autonomic network architectures schemas symbolized by red circles as specified by 3GPP/SA5 for SON related OAM:

- Distributed manner: the AFs are embedded in the NE only.
- EMS-Centralized manner: the AFs are embedded in EMSs and NEs.
- NMS-Centralized manner: the AFs are embedded in the operators' OSS and NEs.

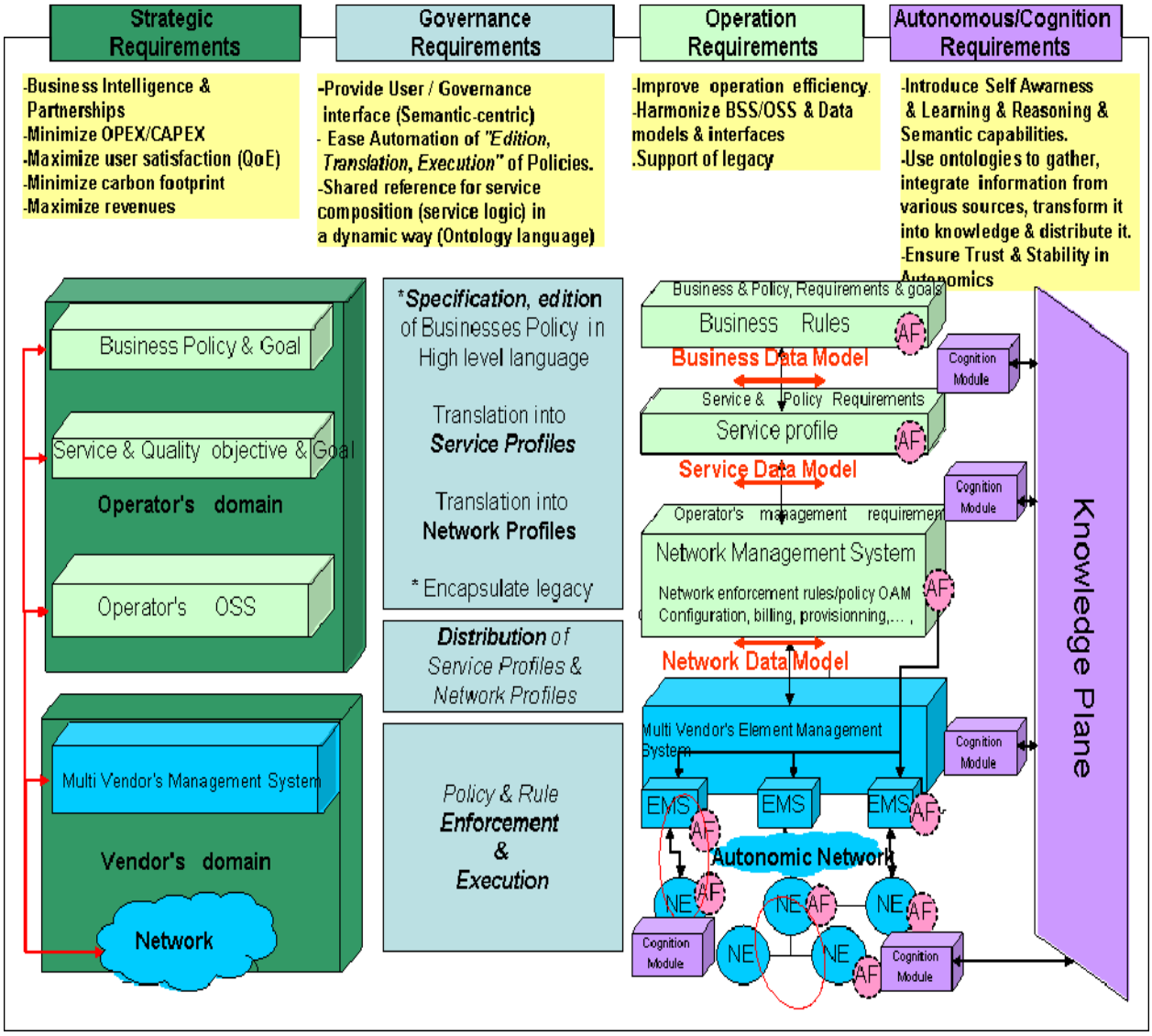

Figure 2: Requirement framework for a Policy- based management of an Autonomics Network

4.4.3 Operator's Policy-based autonomics network vertical framework (cross-layer)

Figure 3, as an instantiation of figure 2, depicts a framework that addresses the relationship between high-level specification of client performance objectives and existing resource management infrastructures with integration of autonomous features and cognition mechanisms in the context of cross-layering, thus providing operators with means for decision oriented towards operational tasks based on the use of policies rather than low level command execution. The strategic requirement just highlights the related requirements.

Strategic requirements

- Business Intelligence and Partnerships with end to end (E2E) view
- Minimize OPEX/CAPEX
- Maximize user satisfaction (Quality of Experience (QoE))
- Minimize carbon footprint
- Maximize revenues

Governance requirements

- Cross-layer User / Governance interface (Semantic-centric)
- Ease Automation of "Edition, Translation, Execution" of Policies
- Shared reference for service composition (service logic) in a dynamic way (Ontology language)

Operation requirements

- Improve operation efficiency
- Harmonize BSS/OSS & Data models and interfaces in cross-layer model
- Support of legacy

Autonomous and Cognition requirements

- Introduce Self Awareness: Learning, Reasoning and Semantic capabilities
- Use ontologies to gather, integrate information from various sources, transform it into knowledge and distribute it in cross-domain model
- Ensure Trust and Stability in Autonomics

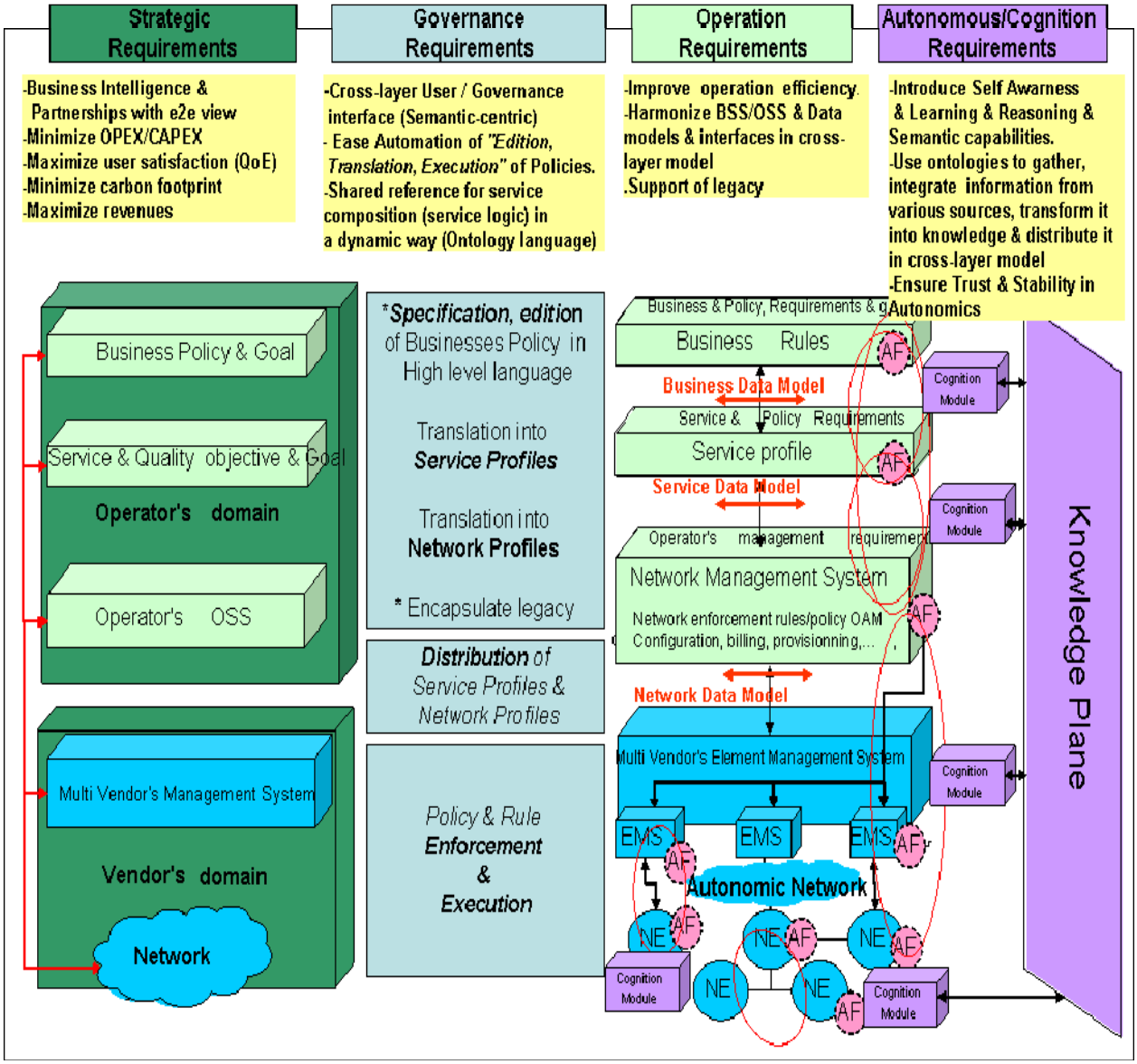

Figure 3: Operator's Policy-based autonomics network vertical framework

From cognition perspective, an upper layer "cognition module" (purple boxes) is able to retrieve from local views a situated view of its environment. From autonomous point of view, these layers are connected through the red loops. Indeed, an Autonomous Function (AF) (pink boxes) located in bottom layer can retrieve objectives from upper layers in order to make a decision locally with a common global objective.

The cognition interaction is required in order to gather and disseminate the knowledge produced at a knowledge / dissemination plane through "cognition function" for the red loop process purpose and it allows the cross-control loop interactions accordingly.

4.4.4 Operator's Policy-based autonomics network horizontal framework (cross-domain)

The aim of **Operator's Policy-based autonomics network horizontal framework** is to describe the cross-domain interaction from autonomics and cognition perspective. It is also an instantiation of figure 2. The description below just highlight the related requirements.

Strategic requirements

- Business Intelligence
- Common business goal (creation of new business before sharing) Operators' agreement
- Minimize OPEX/CAPEX
- Maximize user satisfaction (QoE)
- Minimize carbon footprint
- Maximize revenues

Governance requirements

- Cross-domain User / Governance interface (Semantic-centric)
- Ease Automation of "Edition, Translation, Execution" of Policies
- Shared reference for service composition (service logic) in a dynamic way (Ontological language)

Operation requirements

- Improve operation efficiency
- Common Management Framework
- Harmonize BSS/OSS, data models and interfaces in cross-domain model
- Support of legacy

Autonomous and Cognition requirements

- Introduce Self-Awareness, Learning, Reasoning and Semantic capabilities
- Use ontology to gather, integrate information from various sources, transform it into knowledge and distribute it in cross-domain model
- Ensure Trust and Stability in Autonomics

The cognition modules (purple boxes) are used here with the goal to disseminate the knowledge through various domains. Domain means here an operator network or an administrative view of a global operator network (Access or Backhaul or Core). It corresponds to a partitioning of a global network. These cognition modules as "brokers" where various knowledge from various operators store their knowledge in a controlled and secured way, while, the users (belonging to various players) of these knowledge retrieve required and relevant knowledge they need through a subscription model. This approach gives the operators a mechanism for controlling the knowledge they provide in this cross-domain autonomic management.

