Deliverable D4.1

Synthesis of Use Case Requirements

Release 1

version 02, updated as per year-1 review recommendation #3 for the period under review:

“Deliverable D4.1 should be updated to reflect the fact that UC5 was merged into UC6.”

Grant Agreement	257513	
Date of Annex I	26-07-2010	
Dissemination Level	Public	
Nature	Report	
Work package	WP4 – Deployment and Impacts	
Due delivery date	01 June 2011	
Actual delivery date	04 July 2011	
Updated on	21 August 2012	
Lead beneficiary	TIS	Antonio.Manzalini@telecomitalia.it

Authors	TIS – Antonio Manzalini (editor) , Roberto Minerva ALBLF – Leila Bennacer, Laurent Ciavaglia, Samir Ghamri-Doudane, Pierre Peloso, Benoit Ronot, Martin Vigoureux ALUD – Markus Gruber TCF – Mathieu Bouet, Gerard Nguengang NEC – Johannes Lessmann and Zarrar Yousaf FT – Christian Destré, Imen Grida Ben Yahia, Zwi Altman TID – Alfonso Castro and Beatriz Fuentes Fraunhofer – Mikhail Smirnov IBBT – Vânia Gonçalves, Simon Delaere INRIA – Olivier Festor, Remi Badonnel VTT – Teemu Rautio, Jukka Mäkelä UCL – Alex Galis, Stuart Clayman UniS – Stylianos Georgoulas UT, Ramin Sadre, Ricardo Schmidt and Anna Sperotto NKUA, Nancy Alonistioti, Eleni Patouni, George Katsikas, Panagiotis Spapis, Apostolis Kousaridas, Konstantinos Chatzikokolakis, Vagelis Kosmatos and Evangelos Rekkas UPRC – Panagiotis Demestichas, Kostas Tsagkaris, Nikos Koutsouris, George Athanasios, Aimilia Bantouna, Dimitris Karvounas, Panagiotis Vlacheas, Yiouli Kritikou, Vera Stavroulaki, Marios Logothetis, Evangelos Thomatos, Maria Akezidou, Andreas Georgakopoulos

Summary of changes in version 02

Pages 4, 8 and 55: A note has been added to explain the change from 7 to 6 use cases (i.e. the merging between use case 5 and use case 6).

Executive summary

Deliverable D4.1 provides the synthesis of the requirements collected via the use cases defined in the work package 4 (Deployment and Impacts) of the UniverSelf project. Said requirements are transferred both to work package 2 to define and design the Unified Management Framework (UMF) and to the work package 3 to direct the design of methods and algorithms for Network Empowerment solutions. Moreover, deliverable D4.1 results are transferred to other tasks of the work package 4 and used for the implementation and validation of integrated solutions, business impact analysis and trust development and evaluation.

In the UniverSelf project, a use case is a descriptor of a (set of) precise problem(s) to be solved, in a given technological context. The role of the use case is to formally identify, clarify, and organize both requirements and modelling of the system to be designed; the implementation and evaluation of the designed solution will then validate the resolution of the problem(s) addressed by the use case.

Use cases definition started from the three reference scenarios identified during the project proposal preparation, i.e. Scenario 1 - Operators' Service and Data Management, Scenario 2 - SON for Radio Access and Core Networks, and Scenario 3 - Future Internet Services Management and Network Resource Optimization (see Annex A). These three reference scenarios reflect the network operators needs of reducing the total cost of ownership, exploiting new revenue streams and improving the return on investment for network equipment and infrastructures; furthermore many problems such as fault diagnosis, misconfigurations, performance degradation, etc. are still open problems and, will become even more pressing with the developing trends and scale of future networks. Seven use cases have been identified, whose descriptions are reported in corresponding white papers. The first series of use case white papers cover the use case story line, problem statement, modelling, and innovation parts of the use case template. The white papers are available on the project web page at the following link: http://www.univerself-project.eu/white-papers.

The use cases are:

1. Self-diagnosis and self-healing for IMS VoIP and VPN services
2. Network Stability and Performance
3. Dynamic Virtualization and Migration of Contents and Servers
4. SON and SON Collaboration according to Operator Policies
5. Network Morphing
6. Operator-governed, End-to-end, Autonomic, joint Network and Service Management
7. Network and Services Governance

At the 1st release of Deliverable D41 in the project, it appeared reasonable that UC#5 might be merged with another use case such as UC#3 or UC#6. After some investigations, the decision was made (at PMT17 meeting on 7/07/2011), in consensus of all partners involved and of the PMT members, to actually merge the content of UC#5 with UC#6. The numbering of the use case has not been changed to preserve consistency across the current and following documents. As a direct result of this decision, the project is now studying 6 use cases as initially planned.

Main achievements reported in this deliverable include:

- The telecommunication industry perspective, based on the views of the project industrial partners, in terms of what are the technical and business problems that the ICT industry is willing to solve thanks to the development and adoption of UMF and Network Empowerment technologies developed in the context of UniverSelf;
- A detailed list, an analysis and a synthesis of the functional, non-functional and business requirements of the seven use cases;
- Some considerations on how this process of use case requirements expression and analysis have been (and are being continuously) exploited within the project activities (e.g. with particular reference to the work package 2 and work package 3) and towards relevant standardization bodies, are also given.

In summary, deliverable D4.1 contains all requirements known and defined in the use cases up to the date of release of the document. In an incremental process, new and complementary requirements will be reported in deliverable D4.2 (to be released by March 2012) to list all use case-related requirements of the project. In particular, the D4.2 document will represent a final report to provide further results on the definition of key use cases for the three identified scenarios and the related requirements (at the system, functional and business level).

Table of Content

Foreword

Deliverable D4.1 makes the synthesis of the requirements collected via the use cases defined in the work package 4 (Deployment and Impacts) of the UniverSelf project.