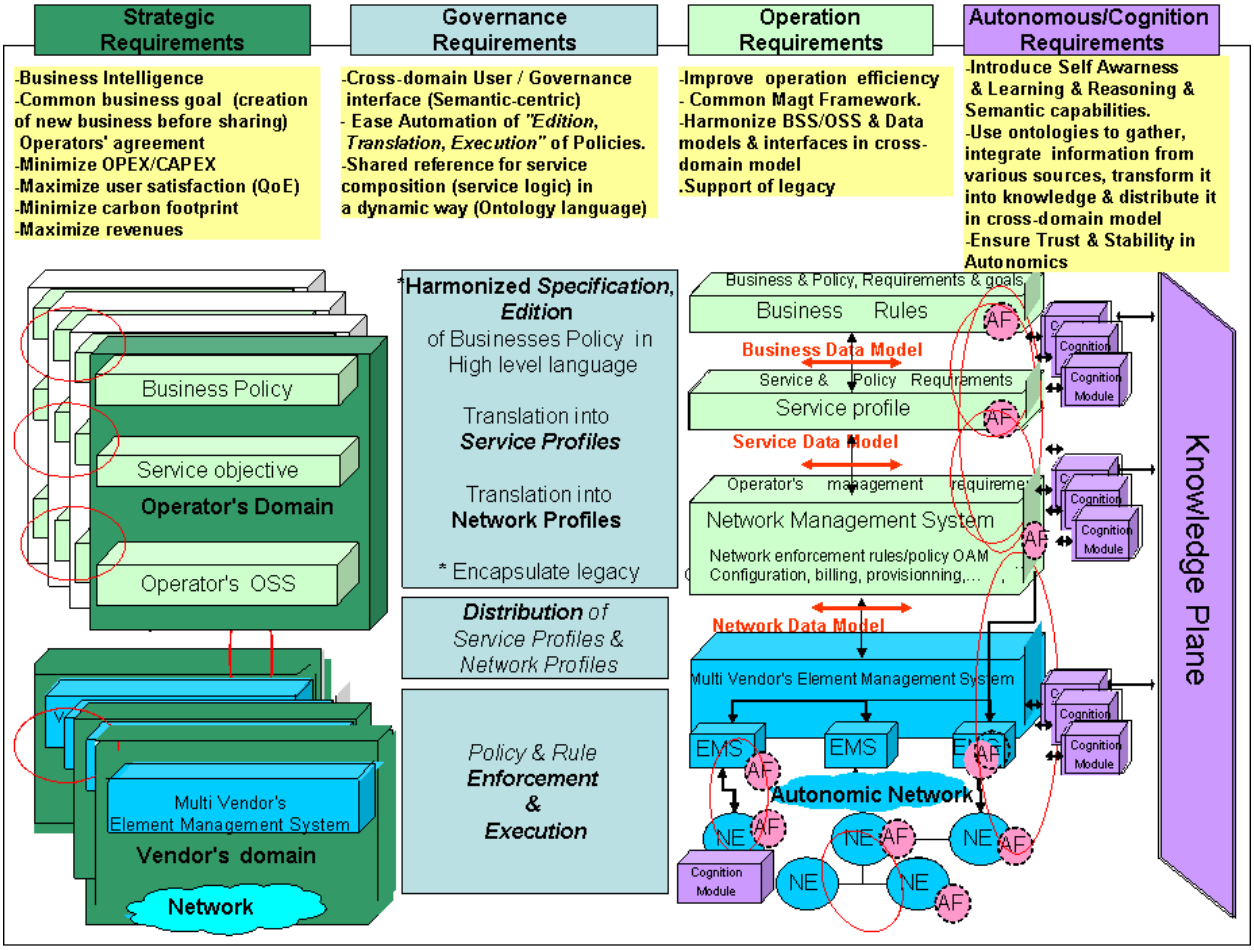

Figure 4: Operator's Policy-based autonomics network horizontal framework

Indeed, each Autonomous Function (AF) (pink boxes) will use this "cognition module" to react locally with a common objective (to different domains). This horizontal autonomics architecture is required in order to manage end to end services autonomously if needed (operators' agreements, regulation constraints, etc.).

4.5 AFI Requirement template

Table 1 depicts the template defined in order to capture relevant data related to the requirements with respect to the given scenarios (clause 5) . It is composed of the following fields:

- Player
- Network Environment
- Requirement Identity (RQ ID). An arbitrary sequential number (without any normative meaning) allocated to each requirement to ease its location in the table
- Autonomic Functionality within the Self* range
- What is the requirement
- What needs to be automated (This field is an input to the technical translation)

Table 1: Requirement template

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated

- **The way to interpret each of the requirements is as follows:**

  Given a particular **network environment**, a **player** of relevance to that environment is perceiving or desiring the network environment to exhibit a specific **Autonomic Functionality**, the **requirement** says what network environment is perceived or desired to fulfil. In addition to that an indication of **what needs to be automated** in order to help implement the requirement is provided. **What needs to be automated** only serves as hint to the developer/implementer of the requirement who may use other additional knowledge to implement the requirement.

4.6 AFI high level requirements attached to network environment

4.6.1 Basic requirements an Autonomic Network shall support

An Autonomic Network shall support the following Self-functions [i.22]:

- Self healing
- Self optimization
- Self protecting
- Self organizing
- Self Configuration
- Self-Diagnosis
- Self awareness

In addition, the Autonomic Network or its internal functions may support the following Self* features:

- Self-advertise
- Self-descriptive
- Self-monitoring
- Self partioning
- Self-regulation

4.6.2 Requirements for specific network environments

Based on the master template of the table 1, tables 2 to 7 are the instantiations of this template to relevant scenarios identified in the present document.

This classification is players-oriented:

- User player requirement (table 2)
- Manufacturer requirement (table 3)
- Access Network requirement (table 4)
- Access and Core Network players requirements (table 5)
- Services players requirements (table 6)
- Access network / core network / Services players requirements (table 7)
- Content player requirement (table 8)

- Cross-players requirements (table 9)

Each of the following tables below contains set of requirements organized primarily by the player involved in the requirement. Furthermore, from a management point of view, the requirements can be classified by the autonomic functionality (defined in clause 4.5.1) needed for each of the network environments indicated.

Table 2: User player requirement

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	Requirement	What needs to be automated with less human intervention
User	Ad hoc	Scenario 5.7	1	Self-organizing	The ad hoc network shall organize its network with volatile UE and let UEs participate to the organization of the network User equipment shall be able to attach itself to the ad-hoc network and participate in self organizing the network in a given context	Decentralized network organization process through network element
User as network operator and developer	Ad hoc	Scenarios 5.4, 5.7	2	Auto-Discovery and Self configuration	UE autonomic establishment of communication with each node in the network shall be available *The node should be able to know which services are available in the ad hoc network*	Network discovery process through network element *(A node joins the network and is able to recognize its neighbours and communicate with them. Through the application of a proper routing protocol, it is also able to communicate with any other node. Multi-hop communication shall be established autonomically)*
User	Ad hoc	Scenario 5.7	3	Self-configuration	UE auto-configuration shall be provided in order to connect to the existing infrastructure	Network configuration process through network element *(The node, upon identification of its neighbours, is able to join the network and self-configure itself and connect to others nodes or network (e.g. with "gateway"). No need for human administrating a centralized or predefining entity in order to provide specific configuration files or guidelines to each new participant node)*
User	Ad hoc	Scenario 5.7	4	Self-awareness	Ad hoc network shall provide and advertise information about its capabilities	Process of gathering information from the network and advertising it. *(The overlay network plays the role of a distributed repository for all network nodes. According to the stored information, virtual communities may be created in the overlay network by sharing specific data on it and permitting access to part of its members)*

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	Requirement	What needs to be automated with less human intervention
User	Home area network	Scenario 5.2	5	Self-Configuration	The HAN shall not prevent the user to configure, add equipment and services, control and optimize the home network *(Home Area Network configuration should take into account user context (user equipment, profile subscription, preferences, user services, etc.) regardless of the access network)*	Home Area network configuration Process under the control of the human
User as network developer	Ad hoc	Scenario 5.7	6	Self-configuration	The network shall provide the autonomic bootstrapping of devices or nodes in the network and the network as a whole *(The network shall be established automatically without the need of any external existing infrastructure)*	Bootstrapping process of node and the network shall provide all the information and process needed by the UE to be operational as the ad hoc network means
User as network developer	Ad hoc	Scenario 5.7	7	Self-configuration	The ad hoc network shall build a registration knowledge plane without human intervention *The network shall be established automatically with knowledge without the need of any existing infrastructure* *A decentralized registration shall be available for special data. Specific nodes in the network shall be selected as registration entities. Registration related roles shall be allocated dynamically according to predefined criteria)*	Process to build a knowledge plane
User as network administrator	Ad hoc	Scenario 5.7	8	Self-configuration	The Ad hoc network shall retrieve, analyse, process (reason, learn) data and transform it into knowledge to be used by authorized requesters	Process to organize and share secure knowledge.

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	Requirement	What needs to be automated with less human intervention
User	All	Scenario 5.2	9	Self-provisioning	The Ad hoc network shall provision services with users context	Process to provision (register, subscribe, publish) services according to the information authorized by users
User	Ad hoc	Scenario 5.2	10	Self-protection	the ad hoc network shall support the addition and creation of services by the different players	-Mechanisms to select the needed functionality to provide advanced and secure services on user requirement basis. -Process to propose/publish services to authorized users. -Process to build services. *(to create, publish, access, control, bill, QoS manage the services provided by the players (e.g. user))*
User	all	Scenario 5.7	11	Self discovery	The network discovery services, connectivities, ad hoc network means shall be secured	Process to share data in secure manner
User	Fixed, Ad hoc	Scenario 5.7	12	Self – provisioning	The ad hoc network shall have the ability to adapt and scale the network and services in a coherent manner	Processes to create network services and change those services related to the network changes (e.g. network size) and to adapt services to the desired usages according to contexts *(e.g. routing, data dissemination techniques, service provision)*
User	Ad hoc	Scenario 5.7	13	Self-healing	The ad hoc network shall ensure service continuity	Process to access data and services in reliable and non interruptive manner.
User as Service provider	Ad hoc	Scenario 5.7	14	Self-healing	The ad hoc network shall have the reliability of data	Process of data replication and optimization *(Storage, efficient usage of storage resources according to network characteristics)*
User Network administrator	Ad hoc	Scenario 5.7	15	Self-healing	The ad hoc network shall repair fault occurring in the network	Processes to identify faults in the network and to perform corrective actions
User	Ad hoc	Scenario 5.7	16	Self-awareness	The ad hoc network shall have context awareness	Mechanisms and processes of extraction of meaningful events in the Ad Hoc network according to the acquired data and management of the events. *(For example, different actions may be undertaken according to the user profile, the volatility of data and the access rights).*
User as developer	Ad hoc	Scenario 5.7	17	Self optimizing	The ad hoc network shall have autonomic establishment of communication with each node in the network	Mechanism for using multiple interfaces for establishing concurrent communication channels with neighbouring heterogeneous devices.
User as developer, Administrator	Ad hoc	Scenario 5.7	18	Self discovery	Physical and Overlay network shall be built in a proximity relationship	Correlation mechanisms among the overlay network nodes and the physical network nodes

Table 3: Manufacturer requirement

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Manufacturer	Ad hoc, Sensor Network	Scenario 5.7	19	Self-optimization	The network shall have an energy-efficient communication	Mechanisms for improving energy saving. *(Energy-efficient routing shall require a limited number of exchanged messages.)*
Manufacturer	Ad hoc	Scenario 5.7	20	Self-awareness	The ad hoc network shall retrieve the network context awareness	Mechanism for retrieving network context in order to build optimized network
Manufacturer	Access, Edge, Core network	Scenario 5.3	21	Self-Configuration and associated Self- Discovery	The network shall be governable	Tools to translate network operator goals into policies and configuration profiles which may be stored into network repositories in order to be communicated or fetched by network devices within a self configuration process. (*Provides a user interface to allow the operator to adjust the features of the demanded service/infrastructure. Tools and GUI for: policy edition , policy validation (conflict detection and resolution) and policy encapsulation into configuration profiles)*
Manufacturer of a network element (Network Element Vendor)	Access, Edge, Core network	Scenario 5.3	22	Self-Discovery and associated self-Configuration	The Network shall be composed of Plug and play devices with self-discovery capabilities and ability to self-advertise capabilities	Mechanisms of describing device or node capabilities and advertising process capabilities. *(Description Model to the entities that need such vital knowledge. This required knowledge is used to assign a role for the newly attached Network Element and to give it a Configuration Profile which helps it to self-configure)* *(Existing discovery mechanisms such as those found in Ipv6 are still limited. Enhanced discovery capabilities are needed to be augmented towards more advanced self-discovery mechanisms, which can include for example event discovery of capabilities with vital knowledge of devices that plug into the network.)*
Manufacturer of a network element (Network Element Vendor)	Access, Edge, Core network	Scenario 5.3	23	Self-Partitioning of a network)	Network Element shall provide capabilities to allow network self-partitioning	Process for taking care of network partitioning as the network size changes for resource optimization

Table 4: Access Network requirement

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Access network provider	Home area network	Scenarios 5.2, 5.4	24	Self-configuration	The home area network shall self-configure according to the user services subscription (Authentication, Attachment)	Authentication, attachment, configuration, security processes of devices according to users subscription within a multi-player agreement. *(for IP and non IP devices, for services and for users devices (home or nomadic) within the Home Area Network)*
Access network provider	HAN, access network	Scenario 5.2	25	Self-configuration	The HAN shall support self configuration and self provisioning according to user online subscription	Provisioning and configuration processes of user equipment to implement new services. With notification to the different players with the new subscription
Access network provider	Home area network	Scenario 5.2	26	Self-diagnose	the HAN shall support self diagnosis and shall report it to the access network in order to reduce human intervention	Processes to diagnose HAN and to notify the necessary result to the access network player • to retrieve data from sensors (statistics event) necessary to fault qualification, based not only on local view alone but also through neighbours • to Analyze data to identify the fault cause (for already known fault type) • to define the test to identify the fault • to continuously discover new faults. (i.e. learning method, data analysis in order to identify new fault cause) • to define the test to identify and validate new faults • to elaborate an end to end diagnosis chain • (identification of neighbours, players or equipment involved in this global diagnose including the agreement between those actors)

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Access network provider	Home area network/ Access network	Scenarios 5.2, 5.4	27	Self-healing	The access network shall notify each failure of the self-healing process to the authorized user • the healing process shall notify the player administrator (owner) the method used and the equipment healed • if the equipment is not self-heal the healing process shall notify the player in case the system could not be repaired remotely • the player, owner (administrator) shall be able to • Validate the method used to repair each fault • Define methods for protection and restoration • Identify new path for services • Define protection mechanism in real time	Healing process *Based on the diagnosis report received from the different players*
Access Network provider	Home area network	Scenarios 5.2, 5.4	28	Self-Monitoring Self-Optimization	The home area network shall be monitored at both network level and service level *HAN shall examine its own traffic load/type parameters (available bandwidth, packet loss, QoS) in order to ensure a reliable and efficient network.* *- Mechanisms achieving this goal shall be done through multi player environment requirements and allow players retrieving monitoring information*	Monitoring process of HAN services

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Access network provider	Wireless Mesh Network	Scenario 5.1.0	29	Self-configuration	Mesh nodes shall automatically connect to the network	Mechanisms of recognition of physical network topology *(neighbour identification, and utilization of heterogeneous network technologies)*
Access network provider	Wireless Mesh Network	Scenario 5.1.0	30	Self-optimization	The wireless mesh network shall optimize usage of capacity versus coverage	Process of selecting radio technologies and their configuration according to current radio/traffic conditions *(channel, rate selection)*
Access network provider	Wireless Mesh Network	Scenario 5.1.0	31	Self-healing	Wireless mesh network shall be resilient to changes of topology and radio conditions	Monitoring presence of neighbouring nodes and reaction to network events (e.g. link failure)
Access network provider	Wireless Local Area Network	Scenario 5.12	32	Self-optimization	Network shall self-adapt to changes of radio channel conditions	Monitoring of available channels and data rates. Mechanisms for selecting best channel, data rate, transmission power, etc.
Access network provider	Wireless Local Area Network	Scenario 5.12	33	Self-protection	Misbehaving nodes shall be detected and dealt with	Monitoring of node behaviour and checking for conformance. Mechanisms for penalizing misbehaving nodes, enforcing their correct behaviour and/or minimizing their impact
Access network provider	Wireless Local Area Network	Scenario 5.12	34	Self-configuration	Intra-node configuration conflicts shall be detected and resolved	Mechanisms for detecting inconsistency of internal configurations of nodes and resolving such issues
Access network provider	Wireless Local Area Network	Scenario 5.12	35	Self-organization	Compatibility of -node configuration profiles shall automatically be validated before injection into the network	Mechanisms for detecting incompatibility of configurations of neighbouring nodes. Mechanisms for correcting cases of misconfiguration

Table 5: Access and Network players requirements

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Access and Core Networks provider	Access and Core Networks	Scenario 5.20	36	Self-configuration	The network shall be configured according to user context	Overall network configuration process according to the user context / player context and current local and global context *(The overall network configuration including the last mile, regardless of the access technology (wired or wireless), equipment, user and services)*
Access and Core Networks provider	Access and Core Networks	Scenarios 5.2, 5.3	37	Self-configuration	The network elements shall be configured in a multiplayers / multiservices context	Management and control process of access, core network and services in a multiplayer, multiservice context

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Access and Core networks provider	Access and Core Networks	Scenarios 5.2, 5.4, 5.5	38	Self-monitoring	The network shall ensure an efficient nodes monitoring with less impact on the performance of the network	Monitoring process of network fitting the needs requested
Access and Core Networks provider	Access and Core Networks	Scenarios 5.2, 5.4	39	Self-healing	The network shall be able to repair each failure happening in order to guarantee the service delivery	Healing process *(Locating the root cause of a fault, which has occurred in the network, correcting this fault and testing the resources of network, regardless of the last mile technology, the services used and the home access. (e.g. Detects and repairs IP connectivity). Advertise services and network (end 2 end management))*
Access and Core networks provider	Access and Core Networks	Scenarios 5.2, 5.4	40	Self-optimization	Manual performance management of the network shall be replaced with end to end automated and autonomic performance management process *Network Node shall be able to adapt and tune its own performance parameters in order to make proper decisions (self-optimization) with a user, network and services context. Decision shall be sent to the player for decision approval*	End to end network Node performance process
Access and Core Networks provider	Access, Core Networks, services (IMS) , content server (Application server)	Scenarios 5.2, 5.4	41	Self-healing	performance management of the network shall be improved with an automated process for detecting and eliminating congestion	Process of detecting and eliminating congestion. *(Define resources element that are under-utilized. Define the functionality needed to be added in the network. Add new functionality in the network with no services disruptions.)*

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Access network and network provider	Access and Core Networks	Scenario 5.2	42	Self-protection	The network and services shall be deployed, activated and delivered in secured manner	Security mechanisms to protect services and data with appropriate mechanisms from malicious attacks and unauthorized terminals/users. *(It can anticipate problems within the network. Functionality distributed in the Home network access and for services layer control)*
Network provider	All	Scenarios 5.2, 5.3	43	Self –Discovery	A new device on the network shall be able to discover its neighbours, inherit routing tables and other information (as today), inherit policies, learn its context and enhance, initialize its configuration settings	Discovery mechanisms
Network provider	All	Scenario 5.2	44	Self-adaptation	Backward compatibility shall be ensured. *(An autonomic network shall be able to perform all of the functionality currently available in today's networks)*	Integration process of legacy network and services
Network provider	All	Scenario 5.2	45	Self-provisioning	The network shall not prevent the user to create / edit / activate / desactivate / business policies. • Activated business policies shall be communicate d to all relevant network devices • All network devices shall adapt their configurations and operations to meet these business policies as best they can	User interface towards Business Policy Manager

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Network operator	All	Scenario 5.2	46	Self-configuration	The network shall not prevent the authorized user operating the network to override the configuration of a device that has been autonomically set	User interface towards configuration process
Network provider	All	Scenario 5.2	47	Self-Monitoring	The autonomic system shall have the ability to report all activities including; current active policies, current devices configurations and the reasons for those configurations. The reasons should include the relevant policy and, the relevant context parameters, the recent autonomic configuration changes and, the reasons for these changes	Monitoring process related to policy, resource configuration and context

Table 6: Services players requirements

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Service provider	IMS application server Content server	Scenario 5.2	48	Self-protection	The self-protection capability shall cover also the protection of user privacy and data. User data shall be sent/shared under user agreement	Mechanisms of accessing and controlling user data in a secure way
Service provider	IMS application server Content server User	Scenario 5.2	49	Self-protection	Multi level Self-protection for both network and services shall provide an authorized user with means to deactivate or activate the right self-protection levels in case of problems with self-protection prohibiting service access or causing other types of problems that might appear The self-protection capability shall cover also the secure services access *User shall always be authenticated.* *-An authorized user is able to access to the services under player's control.* *-Authentication server shall be distributed and duplicated. (in case of authentication server falls down)* *- Third party authentication to be granted by previous authentication in a secure way.* *- An authorized user shall be able to negotiate access to services.)*	Secure negotiation process to access services

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Service Provider	Ad hoc, Sensor Network	Scenario 5.7	50	Self-optimization	The network shall provide service support in mobility context	Mechanism to access user services in case of mobility *(Common services are provided to authorize mobile user and any other authorized user)*

Table 7: Access network / core network / Services players requirements

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Access network/ core network Services provider	Access network/ core network Services	Scenario 5.2	51	Self-optimization	The network shall be able to select and propose the best access service to the mobile user for resource optimization purpose (e.g. Energy saving, Offloading)	Mechanism to select the best access network for mobile user with associated services in use.
Access network / core network Services provider	Access network / core network	Scenario 5.2	52	Self-optimization	The network shall provide adapted services according to user context	Mechanisms to select the best way to deliver services with user context. *(change access, prioritized services, etc.)*
Service Provider, Network Operator	Ad hoc	Scenarios 5.7, 5.4	53	Self-optimization	The network shall guarantee stable behaviour when changes happen (conflict free) Mechanisms to adapt network changes shall not cause inconsistencies in the network or possible deadlocks	Mechanisms to adapt network changes
Service provider Network Operator	Ad hoc	Scenario 5.7	54	self services	The network infrastructure shall support the provision of private services, in addition to the public ones	Provisioning, authorization and authentication mechanisms of public and private services

Table 8: Content player requirement

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
Content provider	Application server	Scenario 5.2	55	Self-optimization	Content provider's Application shall request to the network guaranteed SLA linked to the provisioning and configuration of services, and the network shall be able to guarantee Content application SLA request	Translation mechanisms of user requirements (SLA user profile service profile) into technical requirements within the network (QoS) in order to make the network Application-aware *(Define the resources needed and the functionality needed to provide the (new) services)*
Content provider Services	Service provider (IMS, ISP), content provider Home area network	Scenario 5.2	56	Self-optimization	Interaction between services shall be conflict free	Mechanism of selecting a given service without impacting another active one *(Interaction between services for advanced services. Adapt services with new services activated or closed by user. Identified the prioritized services. Identify the adaptations needed)*

In order to operate Future Networks, knowledge and information are key issue. Table 9 contains a set of requirements on the information and knowledge model needed to build and operate future networks. It is indeed, cross-layer and cross-network environment oriented.

Table 9: All players requirements

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
All	All	Scenarios 5.2, 5.4, 5.5	57	Self-monitoring	The network shall monitor its environnement according to SLA in multipartner use case	Monitoring mechanisms towards assuring SLA agreements between all players *(deployed at the borders in order to identify responsibilities and provide network interoperability)*
All	All	Scenarios 5.2, 5.4, 5.5	58	Self awareness	Networks of involved Players shall share needed knowledge with other players' networks or network elements without requiring human intervention	• Process to describe, to retrieve and to learn knowledge • Process to adapt, to evolve) to the evolution of the network. • *(Cognitive (function) information could be used to retrieve context.)* • Process to translate high level business goals into • specific technical objectives (e.g. configurations) s on the infra structure for enforcement p and execution purpose. • Process to retrieve control/secure/authenticate and encrypt information to be sent to another player. • Process to retrieve knowledge from statistics, estimation and information
All	All	Scenarios 5.2, 5.4, 5.5	59	Self awareness	Information exchanges shall be governed by specific agreements in secured manner and up to date, certified by the sender. Information exchange shall be adapted to the requester	Process of exchanging information within agreement in secured manner and adapted to the requester

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
All	All	Scenario 5.2	60	Self awareness	The knowledge shall be described in a formal way in such a way to be understood and easily interpreted by the Autonomic Functions Context information shall be defined in standardized way	Mechanisms and process to describe and specify knowledge
All	All	Scenario 5.2	61	Self management	Players' Management Systems shall dynamically manage their allocated virtualised resources	Process to manage virtualised resource (communication, processing, storage, etc.) *(supervision, creation, maintenance, allocation, optimization of (overlays) virtual resources)*
All	All	Scenarios 5.2, 5.4, 5.5	62	Self-management	The autonomic network shall not prevent an authorized user from the ability to control and close higher level Control loops *in particular* (decision entity)	The management process in the shared decision schema involving administrator. *(Mapping between classical management architecture and autonomic management)*
All	All	Scenario 5.2	63	Human in the loop	Autonomic function shall provide a hook for man in the loop, to enable or disable the autonomic function. Autonomic function shall provide log of history of decision making. Autonomic function shall communicate tentative decisions (especially before confidence has been build) to enable closure of the control loop by the human when required	Monitoring process Decision sharing process (The means to communicate to the human operator "tentative" decisions arrived at by autonomic function(s) (i.e. before the decision is executed by the autonomic function, e.g. a decision to change a parameter value on a managed entity), Such means could be through logging "tentative" decisions or through some other direct notification means), The means for the human to approve or override the decision proposed. (Operator need to build trust and confidence on the autonomic function)

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
All	All	Scenarios 5.2, 5.4, 5.5	64	Self-awareness	The network may need to be configured according to business objective/goals/ policies (Operator's policy)	Instantiation, enforcement and execution processes of operator policy in the network
All	All	Scenario 5.2	65	Self-management	The autonomic network management shall be backward compatible with legacy management process (co-existence or ability to switch off some Autonomic management aspects and revert to manual management system)	• Process of integrating legacy management and autonomic management • Process of mapping legacy management and autonomic management
All	All	Scenarios 5.2, 5.4	66	Self testing Self Diagnosis	Network as a whole shall provide level of self testing after attempting self healing / repair or after configuration changes	Testing and Diagnosis processes
All	All	Scenarios 5.2, 5.4, 5.5	67	Self configuration (plug and play) and other Self* functions	Autonomic functions shall be designed in a way to ensure multi player implementation support (open interface)	Interface design and generation process

Players	Network environment	Scenarios from clause 5	RQ ID	Autonomic Functionality	What is the requirement	What need to be automated
all	all	Scenario 5.2	68	Self-configuration	While the autonomic network is expected to self-configure resources to fulfil the requirements of subscriber/customer-oriented services, the same autonomic network, shall also automatically self-configure so as to provide universal services (Emergency services, lawful interception) as well). Up to date granted location data shall be provided to the service, as it is used to control nomadic user, and geo-localized services like emergency services and Universal services Lawful interception shall be applied in an efficient way by the different authorized users (in charge of services or connectivity) involved in a multi-players model	Universal services integration process

4.6.3 A guide towards implementation of the requirements and associated autonomic functionality and automated processes

- The implementation should be achieved using architectural Functional Blocks (FBs) that enable to realize (implement) autonomic behaviours in a network and their input interfaces. The **autonomics FBs** that enable to realize autonomic behaviour (autonomic functionality) in a network architecture (network environment) are defined by the GANA reference mode l [i.15].