According to the project lifecycle, the requirements expressed in work package 4 are transferred to work package 2 to guide the design of the Unified Management Framework (UMF), to work package 3 to guide the design of the methods and algorithms of the Network Empowerment solutions, and to other tasks of work package 4 for the implementation and validation of the integrated solutions, the business impact analysis and the trust development and evaluation. This process ensures the necessary interactions and consistency between the work packages while maintaining enough flexibility to progress the work in a distributed way. The interactions are instantiated through synchronization points and materialized by a series of documents as illustrated in Figure 1, which focuses on the WP4-WP2 interactions.

The synthesis of the use cases requirements will be presented in two documents, namely Deliverable D4.1 of June 2011 and Deliverable D4.2 due on February 2012. Intermediate reports are also planned in the form of Milestones MS35 and MS39. Therefore, at this stage, the list of functional and not functional requirements (as reported in D4.1) might not be exhaustive as additional use cases can be defined in the course of the project. Deliverable D4.1 contains all requirements known and defined in the use cases up to the date of release of the document. In an incremental process, new and complementary requirements will be regrouped in Deliverable D4.2 to list all use cases requirements of the project. Additional requirements have been identified in the D2.1 by adopting a top-down approach (e.g. leveraging principles and results from previous autonomic architecture research).

The scope of Deliverables D4.1 and D4.2, which is in line with the Description of Work, is as follows:

D4.1 – Synthesis of use case requirements – release 1: this document will represent the first report on the derivation of technical requirements for use cases (outcome of task 4.1). Specifically, it will propose initial results concerning the definition of key use cases for the three identified scenarios and the related requirements (at the system, functional and business level).

D4.2 – Synthesis of use case requirements – release 2: This document will represent the final report on the derivation of technical requirements for relevant use cases (outcome of task 4.1). Specifically, it will provide further results on the definition of key use cases for the three identified scenarios and the related requirements (at the system, functional and business level).

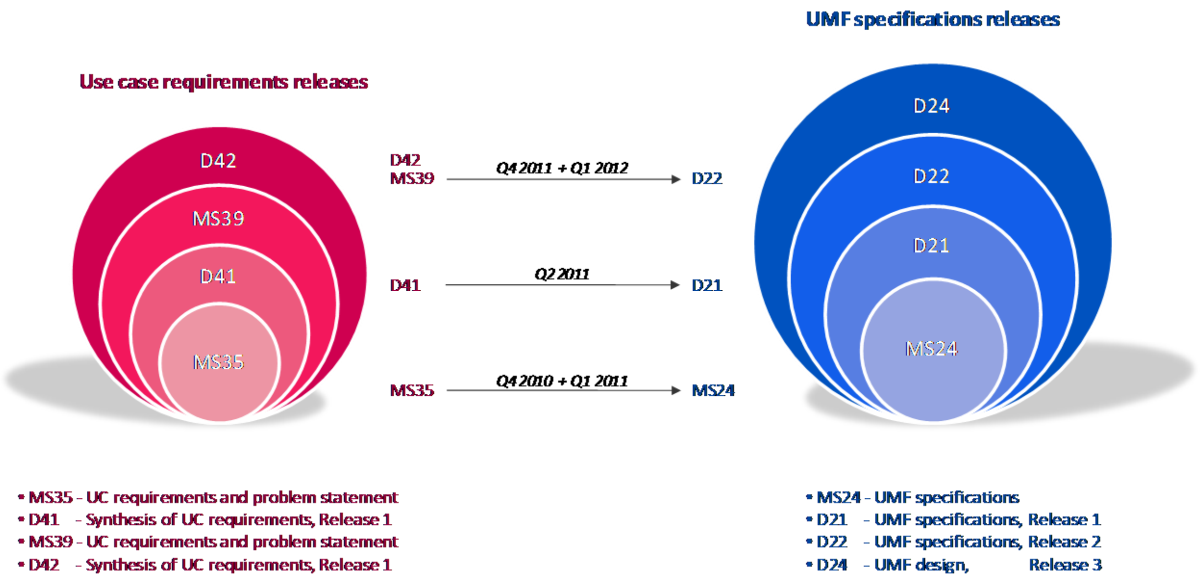

Figure 1 – Documentation roadmap - Synchronization points between use case requirement releases (WP4) and UMF specifications releases (WP2).

1 Introduction

This deliverable has the main goal of providing a synthesis of the use cases requirements. In particular, it represents the first document reporting a preliminary list and an analysis of functional, non-functional and business requirements derived from the development of the selected use cases.

In the context of Task 4.1 activities, the use cases definition started from the three reference scenarios identified during the project proposal preparation, i.e. Scenario 1 - Operators' Service and Data Management, Scenario 2 - SON for Radio Access and Core Networks, and Scenario 3 - Future Internet Services Management and Network Resource Optimization (see Annex A). These three reference scenarios reflect the network operators needs of reducing the total cost of ownership, exploiting new revenue streams and improving the return on investment for network equipment and infrastructures; furthermore many problems such as fault diagnosis, misconfigurations, performance degradation, etc. are still open problems and, will become even more pressing with the developing trends and scale of future networks. .

In the UniverSelf project, a use case is a descriptor of a (set of) precise problem(s) to be solved, in a given technological context. Seven use cases have been identified, whose descriptions are reported in corresponding white papers. The first series of use case white papers cover the use case story line, problem statement, modelling, and innovation parts of the use case template. The white papers are available on the project web page at the following link: http://www.univerself-project.eu/white-papers.

The use cases are:

1. Self-diagnosis and self-healing for IMS VoIP and VPN services
2. Network Stability and Performance
3. Dynamic Virtualization and Migration of Contents and Servers
4. SON and SON Collaboration according to Operator Policies
5. Network Morphing
6. Operator-governed, End-to-end, Autonomic, joint Network and Service Management
7. Network and Services Governance

At the 1st release of Deliverable D41 in the project, it appeared reasonable that UC#5 might be merged with another use case such as UC#3 or UC#6. After some investigations, the decision was made (at PMT17 meeting on 7/07/2011), in consensus of all partners involved and of the PMT members, to actually merge the content of UC#5 with UC#6. The numbering of the use case has not been changed to preserve consistency across the current and following documents. As a direct result of this decision, the project is now studying 6 use cases as initially planned.