- The actual autonomics FBs that need to be operational in a particular reference network architecture (network environment) are defined in a corresponding so-called "*autonomicity-enabled reference architecture*" – created as a result of instantiation of the GANA onto the particular reference architecture. Such instantiations of the GANA onto various references architectures is work being done by AFI.

- For a particular network environment, the **implementer of the requirement and associated autonomic functionality** should use the corresponding "*autonomicity-enabled reference architecture*" e.g. "*autonomicity-enabled mesh/ad-hoc network architecture*", "*autonomicity-enabled BBF reference architecture*", autonomicity-enabled IMS reference architecture and autonomicity-enabled EPC reference architecture respectively, to analyze the requirement and derive behaviour of the autonomics FBs, their communication flow and data exchange on reference points /interfaces that enable to implement the requirement.

5 Use Case and Scenarios

5.1 Use Case and Scenario Template

Template

Table 10 depicts the template defined in order to capture relevant data related to the AFI Use Case and Scenarios. It is composed of the following fields:

- Title
- Description/Story
- Network Environment(s)
- Problems
- Functions Impacted
- Systems Involved
- Indicators / Evaluation criteria /Metrics
- Players
- Beneficiaries and the Benefits

This Use Case and Scenario Template is linked to the Requirements Template (table 1 column "Scenarios"). Indeed, both share two fields "Player" and "Network Environment".

Table 10: Use case and Scenarios Template

Title	**<Scenario Title>**
Description/Story Use Case	<steps / scenes>
Network Environment(s)	
Problems	<be accurate, specific, user-facing>
Functions Impacted	<system view>
Systems Involved	
Indicators / Evaluation criteria / Metrics	
Players	Network Operator: Content Provider: Vendors/ Manufacturers: Application Developers: End User:
Beneficiaries and the Benefits	

Categorization of the Use Cases and Scenarios

Based on the master Template of table 10, the following tables are the instantiations of this template to relevant Use Cases and Scenarios. Ten Use Case and Scenarios (one per sub-clause) are selected in order to illustrate this AFI approach. These Use Cases and Scenarios are listed without any consideration of categorization or classification.

This list could be extended to other Use Cases and Scenarios within the AFI scope.

5.2 Autonomics in legacy network (NGN)

Table 11: Autonomic in legacy network (NGN)

Title	Autonomic in legacy network
Description/Story Use Case	The legacy network is composed of a panel of players which need to cooperate in order to provide user services with associated QoS and security as prerequisite for launching a service. The number of equipment and players is continuously increasing in order to cope with the development of new services and to satisfy new demands/customers, while the manageability of this legacy infrastructure and cooperation among these players is reaching the limits of human capacity. Adding new service needs is challenging. Indeed, more and more strong cooperation between all the players even the user is required in order to provide these new services. This multilateral cooperation is handled manually without automatic process, because the case by case manner needed to address the particular constraints of each player. Information exchange provides the context, of the user, network and service. The Service Provider is expecting a service delivery through an ubiquitous infrastructure as well as a transparent management through this multi-player infrastructure, such as programmable overlays of virtualised resources (communication, processing, storage, etc.). The major shift here is the dynamic provisioning whatever the underlying physical resources. Users are not techno aware. They just want plug and play services with no configuration and they want to select/use services existing in the marketplace [i.11], [i.10].
Network Environment(s)	All
Problems	**Current Management practices:** Within the current network management practices, a network administrator needs to manually interact with infrastructure and players. Incoherence in the management could happen between the different agreements: Services interactions conflict are manually resolved. Equipment shall be manually configured by users/administrators in order to connect to the infrastructure. Infrastructure is not updatable, optimisable, etc. End to end management needs the involvement of numerous experts at each level of the operation organization (vertical layers and horizontal domains) because monitoring information is provided with no coherence and no consistency. Detect congestion or adapt the performance node is difficult to realize between players. Seamless continuity of services is difficult to deliver, because services are statistically configured for a type of access network and for a set of users. Service continuity needs to analyse the user environment in real time (whatever the state of network is) in order to reconfigure the network and provide adaptable services continuity.
Functions Impacted	Management, control, transport, Applications
Systems Involved	Management system Control system Media transport system
Indicators / Evaluation criteria / Metrics	**Zero configuration** for users' equipments connected to the Home area network with IP connectivity through Self configuration mechanisms. **SLA agreements** for commercial services and universal services shall be met within multi-player environment thanks to network interoperability and monitoring mechanisms. These mechanisms shall be able to identify responsibilities of each player in case of degradation or deviation from the SLA agreement. It can be achieved through Self monitoring mechanisms. **Level of human involvement in the network management:** a control plane and the management plane shall orchestrate self-optimization of different resources (nodes, virtualised nodes, overlay functions, last mile, etc.) of the network belonging to different players with coherence, consistency, security in order to provide service continuity adapted to user environment with less human intervention under confidence and trust conditions. It can be achieved through Self organizing mechanisms. **Improvement of processes:** delivery time, level of security quantity and relevance of alarms reported with less human intervention.

Title	Autonomic in legacy network
	These 4 indicators need a decision provided in global coherence with situated and appropriate view. Indeed, information exchanged between players should provide knowledge with guarantee of security, integrity, privacy and described within a common language. This knowledge shall be adaptable, up to date, consistent, etc.
Players	Network operator
Beneficiaries, and the Benefits	**Operator:** reduction of OPEX by minimizing the time and effort needed for managing network devices by the network management personnel (i.e. administrators). **Manufacturer:** by updating existing products and developing and selling new product lines embedding new and advanced features interoperable. **Users and other players**: could use plug and play infrastructure.

5.3 Auto-Configuration of Routers using Routing Profiles in a Fixed Network Environment

Table 12: Auto-Configuration of Routers using Routing Profiles in a Fixed Network Environment

Title	Auto-Configuration of Routers using Routing Profiles in a Fixed Network Environment
Description/Story Use Case	The network operator, network provider, or an enterprise, an ISP or simply a actor/player who wants to build a network from scratch, has just purchased routers designed following GANA principles (see ETSI GS AFI 002 [i.15]) and has been advised by the manufacturer (consults the device manual) as to what minimal manual settings user (the player purchasing the equipment e.g. operator) needs to configure on the new router before initializing the router on a link. What he has learnt also, is that user needs not worry anymore about the following (as it is the case today): - Thinking of dividing and when to divide his/her network into Routing Areas while taking into account the Capabilities of routing devices. - Sitting in front of each router, configuring the router by activating a Configuration Profile via the Command-Line Interface (CLI). User (the player purchasing the equipment) has been told that from the moment user builds the network from scratch, provided that user deploys first the following systems required for supporting the plug and play of the "autonomic" routers: - A System that supports publish/subscribe, query and find type of services for **Information/Knowledge** such as Capabilities of network elements, Profiles, Goals and Policies of the autonomic network, pointers to resources and Data, and other types of **Information/Knowledge.** - Network-Level Autonomic Manager Elements (referred to as Network-Level-Decision-Elements in GANA (see ETSI GS AFI 002 [i.15])). The "User" only needs to do the minimal manual settings to initialize a router on a link, since the GANA based network would start automatically taking care of performing full configuration the routers into service as well as network partitioning as the network grows.
Network Environment(s)	Access, Edge and core network
Problems	**Current Configuration practices:** With the current network management practices, a network administrator needs to initialize a router on a link after the purchase, and manually create a configuration profile for the router while at the same time think how to assign the router to a routing area (talking about large ISPs) when taking care of network expansion and the benefits of dividing a network into areas. **Current Configuration technology:** **(A):** With current technology that comes with a router (as manufactured by the manufacturer), the device can only activate factory settings upon initialization on a link(s) while requiring the operator to manually configure its interfaces and routing protocols. **(B):** On the other hand, with current network management technologies, though some limited remote configuration management commands/data can be issued/communicated to a router, this can only be done after a human has done some initial configuration of the device e.g. IP interfaces (especially the management interface) has been configured. The configuration commands or data do not cover complete or partially complete configuration profiles for the device. **Current Discovery Capabilities and technology:** The current technology that comes with a router does not enable the router to discover entities such as Autonomic Manager Elements (i.e. Network-Level-Des in the GANA Model) in the network that are tasked with providing each routing node/device with a Configuration Profile that tells it the role the router should play (whether to play the role of an access/edge, core or

Title	Auto-Configuration of Routers using Routing Profiles in a Fixed Network Environment
	area-border router, etc) as well as the interfaces for which it should configure some routing protocols and their parameters. Though Ipv6 brings some aspects of neighbour discovery allowing on-link neighbouring nodes to discover each other and some basic parameters for auto-configuration, these enabling Ipv6 mechanisms are still limited and need to be augmented towards more advanced Auto-Discovery, to include even discovery of Capabilities of devices that plug into the network. **Current Capabilities in relation to Device Description and Advertisement technology:** The current technology that comes with a router does not enable the router to ***self-describe*** its *Capabilities* as a device in order to then ***self-advertise*** the *Capabilities Description Model* to the entities that need such vital knowledge such as the Network-Level-Des (Decision Element) that require such knowledge in order to assign a role for the newly attached router and to give it a Configuration Profile which shall be used by the router to ***self-configure***.
Functions Impacted	<system view>
Systems Involved	Core Routers Edge Routers Access Routers
Indicators / Evaluation criteria / Metrics	
Players	Network operator
Beneficiaries, and the Benefits	**Operator:** Reduces OPEX by minimizing the time and effort requirements needed for configuring network devices by the network management personnel (i.e. administrators). **Manufacturer:** Need not explicitly provide own management software tools for configuration of each type of the network devices, and by designing GANA conformant devices, interoperability with other GANA conformant devices is guaranteed.

5.4 Self-Management of Coverage and Capacity in Future Internet Wireless Systems

Table 13: Self-Management of Coverage and Capacity in Future Internet Wireless Systems

Title	Self-Management of Coverage and Capacity in Future Internet Wireless Systems
Description/Story Use Case	In a wireless infrastructure, network management and, in particular network planning, becomes a challenging task because of the volatile and unpredictable nature of the wireless medium and the mobility patterns of terminal devices. Due to the strong demand for efficient wireless resources utilization, wireless network planning and management is a sophisticated task, which, more often than not, requires expert knowledge, especially in a dense urban environment. In cases where homogeneous and heterogeneous wireless networks operating under different administrations reside in the same geographical area, the complex problem of efficient wireless resource management arises, under several constraints. Network nodes (i.e. access points) that have several configuration capabilities and observe their local operational status should coordinate for network management. A centralized approach is not effective due to scalability and complexity issues. Thus, a more localized and distributed architecture is necessary for the orchestration of various heterogeneous or homogenous access points (Aps) or base stations (BSs). This use case presents the steps taken by self-manageable Aps or Bssin a wireless network: a) to make deductions about its operational status; b) to proactively react to internal/external triggers; and c) implement the necessary actions based on its decision mechanism, thus seizing the need for human intervention.
Network Environment(s)	Wireless Access Network
Problems	Autonomic and localized management of variable capacity and coverage requirements as well as of the configuration actions for the identified symptoms in the wireless medium e.g. high load, interference. Some, management problems that will be addressed: a) Efficient channel allocation among homogeneous Radio access technologies (RATS (e.g. IEEE 802.11 [i.14]) by making better use of the channel allocation conflicts. b) Activation or de-activation of access points/base stations (e.g. IEEE 802.11 [i.14]) assessing the specific characteristics of the specific network area. c) Base stations-assisted user equipment handover (vertical, horizontal).

Title	Self-Management of Coverage and Capacity in Future Internet Wireless Systems
Functions Impacted	The following autonomic functionalities are provided: • Self-optimization of Aps/BSs capacity and coverage features during their operational state in order to proactively and autonomously configure them according to local and global requirements. • Self-configuration of Aps/BSs in the context of their pre-operational state and autonomous selection of execution options during their operational state. • Self-organization: In a distributed and collaborative way the network nodes (Aps/BSs) decide the optimal formations according to their knowledge models and policy rules/SLAs that are locally stored and updated or provided by the respective network operators. • Self-awareness: Access points by sensing the wireless medium and communicating with neighbouring network nodes exchange knowledge data, KPIs as well as policy rules in order to develop their situation awareness for the next nodes. User devices are also used as monitoring points from the respective Aps/BSs.
Systems Involved	Wireless access points or base stations as well as user devices (e.g. mobile devices) are the main systems of this use case
Indicators / Evaluation criteria / Metrics	• Measure wireless resources (or capacity) usage improvement (cells load, cell throughput) juxtaposed with communicational or computational load (e.g. transmission overhead) due to the introduced mechanisms. • Pattern recognition and knowledge extraction processes will be evaluated with respect to their classification ability, i.e. how well they can identify a problematic situation and its corresponding solution. • The applicability of the dynamic combination of rules will be evaluated with respect to the computational resources it will require and compared against the baseline approach (application of static rules). • Optimize the induced solutions and minimize delay.
Players	**Network Operator** **Manufacturer** **End user**
Beneficiaries	**Network Operator:** will minimize the cost related to network management and maintenance (OPEX), while having the ability to identify optimization opportunities and handle proactively alarms. More efficient usage of the available resources means less energy cost and better Quality of Service. **Manufacturer:** will develop and update the software for self-manageable Aps/BSs. Improved product portfolio with optimized performance status. **End user:** will be benefited by receiving better QoS features as well as fewer disruptions.

5.5 Cognitive event management (Fault/Anomaly/Intrusion Detection)

Table 14: Cognitive event management (Fault/Anomaly/Intrusion Detection)

Title	Cognitive event management (Fault/Anomaly/Intrusion Detection)
Description/Story Use Case	Advantages in telecommunication networks have fuelled the rapid growth of new services. User mobility has become an important factor in the quality of service provision for every network operator. Current network management requires specific human intervention to oversee network behaviour and ensure that they deliver services requested. Every day running tasks include the ongoing detection of unusual or undesirable behaviours in order to address issues like fault diagnosis and problem resolution. The achievement of these goals is extremely difficult in distributed wireless environments where it is necessary to correlate information from different network levels and network elements. Typical problems like anomaly detection, fault prediction or intrusion detection can be addressed through the identification of unusual behaviours. The idea is based on the fact that the occurrence of faults notification and alarms should follows patterns, which, upon recognition, can be used to predict the fault's occurrence. The last one ensures the remedial actions that can be taken beforehand in order to achieve the system functioning without interruptions. The above processes should be automated by an autonomic core network and human intervention should be minimized, thus providing a viable solution for self-healing in wireless networks. Thus, when an anomaly is discovered, the involved network elements can use alternative setting profiles or configurations. The scenario is realized in the following specific steps: 1) Continuous monitoring of selected features in the prediction model will provide at each given time a view of the element's internal functions as well as its environment. This information will serve as the current situation input to the fault prediction model (a model which is able to proactively detect fault and instability in the network, this model could learn on the fault which could happen according to within the prediction model. 2) Monitoring data is classified into three categories based on the source: network sources, system sources and application sources (e.g. IP packets, syslogs, application logs, MIBs). 3) Appropriate mechanisms take part to associate the current situation with the patterns recognized and depicted in the prediction model. 4) In case the association results point to an imminent fault or anomaly, preventive measures are undertaken and selected by a pool, where symptoms and measures are paired. The measures might point to an alternative configuration, traffic rerouting, load balancing, node isolation, etc. 5) A feedback loop with the knowledge base is also envisaged to update and improve the prediction model on a regular basis. 6) Moreover, artificial intelligence methods (e.g. unsupervised) will contribute to the training process by identified unknown alarms or attacks. This enables the cognitive capability of detecting previously "unseen" attacks or faults. This enables the network to assess the threat earlier than traditional mechanisms. 7) In addition, the decision mechanisms ensure that an event based on monitoring data and existing knowledge can be characterized as an alert or possible alert. 8) In execution step, the actual reconfiguration takes place. Parameters are tweaked or alternative preventive measures are taken in order to avoid the imminent fault or attack. 9) The execution process is realized in activation of planned processes or information dissemination about the current status of intrusion detection or anomaly detection to other nodes.
Network Environment(s)	Wireless access Environment

Title	Cognitive event management (Fault/Anomaly/Intrusion Detection)
Problems	The dynamic wireless networking environment and the mobility of the devices give off problems that increase the network management complexity. The emergence of common problems can affect a much larger number of users and services. Therefore, the cognitive deduction for event management can improve current network management procedures and some problems that will be addressed include: Anomaly detection, as the realization of unusual or undesirable situations. For example, detection of the nature of traffic anomalies in a wireless network is a vital problem, because of the volatile and unpredictable nature of the wireless medium and the resource constraints of mobile devices. Available TCP mechanisms cannot discern timeouts caused by short scale fluctuations in the wireless medium status from delays due to congestion or any other cause e.g. environmental factors, interference. Usually, traffic anomalies can create congestion in the wireless links and stress resource utilization, which makes early detection crucial from an operational standpoint. Of course, a non detectable anomaly event at one network level could be easy to detect using monitoring data from different networking levels. In a real distributed environment, the challenge point is the collection of appropriate statistics at the local level and the pool of these at the regional level to detect these patterns following a bi-directional reasoning. Moreover, the task of anomaly detection can be useful for fault isolation and identification. Another problem that can be addressed is the enhancement of the existing intrusion detection mechanisms. Most current network "intrusion detection systems" (IDS) make use of techniques which rely on labelled training data (e.g. data mining-based or signature-based). This approach has shortcomings, such as the expensive production of training data or the difficulty in detecting new types of attack. Moreover, the cognitive mechanisms of anomaly detection, which rely on unsupervised methods, can help the network be trained with unlabelled data. This enables the cognitive capability of detecting previously "unseen" attacks. In this way, the network assesses the threat earlier than traditional IDS mechanisms.
Functions Impacted	The self-awareness autonomic functionalities are provided to facilitate self-protection and self-healing: • self-awareness, as continuous knowledge building process to assess operational status and finding of patterns • self-protection, proactively compensating/overcoming foreseen events • self-healing, reactively responding to unplanned events (e.g. failures) and providing corrective actions
Systems Involved	Wireless Access Points, Routes, Firewalls, IDS
Indicators / Evaluation criteria / Metrics	• Precision (as the ratio of correctly identified failures to the number of all predicted failures). This ratio refers to the number of true positives prediction to the total number of predicted positives analysed by the prediction model, against the detection rate which are predicted, i.e. the proportion of total true anomalies that are detected • Recall (as the ratio of correctly predicted failures to the number of true failures) • Precision/Recall-Curve (as mechanism to precision over recall for various threshold levels • In case of statistical approaches, the performance of the statistical algorithms can be expressed in terms of the prediction time and the mean time between false alarms
Players	• End user • Network operator • Manufacturer • Service Provider
Beneficiaries	**End user:** satisfied users (enjoy better services), thus they assess positively the network and services **Network Operator:** reducing human intervention **Manufacturer:** feedback from specific network management events may lead to better product development **Service Provider:** convergence to achieve the desired QoS

5.6 Coordination of Self-* mechanisms in autonomic networks

Table 15: Coordination of Self-* mechanisms in autonomic networks

Title	Coordination of Self-* mechanisms in objectives autonomic networks
Description/Story Use Case	The goal of this scenario is to capture the requirements stemming from the introduction of various Self-* mechanisms in to the network elements. In particular, it highlights the need for proper coordination among the Self-* functions and control loops of each individual network element, which may have the same or different objectives.
Network Environment(s)	Any network element (fixed/wireless) equipped with one or more Self-* mechanisms Network Operator (NO) Mobile devices (in case of mobile networks, assisting role)
Problems	Each autonomic element performs a self management in a selfish manner, by executing its own control loop independently of the others. Will provide Performance deterioration (due to uncontrollable behaviour of Self-* mechanisms) as perceived by the monitored, preset KPIs. Interactions between controls loops could redefine the action of an equipment with no coherence and crash the system.
Functions Impacted	<system view>
Systems Involved	
Indicators / Evaluation criteria / Metrics	The performance of the network converges at a desirable operating point e.g. in terms of achieved throughput: The network converges to a desirable and stabilized operating point. Functionality in management/control planes for coordinating simultaneously running Self-* functions/control loops. Advanced knowledge sharing mechanisms. Efficient KPI management. Proper selection of speed, convergence and stability criteria. Interactions of control loop involved in the reaction of an equipment shall be analysed. A control loop not stable shall be deactivated.
Players	Network Operator Content Provider Vendors/ Manufacturers Application Developers: End Users
Beneficiaries	**Manufacturer:** provide a manageable autonomic system **Operator:** • Could control loops and deactivate it (them) if they do not reach the stability objective. • Could control Interaction between control loops of different manufacturers could be managed.

5.7 Autonomic Network Monitoring

Table 16: Autonomic Network Monitoring

Title	Autonomic Network Monitoring Scenario
Description/Story Use Case	The scenario refers to autonomic network monitoring in a dynamic environment. Other services may also be deployed following similar principles, as discussed below (see also figure 1). In the following scenario, the network administrator desires to have a complete view of the network topology and to be able to assess network conditions, e.g. calculate various performance metrics. An overlay network is automatically set up by participating nodes, which (overlay network) hide any details of the underlying infrastructure, such as links established or torn down, failure of nodes, mobility of nodes, etc. Any (monitoring) service may now be built on top of a small set of well-defined abstract APIs, which allow interactions between nodes and the rest of the overlay network. There is no need for centralized control or infrastructure in order to set up new services. All the necessary functionality is shared by peers in the network. Some functions are delegated to more than one node for higher reliability. Moreover, the overlay network is designed to be established autonomously with minimal end-host configuration and human intervention. Thus, it could be argued that rapid deployment of new functionality may be achieved in the network. The network monitoring scenario is realized in the following specific steps: 1) An autonomic node initially searches for neighbours in its proximity, and if successful, joins an ad-hoc network. 2) After being able to communicate with neighbours at the physical layer, it participates in a peer-to-peer overlay network by using pre-installed software. An overlay topology (e.g. ring) is formulated by all participating nodes in the ad-hoc network. While nodes join or leave the network, the overlay ring is autonomously updated by applying specific ring maintenance protocols. 3) Any nodes connected to the p2p network are able to store or retrieve information related to the services using a small set of functions that are based on Distributed Hash Tables (DHT). Autonomicity is derived by the fact that nodes do not need to address network topology changes, e.g. due to node failures. 4) When an autonomic node wants to provide a new service to its peers, it should retrieve the necessary data from the network. Data is stored beforehand by peering nodes in the overlay network using predefined keys, as discussed in the following examples. Therefore, each service is implemented through the cooperation of a large number of autonomic entities that interact by storing and retrieving meaningful keys across the overlay topology. In this way, the network administrator can achieve autonomic functionality that emerges in a decentralized manner without explicit action or control. EXAMPLE 1: The provision of a visualization service for an (ad-hoc) network requires knowledge of all the operational nodes/links/functions in the network. In an autonomic scenario, all the network nodes store topology data to one location which may be a network node. This storage location may be dynamically chosen. A common key, included in the pre-installed p2p software, is used for this operation. If necessary, data redundancy is achieved automatically by the selected peer to peer protocols without any intervention from the administrator or the network nodes. Consequently, all topology information is available to any node aiming to provide a new service. EXAMPLE 2: The provision of a performance monitoring service for all the links in an (ad-hoc) network is based on similar techniques as in the previous example. The difference in this example compared to the previous one is that multiple keys are now necessary for storing monitoring information for each operational link in the overlay network. A simple function on the IP addresses of the nodes terminating a link may be used for generating necessary keys. This function is included in the pre-installed software of each node.
Network Environment(s)	Mobile Ad-hoc Networks (MANETs) (dynamic topology, unreliable operation of nodes and links, lose control of nodes) The scenario may also be applied in other environments such as fixed/wireless networks.