A systemic analysis of above use cases has led to the following list of problems (as reported in Milestone 35). This list of problems has been used (see section 7.2.2) to underpin the interactions with work package 3, by making a correspondence "problem-task force in charge of looking for its solution". The list includes problems which are shared, at least from certain perspectives, by different use cases. This will allow each task force to provide solutions to more than one use case. Table 1 summarizes the use case problems.

Table 1 – List of use case problems

Use Case	Problems
UC1 - Self-diagnosis and self-healing for IMS VoIP and VPN Services	Problem 1: To develop algorithms and models to support reusable end to end cross-layer and local self-diagnosis related to networks and services. They should be able to provide macro/micro granularity for the end to end view and for local view or subscriber's view. Self-modelling will be investigated to create models related to managed objects topology (and interaction) and related behaviours, associated with correlation algorithms. Defined models and methodology should be compatible with other management functions (e.g. configuration).
	Problem 2: Enabling end to end and local self-Proactive and reactive diagnosis, including the detection, estimation of possible anomalies/issues/problems before occurring (proactive), known and occurring anomalies (reactive) or unknown anomalies. It also includes the analysis and qualification of incidents and related causes. Knowledge must be built from service and network data, alarms and events
	Problem 3: Based on diagnosis and defined mitigation & reparation plans, self-healing is enabled by applying the correct mitigation or reparation plan based on business goals
	Problem 4: Self-Diagnosis/healing functions should be triggered by network/service events but also by subscriber events (in the case of a subscriber signalling). Validation by human operators of diagnosis should be possible, reporting of mitigating/reparation actions should be done. Link with configuration processes is tight.
UC2 - Network Stability and Performance	Problem 1: To develop (leveraging prior-art) continuous and/or discrete models and related open source tool-boxes for simulations and emulations of stability and performance of networks with (large) number of nodes embedding self-configuration mechanisms/control-loops. Modelling includes network segments, nodes, control-loops rules and mechanisms (e.g. monitoring/actuation), etc. and their interactions in wide areas.
	Problem 2: To make simulations and emulations about stability and performance of networks in presence of various potential roots causes of instability (as identified in this and other UCs, if requested)
	Problem 3: To define the necessary and sufficient level of “cross-layer knowledge of the network” to be monitored and controlled (e.g. order and control parameters) to predict behaviour and assure network stability and performance
	Problem 4: To define the most effective and low-cost network decision logic distribution to assure network stability and performance.
UC3 - Dynamic Virtualization and Migration of Contents and Servers	Problem 1: To develop strategies that would reduce the load (traffic, processing, signalling etc.) on the core network segments and data centres for efficient delivery of data/service/application to the mobile user. This would be achieved by decentralizing and migrating frequently used/critical resources/functions/services from the core/data centres towards the access and backhaul network nearer to the user. This issue will be studied and analyzed with respect to the best practice solutions of network virtualization techniques for enabling dynamic migration of functions and resources.

	Problem 2: Specifying the resources and functions used (or required) by a mobile user (with varied mobility patterns) for accessing commonly used network services and applications (real time and non-real-time) in the context of 3GPP network architectures. Specifying the KPI for each of these services and applications and defining network/configuration/performance parameters for the commonly used services. Identifying the functional and operational enhancements of existing segments at the access/backhaul for supporting and hosting the migrated resources/functions/services).
	Problem 3: Develop algorithms that would leverage the virtualization techniques and cloud concepts for seamless migration of resources/services/functions context. Develop novel techniques and algorithms for enabling the seamless mobility of resources/services/functions virtual clouds in sync with the user mobility.
	Problem 4: Develop simulation models to understand the implication of decentralizing the resources/functions/services from the core and migrating them towards the access and backhaul segments and their impact on the network architecture and the corresponding network entities.
UC4 - SON and SON Collaboration according to Operator Policies	Problem 1: Design of distinct SON functionalities in network nodes to efficiently self-configure and self-optimize network resources. The SON functionalities at a given node (e.g. base station) should allow self-adapting to varying operation conditions, in the presence of other self-organizing neighbouring nodes, to assure stability and scalability.
	Problem 2: Design of different SON functionalities operating simultaneously to achieve one or several performance objectives. The solutions should guarantee coordinated operation of the SON functionalities, while avoiding or solving conflicts between conflicting objectives.
	Problem 3: Govern radio access networks by means of high level policies triggering coordinated SON functionalities. Definition of objectives and rules in the different network levels from the OAM till the SON algorithms embedded in the radio access nodes. Monitor the full SON processes to provide assurance.
UC5 - Network Morphing	Problem 1: To adapt traffic routing configuration of the network consequently to monitored traffic evolutions in order to ensure a low cost of the traffic routing configuration
	Problem 2: To enrich traffic variations with self-built knowledge of probabilistic traffic trends -> Pro-activity in routing adaptation to traffic. Traffic can be either monitorable IP traffic or sets of services demands
UC6 - Operator-governed, End-to-end Autonomic joint, Network and Service Management	Problem 1: To enable operators to describe their goals and objectives in high-level terms (H2N interface). To derive policies according to the higher level goals, to provide constraints and priorities. The assess the derived policies against existing goals/policies so as to identify and resolve conflicts (in fact, conflicts can arise if the defined goal/objective/policy are antagonist with respect to previous goals or the impact of these goals on already deployed services)
	Problem 2: Analyzing the business request, to develop the inputs/requirements derived from the business entry and to correlate them together with pertinent knowledge stemming from user and service raw data so as to derive technology specific (network specific) requirements.