Title	Autonomic Network Monitoring Scenario
Problems	In a dynamic environment with frequent topology changes and link failures, centralized approaches suffer from low service operational quality –e.g. performance is reduced when connectivity is not feasible to the central node-, have limited scalability (e.g. data is stored in a single node and service degradation is expected by increasing the incoming requests)), and resilience (e.g. the central node is a single point of failure). The creation of overlay networks is proposed as a decentralized solution for designing and providing (monitoring) services. These overlay networks are based on p2p protocols and provide storage and retrieval functionalities. Resources may be combined in a distributed manner and the following characteristics may be supported: scalability, decentralization, high availability of the provided services, fault-tolerance. However, p2p protocols are capable of handling dynamic incoming / outgoing nodes and registration / deregistration of resources but still under the assumption of a fixed topology and minimum uncertainty. Thus, specific mechanisms for topology formulation and maintenance have to be applied. These mechanisms have to be able to converge after network changes and not to impose high operational burden to the overlay network.
Functions Impacted	The following autonomic functionalities are provided: • *Self-configuration of the autonomic node*. Each autonomic node recognizes its neighbours, joins the overlay network and is able to store and retrieve data autonomously. • *Self-organization of the network* – establishment of the network and the communication links. Join and leave node requests are handled autonomously. • *Self-optimization* – data and services are distributed uniformly among the participating nodes. The established overlay topology is maintained and updated after changes in the network.
Systems Involved	Core/Edge Routers End Systems connected in a wireless infrastructure
Indicators / Evaluation criteria / Metrics	Network Bootstrapping: 1) How many messages are exchanged in order to achieve stabilization in conjunction with the network size and the network density? Storage and Querying: 1) What is the average cost (in messages) order to store specific amount of data in conjunction with the network size and the network density? 2) What is the average querying cost of a key? Reaction to topology changes: 1) How many messages are exchanged in order to achieve stabilization in conjunction with the network size and the network density? 2) How many messages are exchanged in order to achieve DHT stabilization in conjunction with the network size and the network density? One node chooses to query all Z keys. How many keys are unreachable? How is the redundancy ratio connected to the failure percentage?
Players	End users Network operator Manufacturer Service provider
Beneficiaries, and the Benefits	**System Administrators:** Responsible for network monitoring and management. Monitoring services are automatically adapted to network changes. **Vendors:** Implement necessary functionality to core/edge routers. Network infrastructure has to support necessary functionality for supporting autonomic services. **Application Developers:** Build new services without addressing any challenges regarding the underlying network infrastructure. **Manufacturers:** Design personal devices able to connect to any autonomic network with minimum software pre-installed. **End Users:** Accessing services provided by other peers with minimum user intervention and any support from (centralized) infrastructure.

5.8 Scenarios Overlay Virtual Network Service Breakdown

Table 17: Scenarios Overlay Virtual Network (OVN) Service Breakdown

Title	Overlay Virtual Network (OVN) Service Breakdown
Description/Story Use Case	This scene focuses on how a network can react to problems disrupting the consumption of a given OVN service, for example photo sharing (an OVN is a virtual network allowing users to access services and content and located on top of the physical network).The OVN targets connectivity problems or equipment failures that can result in a full service outage. Once this situation has taken place, the OVN will first try to diagnose the root cause and eventually re-establish the service by automatically performing some configuration actions. In case automatic recovery is not feasible, the problem will be communicated to the customer and/or the service operator so manual interventions can be performed. The following paragraphs describe in detail the different scene steps, considering a photo sharing service. Note that the same concepts can be applied to other OVN services like video streaming. Bob, or an agent acting on behalf of him (hosted on the management device on Bob's side), detects connectivity problems. The agent will try to diagnose the cause of the problem locally with the information it has, which can be enlarged by conducting available tests. If the problem is not local, agents in Alan's HAN or in the ISP's access network will be contacted for further diagnosis. In the latter case the agent may, if necessary, use services provided by the OSS belonging to the ISP to perform a set of additional tests to retrieve relevant information about network configuration and status. Once the diagnosis results are available, the agent will try to solve the problem by executing the appropriate actions based on the diagnosis results and corresponding management policies. For example, it may try to reset the residential Home Gateway, re-establish its configuration parameters, or assign a free wireless channel to a disconnected device, etc. In the case where self healing is not possible, the agent may request some action from Bob, such as manually resetting his router. This will require some means of communication with him, like the PC or TV screen, an SMS message sent to his mobile, etc. Such a communication would also be useful in the case where the root problem lies outside the HAN, and the operator / service provider is already working to resolve it ("OVN service temporarily down due to XYZ. Your service will be available again in 15 minutes"). Note that for some types of problems a smart communication concept will be required, e.g. sending an SMS message in case of a complete outage of the xDSL line. Eventually Bob may need to call the helpdesk. In this case, the diagnosis report generated automatically will guide the technician and reduce the time needed to solve the problem. A trouble ticket will be also automatically opened and passed on to the relevant OSS in case it is required to solve the problem. Since, sometimes, the same problem may be affecting different HANs, the OVN will temporarily store diagnosis results, including local HAN diagnosis, to aggregate problems and detect common causes. Feedback from the results of corrective actions taken would also enable self learning and tuning of the diagnosis process.
Network Environment(s)	Wired and wireless: • Home Area Networks (HAN) • Small Office Home Office (SOHO)

Title	Overlay Virtual Network (OVN) Service Breakdown
Problems	1) Distributed diagnosis. Different mechanisms to perform distributed diagnosis should be analysed. These mechanisms should be flexible enough to smoothly include new diagnosis cases. It shall also be possible to share diagnosis information between different HANs and ISP networks. 2) Accessing all relevant events and context information. In addition to the above, it should be ensured that all relevant information for the diagnosis is accessible. This includes the intelligent processing of events issued from any devices inside the home environment, from the OSS/BSS infrastructure of the operator, and from a variety of other possible sources. 3) Interaction with the user. Although autonomics prefers to foster a zero touch approach, sometimes it may be necessary to request the user to perform simple actions himself. User friendly ways to communicate with the customer should therefore be studied. Depending on the type of the problem being diagnosed, the proper channel for information and interaction shall be selected. 4) Self learning. Being able to automatically improve the diagnosis algorithms by incorporating the experience from past corrective actions, even from unsuccessful ones, is a very interesting challenge since it would allow the network to automatically adapt to changing situations and shares this knowledge among multiple HANs. 5) Self healing. Automatic problem correction should follow operator's policies and lead the system to a stable state. With reference to the "Service Breakdown" diagram below (figure 5), once the node has detected (1) a violation of some monitored function or (2) a fault on the network and / or device, then the Fault-Detection-ME (see definition of Managed Entity (ME) in ETSI GS AFI 002 [i.15]) will liaise with the Fault-Diagnosing-DE (see definition of a Decision Element (DE) in ETSI GS AFI 002 [i.15]) to determine the root cause. Where a root cause and solution are deduced, the network will try to conclude the next step in terms of healing itself. If a solution is not known or cannot be calculated, then it is possible that some manual intervention is required. In such instances, then management agents should learn the resolution of this fault for future reference (figure 5).
Functions Impacted	The following autonomic functionalities are impacted: • *Self-configuration* of the autonomic agent. Each node recognizes its neighbours, joins the overlay network and is able to store and retrieve data autonomously. • *Self-organization* of the network – establishment of the network and the communication links. Join and leave node requests are handled autonomously. • *Self-healing* – reactively responding to unplanned events (e.g. failures) and providing corrective actions.
Systems Involved	Operators ISP Source and Destination access networks Core/Edge Routers HAN devices – Home Gateway, End User Devices
Indicators / Evaluation criteria / Metrics	1) How to connect the components deployed in different IP addressing spaces? 2) How to send configuration commands to the different HAN devices and retrieve management information from them? How does this fit into existing device management solutions currently used by operators (mainly based on TR-069 and related standards)? 3) Initial modelling of the probabilistic network (decision trees) for each possible use case. 4) How the agents will identify and authenticate in the OVN? 5) How to handle problems that have been resolved either automatically or by interaction with the end-user only? What amount of information is relevant for the administrator?
Players	Network Operator; Vendors/ Manufacturers; End Users

Title	Overlay Virtual Network (OVN) Service Breakdown
Beneficiaries and the benefits	***Operator's perspective:*** automatically solving problems in the HAN has two main advantages for the operator: it saves resources (both human and computing) needed and improves the customer experience. However, the autonomic agent has to ensure that these automatic actions strictly follow the operator policies. As part of the autonomic concept, self-healing processes are intended to automatically recover the status of a system after a deviation from its normal working conditions. Self-healing actions are normally expressed in the form of management policies that instruct the systems what to do under certain circumstances. To implement these actions, the system shall first be able to know itself and its context. This is a fundamental requirement for any autonomic framework. The system shall be able to monitor the service, the devices involved, etc., to analyse (diagnose) these data, to take a decision according to the analysis and to execute an action to try to solve the cause of the problem. However it is very important to remark that self-healing actions shall make the system converge to a stable state. This is an important challenge that has to be taken into account and requires a detailed knowledge of the consequences derived from previous self-healing actions. ***System Administrators*:** Responsible for network monitoring and management. Monitoring services are automatically adapted to network changes. ***Vendors*:** Implement necessary functionality to core/edge routers. Network infrastructure has to support necessary functionality for supporting autonomic services. ***Application Developers*:** Build new services without addressing any challenges regarding the underlying network infrastructure. ***Manufacturers*:** Design personal devices able to connect to any autonomic network with minimum software pre-installed. ***End Users*:** Accessing services provided by other peers with minimum user intervention and any support from (centralized) infrastructure.

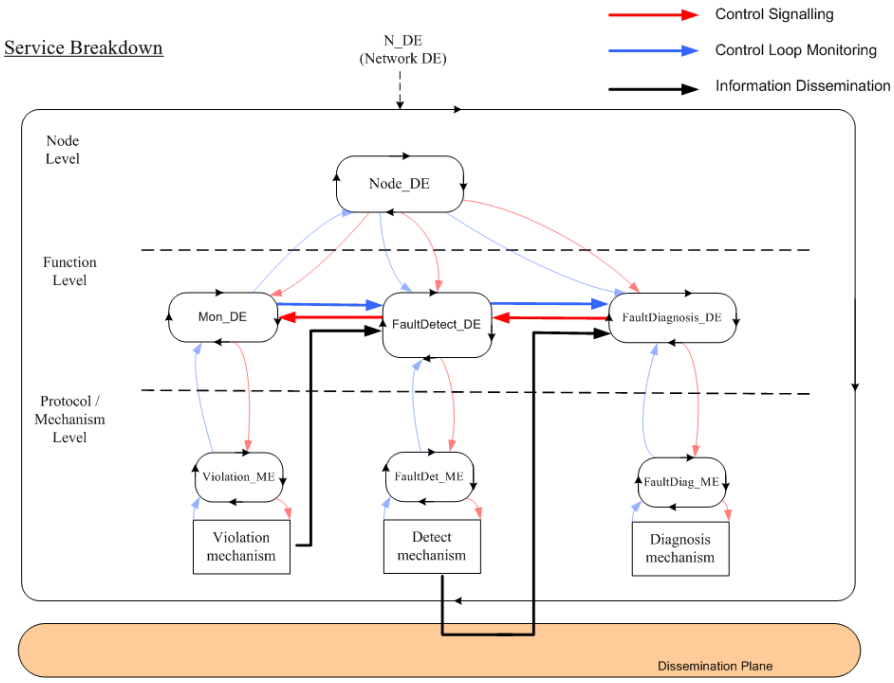

Figure 5: Service breakdown

5.9 Scenarios Overlay Virtual Network Service Quality Degradation

Table 18: Scenarios Overlay Virtual Network Service Quality Degradation

Title	Overlay Virtual Network Service Quality Degradation
Description/Story Use Case	As Alan travels, he wants to access content from his HAN, for example video content from his video database. He typically wants to see this content at a particular quality level. This quality level is set in the management policy in the HAN/SOHO Management Device and can be made known to each of the devices in the HAN. When Alan attempts to download information from his HAN to his laptop, the admission control (AC) mechanism (see "Problems" section below for further issues relating to AC) will either prompt Alan or try to enforce conditions predefined in the management policy set up on Alan's HAN. The quality of the end-to-end communication will be iteratively monitored on the source side (period to be configured) and QoS parameters including packet delay, packets dropped, jitter (and others) will be monitored. It is envisaged that an intelligent management application will be deployed in the HAN. The functionality of this application will be responsible for deciding what action to take if/when the communication parameters drop below predetermined thresholds. Note that initial admission control will use only bandwidth as a determining fact; however, iterative monitoring of the link will use available bandwidth along with other QoS connection parameters such as the ones given above. As part of its context aware nature, the autonomic application should sample these parameters more frequently when the QoS is close to one of its thresholds. As well as solving the problem for the viewer at that moment, the management application should try to solve the underlying problem and report any bigger issues to the user. The following cases can be diagnosed: • Congestion in the OVN user HAN, i.e. destination hotel network. In this case, the management application detects any errors within the hotel network caused by interference between incoming video traffic and other traffic sources (mainly Internet and intra-hotel traffic). • Congestion in the content source HAN i.e. Alan's HAN. In this case, the management application detects errors within Alan's network due to excessive outgoing traffic caused by the interference between video and other types of traffic. • The impact on the source HAN of multiple subscriptions to OVN services and the consequent increase in HAN traffic should be taken into account. At the content source HAN, there should be a mechanism to detect if poor QoS within the HAN is caused by the fact that the OVN service is being used. If that was the case, a proper action should be taken (for instance, stopping temporarily the OVN service). This is a very important issue because, it may impact the quality of experience related to the OVN service. Therefore, it may be convenient to split this case into a different scene on its own. • QoS degradation at the access network. This use case is meant to detect QoS deficiencies in the access network caused by excessive traffic or access network malfunctioning. • Lack of sufficient available end to end bandwidth. Since several ISP networks can be involved in delivering the OVN service, it might happen that, due to problems in any of these ISPs, the available end to end bandwidth drops below the required threshold. • Degraded video signal received from the video server. In this case the management application will detect that the video server is delivering a low quality video signal.
Network Environment(s)	Home Area Networks (HAN) Small Office Home Office (SOHO)