	Problem 3: Determination of candidate solutions, to determine (reason with) the candidate solutions (networks) that can satisfy the derived network requirements. The candidate technologies and networks which can contribute to this satisfaction need to be discovered also taking into account existing knowledge that was extracted from raw network data to knowledge.
	Problem 4: To invoke the selected RANs and request for an offer in terms of the quality which the RAN can provide. Then, RAN investigates way to accommodate the request (anticipated load). In OFDMA-based (LTE) case this may result in problems related to radio resource allocation, Admission/Congestion control and scheduling, relay selection in case of multi-hop networks, link positioning, compensation by means of SON mechanisms etc.
	Problem 5: Invocation of backhaul/core segment, the backhaul/core segment is triggered and the problem aims at finding the best configuration and accordingly offer of quality, so as to support the solution (offer) provided previously by RAN. The backhaul/core investigates way to accommodate the request. At the backhaul side, this may involve LSP configuration in IP/MPLS case. At the core side, it also involves GW (e.g., SGW, PDN-GW) (re)selection/configuration, GW migration/dimensioning.
	Problem 6: The problem here is to resolve possible incompatibilities between the offered QoS from RANs and backhaul/core segments, respectively. For that reason, some sort of negotiation and cooperation between segments is needed that will be used to fine-tune the resulting offers from the underlying segments, in order to achieve coherence.
UC7 - Network and Services Governance	Problem 1: To enable operators to describe their goals and objectives, through high-level means and govern their network. Derivation of network policies from the business goals through the use of semantic techniques.
	Problem 2: Evaluation of the network governance tool, in terms of examining whether the generated policy rules and the applied configuration actions meet the initial business requirements. This evaluation will be realized through a feedback loop procedure that will realize the following actions: a) evaluation of the applied configuration actions in the infrastructure part and generated policy rules and b) evaluation of the business requirements through examining how well the specific goal is met.
	Problem 3: Implementation of algorithms so that the network elements in FTTH environments can self-discover their context, through the use of network protocols.
	Problem 4: Implementation of self-monitoring algorithms in network elements in FTTH environments.
	Problem 5: Probabilistic self-Diagnosis functions should be implemented in the network elements, based on their own state and their operational context.
	Problem 6: Decision making processed based on semantic models and inference engines must be supported for self-healing purposes.

The rest of this Deliverable is structured in seven sections:

- Section 2 provides the telecommunication industry perspective, based on the views of the project industrial partners, in terms of what are the technical and business problems that the ICT industry is willing to solve thanks to the development and adoption of UMF and Network Empowerment technologies developed in the context of UniverSelf;
- Section 3 describes concisely the approach and the methodology adopted in the derivation of functional, non-functional and business requirements of the use cases;
- Sections 4, 5, and 6 report respectively the list of business, functional and non-functional requirements identified for the seven use cases.
- Section 7 develops the design information gained from the definition of requirements: specifically this section provide a first synthesis coming from the use case requirements analysis; it also provides some guidelines on how this process of use case requirements derivation and analysis is being exploited within the project activities and towards relevant standardization bodies. For example, a comparison with ETSI AFI requirements definition is proposed as an action for the project.
- A detailed list, an analysis and a synthesis of the functional, non-functional and business requirements of the seven use cases;
- Some considerations on how this process of use case requirements expression and analysis have been (and are being continuously) exploited within the project activities (e.g. with particular reference to the work package 2 and work package 3) and towards relevant standardization bodies, are also given.
- Section 8 concludes the report, by providing some remarks on the lessons learnt and describing the next steps of this activity within the project.
- Abbreviations and definitions are provided at the end of the document
- Annex A contains the description of the three reference scenarios developed during the preparation phase of the project, as per the Description of Work document.

2 Stakes for the telecommunication industry

2.1 Network operators and service providers viewpoint

Network operators are in a strong need of reducing the cost of ownership and improving the return on investment for network equipment and infrastructures. Many problems such as the ones related to inefficiencies in faults management, miss-configurations, performance degradations, etc. are still unsolved, and they will take on additional dimensions in the future. Scalability, for example, is one of the biggest problems that future management systems have to face: this will progressively exacerbate in future networks, which are expected to be more and more cost-aware, service-aware, environment-aware, management-aware, content/data-aware ubiquitous, dynamic and heterogeneous. It will impact at the level of (real and virtual) nodes (e.g. cross-connects, routers, and switches), devices (e.g. users' devices, devices for Machine-to-Machine), and the related interfaces and links.

Network operators' needs could be split into short-medium (e.g. 3-5 years) and long term (e.g. 5-10 years) perspectives.

In the short-medium term, network operators are looking for increasingly effective management capabilities, overcoming current complications: one of these is moving away from error-prone, manually intensive operations to autonomic end-to-end operations. As such, there is arguably the need of introducing semantics, end-to-end service view (+cross-techno/ FMC), shared knowledge, governance, intelligence embodiment. These are enablers to solve the OPEX challenge:

- Network elements management ecosystems differ depending on the technologies (e.g. Fixed/Mobile), on vendors (proprietary interfaces/data models), IT editors (proprietary solutions). The Operations Support System (OSS) is trying to glue all these differences together to enable the overall management functions (fulfilment, assurance, and billing), inducing OPEX and Information System (IS) ossification and complexity.
- Complexity has a strong impact in the time to market for new services and applications, including cloud based services, internet of things services, ICT services and applications of any complexity. The delivering of a new service implies not only the deployment of the appropriate infrastructure (if needed), the work on research and development of the service itself, but also the modifications in the OSS and Business Support System (BSS) for the management of the new services. The simplification and automation of this process will help network operators not only to reduce the Capital Expenditures (CAPEX), but also to provide a larger service portfolio, offering the possibility to increase the incomes.