Title	Overlay Virtual Network Service Quality Degradation
Problems	Admission Control will primarily be used as a decision making component, which the main role is to admit or reject a new session trying to access content in the HAN. The Admission Control Managed Entity (AC_ME) (see definition of Managed Entity(ME)) will receive input from the QoS decision element (QoS_DE) (see definition of Decision Element (DE)), which exchanges information with the Application Decision Element (App_DE) in order to define the requirements for a particular session. A tailored AC mechanism decides whether or not a HAN device should accept a new session. Such decision shall be concerned basically on two issues: a) Short-term issue: Can the HAN gateway device and the host afford a new session and its respective requested QoS? Is there enough initial end-to-end (E2E) available bandwidth for transporting a new session? (figure 6) b) Long-term issue: Will the new session affect the current QoS levels already being held and committed by the HAN gateway? (figure 7) Information exchange will be kept simple between the AC_ME and its correlated components. Fundamentally, AC_ME needs to receive a traffic specification (TSPEC) for the requested session and will return a reply informing whether such session will be allowed to be initiated, an offer for an alternative QoS level (normally, with less strict QoS requirements), or a direct rejection. TSPECs may follow any standard format, such as TSPECs for Integrated Services or for IEEE 802.11e [i.14]. AC_ME may also follow an interactive negotiation strategy or different parameter description of traffic. In other words, appropriate TSPECs are required from new sessions and the AC_ME will admit only the traffic that satisfies the TSPECs, offer a different TSPEC or reject the connection. AC_ME will be then a mix of traffic descriptor-based and measurement-based AC. After a TSPEC is provided by the QoS_DE for each new session prior to its establishment, a fast E2E available bandwidth technique shall be launched in order to have a current view of the network path condition between the content provider host in the HAN and a user device that joined the OVN. Particularly, AC_ME will rely on accurate techniques for estimating the current E2E available bandwidth, such as Pathload, ABGet or IMR-Pathload. This information is then disseminated to the AC_ME where it can make AC decisions to allow the service to proceed as requested. Additional attention may be given to bandwidth fluctuation over multiple time scales (i.e. when the traffic profile shows long-range dependency) in order to avoid overestimation or underestimation of TSPECs, which could lead to QoS degradation, poor HAN resources utilization, or high rate of refused session admission.
Functions Impacted	The following autonomic functions are impacted: • *Self*-optimization – data and services are distributed uniformly among the participating nodes. The established overlay topology is maintained and updated after changes in the network.
Systems Involved	Operators ISP Source and Destination access networks Core/Edge Routers HAN devices – Home Gateway, End User Devices
Indicators / Evaluation criteria / Metrics	1) How is the autonomic application installed and updated on the HAN Management Device? 2) How are the control mechanisms installed and updated on the other HAN Devices such as the travelling laptop? 3) Will content providers be willing to provide available bandwidth information to end-user applications in their networks? What agreement needs to be set up to allow the user to get this information? 4) Availability and cost of probes inside the HAN. 5) Performance of QoS monitoring components deployed in HAN devices. 6) Privacy issues when accessing customers' traffic.
Players	Network Operator; Vendors/ Manufacturers; End Users
Beneficiaries and the benefits	***Operator's perspective*:** Being able to proactively diagnose and solve QoS problems in the HAN would be a very good way to increase customer satisfaction. This has to be balanced with the cost of deploying QoS monitoring components inside the HAN. This scene directly involves the operator. The admission control mechanism extends from the HAN/SOHO Management Device to the User device. The operator is required to carry the bandwidth determination criteria and the control packets (as well as the content). The control packets will allow the user device (in this case, the laptop) to inform the HAN/SOHO Management Device in an ongoing manner of the video quality being received.

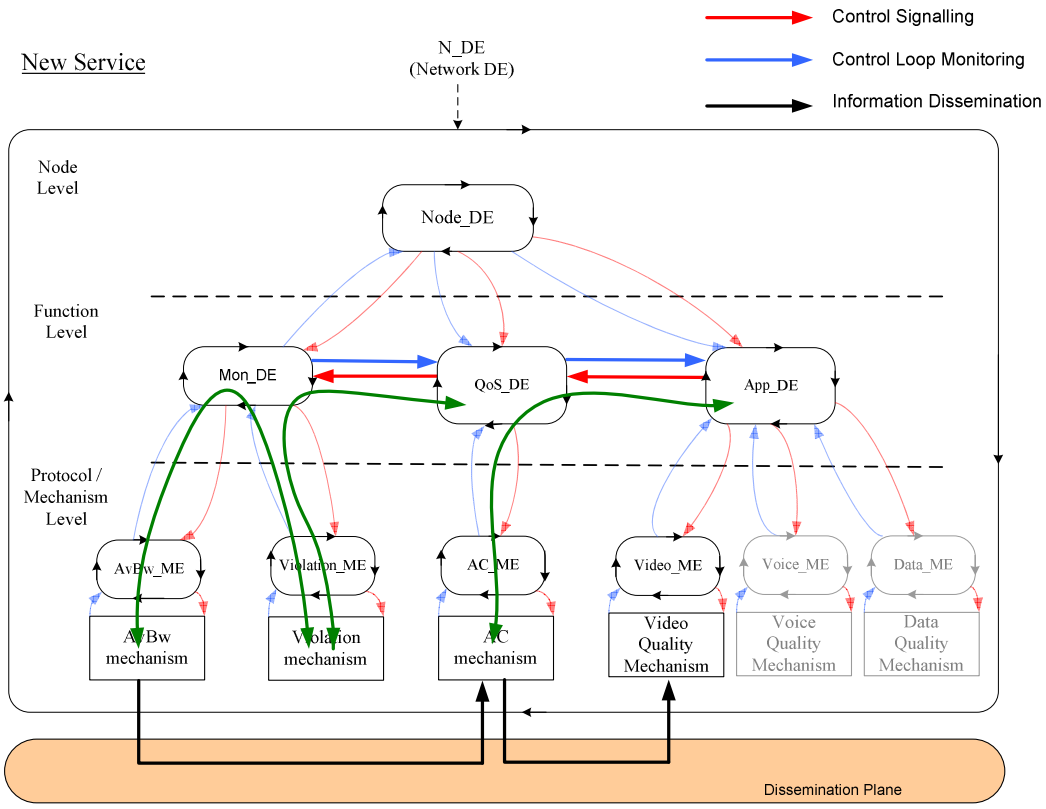

Figure 6: New services

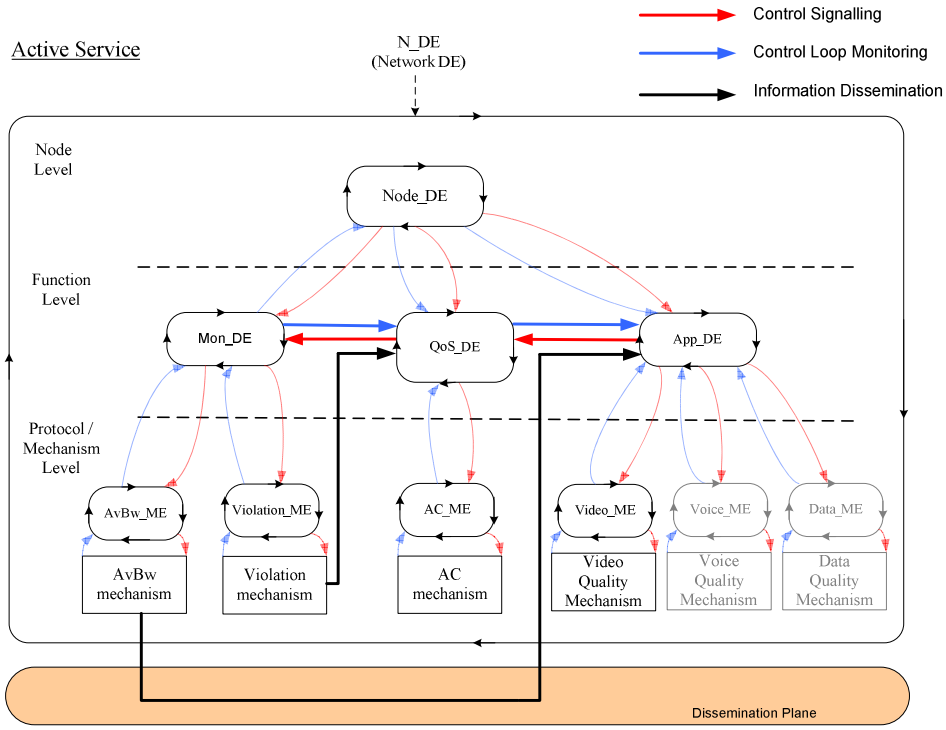

Figure 7: Active services

5.10 Monitoring in Carrier Grade Wireless Mesh Networks

Table 19: Monitoring in Carrier Grade Wireless Mesh Networks

Title	Monitoring in Carrier Grade Wireless Mesh Networks (CARMEN)
Description/Story Use Case	Mesh networking technology provides a cost effective and efficient alternative for realizing backhaul networks to provide mobile users with high quality services. Wireless mesh networks are dynamically self-organized and self-configured, which ultimately results in reduced deployment costs and lower network maintenance costs for the operator. CARMEN focus on mesh networks which provide carrier grade services with low operational maintenance, low cost and high flexibility in deployment. Furthermore, CARMEN focus on continuous monitoring features, which allow self-configuration and self-healing properties reducing the maintenance cost of the infrastructure. The monitoring system plays a critical role in supporting the self-* functionality. The main role of the monitoring system is to supply other modules with accurate and timely information regarding the status of the network in both a technology-dependent and technology-independent manner. Specifically this requires measurement, aggregation, correlation and statistical analysis of the raw data. The reports from the monitoring system are not only crucial for self-configuration and planning functions, but also important for dynamic resource management, such as routing updates or admission control decisions. Steps: 1) After a mesh node is activated, the node starts discovering its radio neighbourhood as seen by each of its multiple radio interfaces of different technologies. This is based on passive scanning by the monitoring function and facilitates the discovery of the mesh gateway node. 2) The monitoring function supplies the necessary information to create a view of the physical network topology. This view describes which radio interfaces can be used by two neighbouring mesh nodes to communicate with each other. 3) The monitoring function gathers information on the level of potential interference between radio links as well as interference resulting from external sources. 4) This information drives other mesh network functionalities, such as network planning, radio resource management, routing, mobility management, etc. 5) During the operation of the network, the monitoring function continuously measures network performance characteristics and reports any deviation so that corrective action can be taken. EXAMPLE: City coverage scenario – a wireless mesh network is deployed in selected areas of a city centre to provide users access to the operator's services. The mesh network consists of a small group of nodes which are connected into the operator's wired infrastructure and a larger number of wireless nodes. The self-configuration functionality allows easy network deployment and extendibility. Constant monitoring assures an accurate view of the physical network topology and aids in radio management, especially in dense urban environments.
Network Environment(s)	Wireless mesh network (heterogeneous, multi-hop, robust topology with dedicated mesh routers), support for carrier grade services
Problems	1) Determining network capacity (e.g. available radio channels) 2) Determining link quality (e.g. bandwidth, delay) 3) Detecting neighbouring nodes (passively) 4) Allowing prompt reaction to network events (e.g. link failure) 5) Utilizing heterogeneous network technologies
Functions Impacted	The following autonomic functionalities are provided: 1) *Self-configuration of the mesh nodes*. Each mesh node recognizes the physical network topology, identifies its neighbours, and utilizes heterogeneous network technologies. This is performed in particular during the initial bootstrapping phase. 2) *Self-organization of the network.* The whole network and all communication links between mesh nodes are established. 3) *Self-healing*. The network is robust to changes of topology and radio conditions.
Systems Involved	Core/edge wireless mesh routers

Title	Monitoring in Carrier Grade Wireless Mesh Networks (CARMEN)
Indicators / Evaluation criteria / Metrics	1) How much resource (in terms of memory, interfaces, computational power) does monitoring require? 2) How long should monitoring data be stored at a node? 3) How long does it take to notice link changes? 4) What is the accuracy of a link failure prediction? 5) How long does it take to detect neighbouring nodes?
Players	Network Operators: deploy wireless mesh networks Vendors/Manufacturers: provide equipment supporting carrier grade services in wireless mesh networks
Beneficiaries	Network Operators: can easily deploy new networks, extend existing networks, and assure QoS to meet users' expectations at a reduced cost End-users: gain access to triple-play services (with a required level of QoS) through a ubiquitous wireless network

5.11 Network self-management based on capabilities of network behaviours as described to the overlying OSS processes

Table 20: Network self-management based on capabilities of network behaviours as described to the overlying OSS processes