  Part of the complexity described above comes from the different languages used in the service management operation. On one hand, at the business layer, an implicit or explicit agreement between a client and a service provider specifies service level objectives, both as expressions of client requirements and as provider assurances. These objectives are expressed in a high-level, service-, or application-specific manner rather than requiring clients to detail the necessary resources. On the other hand, the network management requires low-level, resource-specific performance parameters that can easily be interpreted and provisioned. The translation from the former to the latter is realized by specialized personnel, using semi-automated procedures. As a consequence, a framework that addresses the gap between high-level specifications of client performance objectives and existing resource management infrastructures of network operators is traditionally required.
- Existing management elements are dedicated to one technology or to one vendor. They are hardly reusable and rely on human expertise from their deployment/development (processes, configuration, integration, scripts) (humans who are using the tools to take decisions and drive the management); There is a lack of machine readable network/service models, correlation, automation, etc. Extra time and effort are induced by new network elements or services deployment.
- End-to-End management needs to consider networks and services in a "coordinated" way (e.g. to consolidate on-demand service provisioning or to address end user QoS related issues and requests). The end-to-end management needs to consider services running in multiple domains and/or multiple vendor environments managed by several organizational entities. Having more than one business

organization involved requires (a) that agreements between parties include clauses to exchange runtime service information, (b) consideration that such agreements can only be established between trusted parties, that is, only the monitoring information coming from a trusted party can be used for the calculation of the runtime end-to-end QoS that is being offered to a customer, (c) therefore, consideration of automatic procedures for trust management.

- This will also imply assuring the stability of future networks and services. As a matter of fact cascading and nesting of self-* mechanisms can lead to the emergence of non-linear network behaviours. This is one of the most challenging unsolved problems in mathematical systems and control theory, which is "decentralized control with communication between controllers" [1].
- In current networks, implemented control and management functions are governed by entities which have to be configured through several low-level configuration commands (mostly hand-made); furthermore there are several dependencies among the states to be set by the configuration logic (most of which are not kept aligned automatically). Overcoming these complications should allow reducing OPEX whilst assuring, at the same time, high quality of services.
- The current lack of proper monitoring procedures results in operators over-provisioning the network capacity and devices, due to the incomplete knowledge on the real traffic carried. Probes are used to monitor traffic but they do not provide a fine-grained information related to the flows and usage by subscribers (unless there is a very large number of probes).The enhancement of the network monitoring, especially if it is accompanied by dynamic reallocation procedures, will allow the operators to improve the management of their resources (routers, fibres installed) and to plan and deliver new services facing revenue evolution.
- A general problem with telecommunications systems is that it is difficult to provide service content to a multitude of targeted users of different telecommunication operators in a manner that is well suited to individual terminal and access capabilities. Offering services adapted to the context and needs of each customer will increase the quality of experience. Self-adaption is then needed based on related evolving knowledge and on-demand provisioning.

In the long term, network management and control should be ready to face the challenges of future networks, which will be more and more cost-aware, service-aware, environment-aware, management-aware, content/data-aware, highly dynamic, pervasive, comprising large numbers of interconnected real and virtual resources (e.g., routers, switches, cross-connects, servers), users' devices (e.g., smart phones) and machines (e.g. sensors, smart things and actuators). If current management and control approaches do not properly evolve to face this level of complexity and scalability there will be a risk of unmanageability of future networks.

Specifically, in this evolution stage it is likely to see a deeper introduction of Network Empowerments features (i.e., less management, more control). From this point of view more profound changes are expected and clear evolution and migration strategies should be identified. **Error! Reference source not found.**[1]

2.2 Solution providers viewpoint

Solutions and equipment providers are privileged partners to network operators and service providers in their quest to combine, in the most efficient way, rich communication service offerings with scalable and flexible infrastructures and assets. Successful projects and partnerships rely in the capability to provide the right synergies through complete fulfilment of needs and requirements, minimization of the [cost * complexity]/ [performance * functionality] ratio, and continuous innovation.

In our field of research (*network control and management*), one of the biggest challenges is mastering complexity. Complexity arises from several sources: number and sophistication of communication services and applications, heterogeneity of equipment, protocols and technologies, backward compatibility with legacy and deployed systems, multiplicity of standard and proprietary solutions, explosion of the number and reach of connected devices. For network operators and service providers, this surrounding (and growing) complexity of communication networks materializes day after day into a pressing challenge to reduce or at least constrain the Total Cost of Ownership (TCO), and especially the Operational Expenditures (OPEX).

From the point of view of an individual solution provider, the goal is to differentiate from the competition thanks to innovation, technology leadership, and a sound and attractive portfolio. Today, fixed/mobile and all-IP convergence is blurring the boundaries between traditional networking technologies and between network segments, pushing for rationalization and simplification. Solution providers have to adapt not only the networking platforms but also their control and management architectures to integrate for flat, end-to-end, and modular requirements. Objectives are thus to design the functions that will enable these new self-managing networks and embed these functions directly within the systems and elements that comprise the network infrastructure and support service delivery. This is all the more difficult, as operator networks are typically multi-vendor networks, which means that non-standardized self-management approaches that involve multiple devices are in many cases not supported by all devices uniformly.

Beyond pure technology, adoption by the industry will be driven by the availability and demonstration of standard, interoperable solutions. To reach this objective and generate confidence in the viability and use of autonomic technologies in telecommunication networks, stakeholders need defining a proper "certification" framework and parameters for autonomic networking products. This requires action at a more global scale and coordination among solution providers, network operators, service providers and ultimately end-users.

The "function" or "business" of solution providers is also evolving for several years from equipment manufacturer to end-to-end solution integrator and outsourcing partner for networks operation and management. The emerging cloud networking business is also developing new types of multiple-partner associations (IT infrastructure owners/operators, Network infrastructure owners/operators, and Service providers) to deliver complete solutions. In these new contexts and environments, the benefits of standardized frameworks and unified processes, with flexible, distributed, automatic and autonomic control and management appear as arguably needed enablers. Obviously, the ability of product and service differentiation despite standardized management processes is again the driver in this evolving market.

For instance, in network operation outsourcing, a solution provider will certainly address different clients (i.e. network operators) with different types of network and technologies. In that case, capitalizing on homogeneous and automated processes, common tools and standardized operations (i.e. the *factory-like approach*) reduces time to model/deploy/troubleshoot services, and increases reliability and availability of the services. Also, equipment vendors are often responsible for the initial deployment of the infrastructure and the maintenance activities.

The introduction of autonomic control and management of networking technologies is therefore of prime interest to solution providers for their own teams and business. Numerous challenges lie ahead but delivering efficient, converged and trustworthy solutions, together with the appropriate standards, are essential to reach true operational benefits and wide deployments.

2.3 Business opportunities and bottlenecks

Taking into account network operators and solution providers needs introduced in previous sections, this section highlights the business rationale of the UMF, according to its current definition. We focus on identifying the main opportunities and relevancy of introducing a toolbox such as the UMF in the market, as well as on understanding any bottlenecks that may impact UMF's business adoption. The following opportunities and bottlenecks will be analysed according to: 1) impact on the internal business processes of an organization; 2) impact on the telecommunications value chain. The work in Task 4.3 will further evaluate these business issues, taking a look at the precise use cases that intend to realize UMF requirements as well as to the strategic positioning of the value chain roles vis-à-vis a specific set of business scenarios that incorporate the use cases.

2.3.1 Business Opportunities

Autonomic networks deliver the promise of dealing with the increased complexity of current and future networks and achieving the desired levels of scalability, efficiency and dynamicity to meet current and future operational demands. At the same time, network and service management will need to evolve to cope with this increased complexity while providing a simplified vision of a network that encompasses multiple and heterogeneous network domains and technologies.

Thus there is clear business rationale behind the provision of a set of tools that integrate the vision of a unified service management such as the vision delivered by the UMF in order to facilitate network operators to meet future operational, service and business challenges.

Consequently, the UMF is expected to have a number of possible effects on the internal organization of adopters, i.e. mainly on network operators. Firstly, the UMF is expected to have a major impact in operational and capital expenditures of network operators. Network operation and maintenance (OAM) tasks are estimated to constitute between 20 and 30 percent of operators operational cost structure [2]. The reduction and simplification of OAM tasks provided by UMF self-x functionalities play an essential role in alleviating human intervention and decreasing complexity of future networks. The UMF would also allow for the simplification of processes and reduction of the life cycle of network functions, which would potentially also impact operational expenditures. Reductions in capital expenditures are also expected through capacity gains and optimal resources allocation allowing for a deferral of upgrades of the infrastructure and reduction of expenditure related to the acquisition of network equipment.

Secondly, the UMF will also influence network operators' legacy processes and strategies. The service-oriented ecosystem enabled by the UMF will impact processes, workflows and tools of network operators facilitating the automation of processes and end-to-end flows, reducing the time-to-market of new services and improving the resolution of problems. This service-oriented ecosystem will allow network operators to move their visions and strategies towards a service management focused on customer satisfaction. With this in view, network operators will thus have the opportunity to further enhance the quantity and quality of services across multiple heterogeneous domains meeting customers' expectations and improving customer experience. The governance layer of the UMF will be the enabler of a straightforward translation of high-level business and service requirements into low-level device-specific and network-specific configuration policies.

More business opportunities can be identified at the level of the telecommunications value chain, especially in the interactions between network operators and Network Management Systems solution providers and/or Equipment providers and between network operators and service providers. On the one hand, the UMF's technology agnostic and openness characteristics will facilitate the relationship between network operators and Network Management Systems solution providers and Equipment providers by simplifying the deployment of the UMF on network operators' infrastructures and provide integration and interoperability between domains (e.g. between core and access domains within an Operator's network), multi-vendor and legacy equipment and systems. All in all, it will also strengthen the intended value of autonomic and intelligent networks.

On the other hand, by delivering an end-to-end view of process flows and services, the UMF will enable network operators to strengthen the relationship with service providers through the assurance of service level agreements, quality of service and support services.

2.3.2 Business Bottlenecks

The introduction of the UMF might suffer from risks and bottlenecks, both at the organizational level as well as in the business value chain.

Although the added value opportunities delivered by the UMF and autonomic networks seem to be straightforward, network operators might be cautious to make the first move towards internal adoption and prefer a “wait and see” position until UMF adoption gathers sufficient momentum.

Beyond the questions of reliability, stability and full control, other business bottlenecks concern the cost of the features and the further costs of the related induced changes. Risks related to (backward) compatibility and reliability issues, upfront investments and uncertainty about benefits might become important bottlenecks for UMF adoption. Moreover, the impact of the UMF on human operator interactions might constitute a level of complexity and need for adaptability that the network operator is not willing to take up right away.

Other business bottlenecks might originate in the process of reaching an agreement between vendors and operators about openness of solutions and standardization of interfaces and models. Although there is an argument for a standardized and open management framework, this will require Network Management systems vendors and equipment vendors to make additional strategic choices, namely to choose the best strategy to compete in the market between peers and to ensure and increase trust in autonomics and the UMF bringing additional bottlenecks.

3 Requirements development

This section describes concisely the approach and the methodology adopted in the derivation of functional, non-functional and business requirements of the use cases.

The approach adopted in the derivation of the requirements started from the analysis of network operators needs and requests which are captured in the three reference scenarios (identified during the proposal preparation, see Annex A). The approach aims at defining the functions or features satisfying the network operators' needs and requests. A complete derivation of requirements requires a detailed description of the use cases with the related business implications.

It is important to understand the clear distinction between needs/requests and functions/features. Needs/requests are part of the *problem domain*, and functions/features are part of the *solution domain*. It is critically important to fully understand the problem domain before deciding on a solution; by separating needs/request from functions/features, a common set of features, which can meet multiple needs, can be identified.