Title	Network self-management based on capabilities of network behaviours as described to the overlying OSS processes
Description/Story Use Case	Nowadays, the technologies often run far ahead of the ability to manage them. This may result in complex networked systems requiring manual configuration and dedicated management provided by very expensive experts. Such a model is obviously cost ineffective and it cannot scale. For this reason there is an urgent need for automation in terms of planning, configuring and assuring network behaviours. Next generation Operations Support Systems (OSS) need to be able to manage a diverse set of network devices offering different capabilities and exposing various behaviours. In particular some of the devices might be equipped with capabilities allowing for certain cooperative and non-cooperative behaviours. Currently developed next generation networks often assume the possibility of having devices able to route data in a cooperative manner to increase the QoS offered by the system. Such devices are preliminarily to be deployed by network operators as fixed, movable and mobile ones, while the mobile relay nodes may be also user devices on a longer perspective. It puts then certain requirements on the system to be able to discover the capabilities of distinct devices and use the acquired information for the purposes of exploiting these behaviours whenever beneficiary for the overall performance. This task involves other OSS level routines such as inventory management and service assurance.
Network Environment(s)	Wireless mobile networks
Problems	One of the aspects that seems to be missing in terms of the desirable behaviours is any consideration of what is the cost of ownership of a given behaviour in the context of planning, fulfilling/configuring and assuring this behaviour in the end to end system. It is very easy to create a network feature that is bespoke and therefore difficult to integrate and from an OSS point of view the need would be to understand how the capabilities of network behaviours can be described in a common standardized way that makes them easy to integrate and describe to the overlying OSS processes. The aforementioned cooperative behaviour can be highly beneficial from the system performance perspective, however, it comes at a certain cost. This cost may result from the fact that either: • additional network operator devices may need to be deployed so they can be automatically configured to expose cooperative behaviours when there is a need, • user devices may be needed to instantiate cooperation and in that case users may want to trade what they can offer for some other privileges or benefits. There is then a need for a logic that would be able to analyse applicability of such a behaviour for specific deployment and in given circumstances (longer term perspective) and consequently make use of them by imposing certain policies. It might turn out that in some cases cooperative behaviours can be translated into revenue, as well as they can add to service assurance. In different circumstances different cooperative behaviours may be exposed: • Base Station/Access Point can instantiate cooperation with Relay Node(s). • Relay Nodes can instantiate cooperation among themselves. Otherwise non-cooperative behaviour may be advantageous.
Functions Impacted	Service assurance Inventory management
Systems Involved	OSS
Indicators / Evaluation criteria / Metrics	Cost of ownership of a behaviour - how capabilities of network behaviours can be described in a common standardized way that makes them easy to integrate and describe to the overlying OSS processes.
Players	Software solutions providers Service providers
Beneficiaries	Network operators (in terms of service provision) End users (in terms of the QoS offered)

5.12 Wi-Fi Network Robustness: "Flexible Architecture for Virtualizable future wireless Internet Access"

Table 21: Wi-Fi Network Robustness: "Flexible Architecture for Virtualizable future wireless Internet Access"

Title	Wi-Fi Network Robustness: "Flexible Architecture for Virtualizable future wireless Internet Access"
Description/Story Use Case	Modern wireless networks are unable to rapidly adapt to evolving contexts and service needs, emerging applications and use cases, due to their rigid architectural design. In order to solve this problem, new flexible solutions are appearing, which promote the concept of wireless Media Access Control (MAC) processors (WMPs). Such solutions support a vision where selected parts of the physical MAC resource control functionalities are easy to program. This enables the implementation and deployment of new solutions tailored to the specific environments and services they are targeting. The flexibility provided by WMPs may lead to new methods of cheating as well as intra- and inter-node misconfiguration. Therefore, new misbehaviour and misconfiguration detection solutions are required which are in line with the promoted flexibility principle of WMPs. Therefore, a flexible architecture responsible for the detection and handling of WiFi misbehaviour as well as intra-node and inter-node misconfiguration is required. Such an architecture should implement advanced passive monitoring and a flexible WMP to achieve the stated goals. Passive monitoring additionally allows detecting the quality of wireless channels. The architecture should include the following components: information base (IB, a local data base containing a set of node capabilities), consistency manager (CM, module responsible for checking and correcting intra- and inter-node configurations), monitoring module (MM, based on passive scanning), and a set of services. Steps: EXAMPLE 1: Wireless channel change (self-healing) The degradation of the radio link quality of the current channel is detected based on the passive scanning performed by the MM. MM provides a ranking of network configurations, based on available channels and data rates. A wireless node switches to a channel with better quality and/or data rate. EXAMPLE 2: Detection of node misbehaviour (self-protection) Based on the passive scanning performed by the MM, node capabilities are discovered. Based on the detected node capabilities, MAC parameter values are calculated. If node misbehaviour is detected an appropriate penalty scheme is employed to force the misbehaving node to start cooperating again. Examples of penalties include disassociation, blacklisting, failing to generate acquittements or even jamming transmissions. EXAMPLE 3: Intra-node consistency check (self-configuration) If one of the services requests a system parameter change, the CM within a node analyses the request. A local set of capabilities is generated based on the information stored in the node IB. The CM verifies the internal consistency conditions and confronts it with an already configured value. If the settings are consistent the CM confirms the requested parameter change. If the settings are inconsistent the CM reports a conflict with an error code. EXAMPLE 4: Inter-node consistency check (self-organization) Network parameters are constantly measured and the capabilities of neighbouring nodes are discovered using the passive scanning performed by the MM. If misconfiguration between two nodes is detected by the CM, i.e. two nodes are determined to be using different configurations, the configuration of the misconfigured nodes is corrected by the CM.

Title	Wi-Fi Network Robustness: "Flexible Architecture for Virtualizable future wireless Internet Access"
Network Environment(s)	Wireless local area networks
Problems	Detecting intra-node configuration conflicts Detecting inter-node configuration conflicts Detecting misbehaving nodes Reacting to misbehaving nodes Detecting wireless link quality
Functions Impacted	The following autonomic functionalities are provided: Self-healing (responding to varying radio channel conditions) Self-protection (reacting to misbehaving nodes) Self-configuration (resolving intra-node configuration conflict) Self-organization (establishing inter-node network configuration)
Systems Involved	Wi-Fi access points and clients
Indicators / Evaluation criteria / Metrics	How long does it take to detect intra-node configuration conflicts? How long does it take to detect inter-node configuration conflicts? How long does it take to detect misbehaving nodes? How long does it take to detect wireless link quality? What is the accuracy of the detection mechanisms? Which misbehaviour reaction methods are appropriate? How much resource (in terms of memory, interfaces, computational power) does passive monitoring require?
Players	Network Operators: provide wireless network Vendors/Manufacturers: provide wireless equipment
Beneficiaries	Network Operators, Manufacturers and End-Users: can easily program the selected parts of the physical MAC resource control functionalities

5.13 Scenarios, requirements and references relationship

To sum up, table 22 lists the relationships between Scenarios and derived requirements. It also mentions the references (European Research projects, SDOs) if any.

Table 22: Use cases, Scenarios and references relationships

Scenarios	Requirement Identifier: RQ ID	Reference
Scenario 5.2 Autonomics in NGN	5, 9, 10, 24, 25, 26, 27, 28, 36, 37, 38, 39, 40, 44, 42, 43, 44, 45, 46, 47, 48, 49, 51, 52, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68	[i.11], [i.10], [i.12]
Scenario 5.3 Auto-configuration of Routers	21, 22, 23, 37, 43	[i.8]
Scenario 5.4 Self-Management of Coverage/Capacity in Wireless systems	2, 24, 27, 28, 38, 39, 40, 41, 53, 57, 58, 59, 62, 64, 66, 67	
Scenario 5.5 Cognitive event management	38, 57, 58, 59, 62, 63, 64, 65, 67	
Scenario 5.6 Coordination of Self		
Scenario 5.7 Autonomic network monitoring	1, 2, 3, 4, 6, 7, 8, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 50, 53, 54 21, 22, 23, 25, 26, 27, 28, 29, 30, 38, 39, 40, 68, 71, 72, 73	
Scenario 5.8 Overlay Virtual Network (Service Breakdown)		[i.8]
Scenario 5.9 Overlay Virtual Network (Service quality degradation)		[i.8]
Scenario 5.10 Monitoring in Carrier Grade Wireless Mesh networks	29, 30, 31	[i.9]
Scenario 5.11 Network Self-management by Overlying OSS processes		
Scenario 5.12 Wi-Fi Network Robustness	32, 33 ,34 ,35	[i.16]

Annex A (informative): Current NGN network as an example of a reference network architecture in which autonomics could be introduced

Next Generation Network (NGN) is a network architecture that almost all operators are deploying. Within NGN, the core network is based on IP and multiple access technologies and devices that can coexist alongside this IP core network. IP connectivity among users is a pre-requisite. IP Multimedia subsystem (IMS) is the first distributed control service architecture for fixed/wired and mobile access convergence network. It is deployed to facilitate service convergence.

NGN is the current network architecture for operators to fulfil the requirements that arise from new market realities:

- Open competition (especially in terms of new services deployment, to provide the best QoS, to reduce prices/costs/OPEX).
- Deregulation of markets (e.g. separation between network and service planes).
- Explosion of digital traffic.
- Convergence (fixed/mobile).
- Mobility (inside converged networks, between several networks (Web services)).

Next Generation Network (NGN) is defined by ITU-T as a layered network and services architecture using a packet-based transport network and a unified control layer that is able to provide telecommunication services with Quality of Service (QoS) over different broadband access networks [i.4]. NGN supports generalized mobility/nomadic functions allowing consistent and ubiquitous access to services.

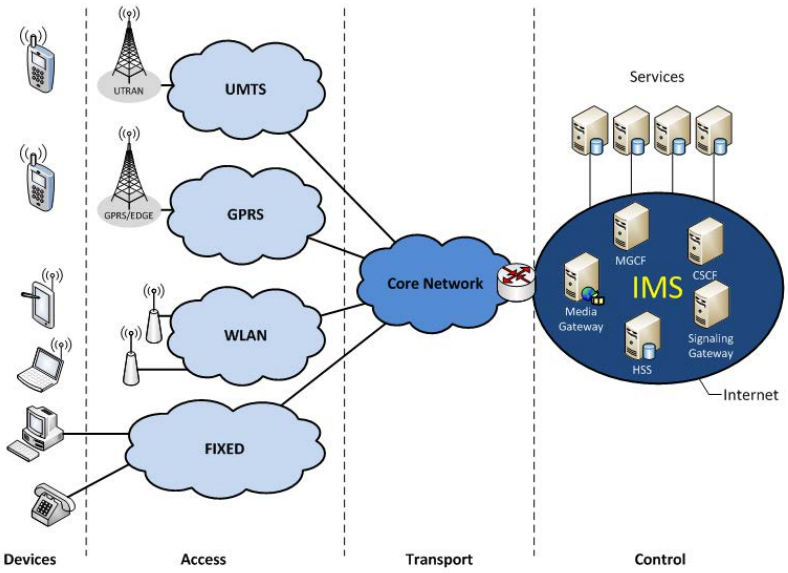

Figure A.1: NGN architecture applied to IP Multi Media Services

Network and service decoupling is one of the main NGN concepts. Such decoupling is reflected in the NGN architecture. As it can be viewed in figure A.1, there is a clear separation between service and transport layers. NGN covers different access networks through a common IP core network. For NGN, it is necessary to have IP connectivity among users.

Annex B (informative): Change History

Date	Version	Information about changes
October 2013	V1.1.1	GS transformation to TS

Annex C (informative): Bibliography

Heylighen F. (2009): "Complexity and Self-organization", in Encyclopaedia of Library and Information Sciences, eds. M. J. Bates & M. N. Maack (CRC Press).

V. Poladian et al: "Dynamic Configuration of Resource-Aware Services" Proc. 24th Int. Conf. Software Engineering, pp. 604-613, May 2004.

http://en.wikipedia.org/wiki/Autonomic-Networking.

J. O. Kephart, D. M. Chess: "The Vision of Autonomic Computing", January 2003 http://users.soe.ucsc.edu/~griss/agent-papers/ieee-autonomic.pdf.

ETSI TS 188 003 (V1.1.1): "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); OSS requirements; OSS definition of requirements and priorities for further network management specifications for NGNOSS definition of requirements and priorities for further network management specifications for NGN".

EC Funded Self-NET Project: "Self-Management of Cognitive Future InterNET Elements".

EC funded FP7 E3 Project: "End-to-End Efficiency" https://ict-e3.eu/.

EC funded FP7 SOCRATES Project: "Self-Optimization and self-ConfiguRATion in wireless network" http://www.fp7-socrates.org/.

EC funded FP7 4WARD Project http://www.4ward-project.eu/.

EC Funded FP7 ANA Project: "Autonomic Network Architecture" http://www.ana-project.org/.

ETSI TS 132 500 (V10.1.0): "Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Self-Organizing Networks (SON); Concepts and requirements (3GPP TS 32.500 version 10.1.0 Release 10)".

History

Document history		
V1.1.1	October 2014	Publication