3.1 Definitions of requirements

A requirement can be defined as a statement that identifies a capability or function that is needed by a system in order to satisfy its customer's needs. Actually before effectively discovering and developing requirements, well-defined and well-stated problems should be identified. The problems must be stated in a clear, unambiguous manner: they should explain the customer's needs (in case of UniverSelf, the network operators' needs).

Usually, it is good practice to state the problem in terms of the capabilities that the system must have or the top-level functions that the system must perform. However, it might be better to state the problem in terms of the deficiency that must be ameliorated, as this can create more alternative designs.

In the context of UniverSelf, a functional requirement is meant to describe a function or a feature of a system, or its components, capable of solving a certain problem or replying to a certain need/request. It presents a *complete* description of how a specific system will function, capturing every aspect of how it should work before it is built, including information handling, computation handling, storage handling and connectivity handling.

Non-functional requirements are meant as attributes that a specific system must have. Examples of categories of non-functional requirements are [3]:

- Usability: it describes the ease with which a system performing certain functions or features can be adopted and used.
- Reliability: it describes the degree to which a system must work. Specifications for reliability typically refer to stability, availability, accuracy, and maximum acceptable bugs.
- Performance: it describes the degree of performances of the system (according to certain predefined metrics, e.g. convergence time).
- Supportability: it refers to a system's ability to be easily modified or maintained to accommodate usage in typical situations and change scenarios. For instance, how easy should it be to add new blocks and/or subsystems to the support framework.
- Security: it refers to the ability to prevent and/or forbid access to a system by unauthorized parties.
- Safety: It refers to conditions of being protected against different types and the consequences of failure, error harm or any other event, which could be considered non-desirable.
- Resilience: it refers to the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation
- Compliance: it refers to the conformance to a rule, such as a specification, policy, standard or regulatory.
- Extensibility: it refers to the ability to extend a system and the level of effort and complexity required to realize an extension. Extensions can be through the addition of new functionality, new

characteristics or through modification of existing functionality/characteristics, while minimizing impact to existing system functions.

- Interoperability: it refers to the ability of diverse systems and subsystems to work together (inter-operate).
- Operability: it refers to the ability to keep a system in a safe and reliable functioning condition, according to pre-defined operational requirements.
- Privacy: it refers the ability of system or actor to seclude itself or information about itself and thereby reveal itself selectively.
- Scalability: it refers to the ability of a system to handle growing amounts of work or usage in a graceful manner and its ability to be enlarged to accommodate that growth.

3.2 Characteristics of requirements

IEEE says that "requirements must be unambiguous, complete, correct, traceable, modifiable, understandable, verifiable, and ranked for importance and stability" [4]. In general, there is a rich literature proposing the characteristics of good requirements. However, the following characteristics are widely acknowledged:

- Consistent and atomic: a requirement addresses only one function or feature. The requirement is *atomic*, i.e., it does not contain conjunctions.
- Complete: a requirement is fully defined in one place with no missing information.
- Dependable: a requirement does not contradict any other requirements and is fully consistent with all relevant references.
- Current: a requirement has not been made obsolete.
- Feasible: a requirement can be implemented and supported by the enabling technology
- Mandatory or trade-off: mandatory requirements specify the necessary and sufficient capabilities that a system must have in order to be acceptable. It uses the words *shall or must*. Mandatory requirements are passed or failed with no in between (do not use scoring functions); and should not be included in trade-off studies. Trade-off requirements state conditions that would make the customer happier and are expressed with the words *should* or *may* (often a significant reward or incentive is attached to how well a performance or trade-off requirement is satisfied). Trade-off requirements should be described by scoring (utility) functions or measures of effectiveness [5], they should be evaluated with multi-criterion decision-making techniques, because none of the feasible alternatives is likely to optimize all the criteria; and there will be trade-offs among these requirements [4].
- Verifiable: the implementation of a design goal/objective can be determined through one of five possible methods: inspection, demonstration, test, trial or analysis.

The formulation of functional and non-functional requirements has been carried out by following the above-mentioned characteristics.

3.3 Requirements expression process

There is a rich literature describing possible approaches in the requirements process derivation. An example of requirements expression process [6] is shown in Figure 2. It shows a set of tasks that should be carried out for the requirements derivation. This general approach has been followed in the project. Based on this approach, use cases requirements have been derived by identifying the stakeholders, understanding Industry and customer needs, and stating the problems (cf. Introduction).

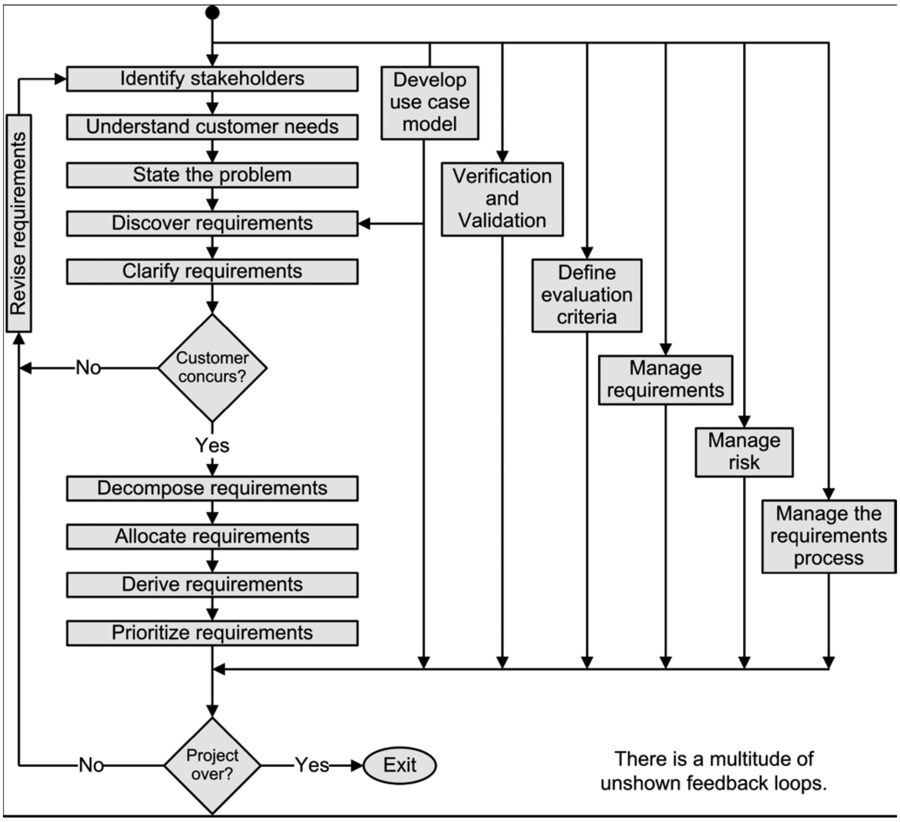

Figure 2 - Requirements expression process as defined in "Discovering system requirements, Chapter 4 in Handbook of Systems Engineering and Management" [6]

As mentioned, the complete synthesis of the use cases requirements will be presented in two documents, namely deliverable D4.1 and deliverable D4.2. Intermediate reports are in the form of milestones MS35 and MS39. Therefore, deliverable D4.1 did not cover the whole requirements process definition of Figure 2. Deliverable D4.1 contains all requirements known and defined in the use cases up to the date of release of the document. In an incremental process, new and complementary requirements will be regrouped in deliverable D4.2 to list all use cases requirements of the project.

In support to this requirement expression process, the project has defined a specific use case template based on the project needs, partners knowledge and experiences in the field of use case definition, the ETSI AFI Industry Specification Group work item 1 – [7], and includes elements of Alistair Cockburn use case template model and guidelines [8].

In the following sections requirements are named in the following way:

- Req_B_x.y is denoted as the *y* Business requirement of use case *x*
- Req_F_x.y is denoted as the *y* Functional requirement of use case *x*
- Req_NF_x.y is denoted as the *y* Non-functional requirement of use case x

The language adopted for the formulation of the requirements is based on IETF and ETSI guidelines [9], [10]. More specifically, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119 [9]:

- MUST: this word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT: this phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.

- SHOULD: this word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: this phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- MAY: this word, or the adjective “OPTIONAL”, means that an item is truly optional.

The following sections (namely Sections 4, 5 and 6) analyse the business, functional and non-functional requirements that have been derived from the set of UniverSelf use cases. As said earlier, at this stage, the list of requirements as reported in D4.1 might not be exhaustive as additional use cases can be defined in the course of the project and further refinement/completion of the use case analysis and feedback can derive in new/refined requirements (MS39/D42). This is conforming to the process identified in the project Description of Work.

4 Business Requirements

This section focuses on business requirements describing in business terms what the UMF should deliver or accomplish to provide value for a network operator, derived from the various use cases.

Considering the operation of today's networks, two main issues can be identified, which have an impact on the business level, as they lead to high costs. One issue is the diversity of the elements comprising in the network infrastructure (e.g. a network operator may operate base stations from various vendors each of which provides a different management entity). Thus configuration of an operators' network often needs to be customized for various parts of the infrastructure, requiring a great deal of human intervention. Another major issue is the gap between high-level specification of human operators' objectives and existing resource management infrastructures towards the achievement of global goals. In this sense, the UMF should provide support for addressing such technical issues, and thus reducing the cost of operation for a network operator.

In this sense, from a business perspective the UMF should enable:

- **Reduction of the time to market (deploy) new services**. The UMF should allow for the dynamic and automated (in terms of network configuration) deployment of new services. This should enable a network operator to provide a larger service portfolio and thus may indirectly lead to an increase of Revenues.
- **Relations with Third Parties**. It should be noted that new services may be provided by third parties, so UMF should allow handling the relationships with these third parties
- **Reduction of the time required to make changes in the network configuration**. The UMF should provide mechanisms to adjust features of the network infrastructure in an autonomous manner, based on service and business requirements as well as the current status of the network. This should lead to OPEX reductions.
- **Reduction of the cost of deploying new services and of operating the network**. The UMF should provide support that will enable the reduction of the human intervention required for deploying new services and configuring the network (OPEX reduction). Moreover, support should be provided for the interoperability between diverse elements (from various vendors) of the network infrastructure, reducing the need for new equipment/software (CAPEX reduction).
- **Increase of the efficiency of deploying new services and making changes to the network configuration.** As already introduced, the UMF should allow for the configuration of the network of an operator in an autonomous, cognitive manner taking into account business requirements as well as the current status of the network. Apart from OPEX reductions that can be derived this should also lead to improved Quality of Experience for users and thus decreased churn rate.
- **Increase of the efficiency of operating the network and handling errors.** The UMF should provide support that will enable reducing the need for human intervention by introducing self-* features in configuration phases thus improving the overall efficiency and reducing errors that may occur. Increased efficiency may also offer opportunities for utilizing network resources in diverse ways, potentially opening new revenue streams for operators. Moreover, support should be provided so that errors can be handled more efficiently, e.g. reducing the time required for their repair.

In the following, business requirements and potential impacts are further analysed per use case.

Use Case #1 - focusing on self-diagnosis and self-healing in IMS environment

Delivering a rich QoS to end-users can take different forms. Realizing self-diagnosis and self-healing can provide new possibilities/means for the network operator/service provider to improve its service offer/quality. For instance, one of the goals of UC1 is to improve diagnosis capabilities, which should enable faster isolation of the failure(s), and mitigate the impact (and even to predict the failure and avoid the detrimental effects). Such technological advance should raise the end-user offered QoS by lower Time-to-Repair (and possibly guided/reparation information displayed on the TV screen/mobile device...) and thus should lead to increased service availability; it should also reduce the cost per service/per customer with less calls to the help desk. A unified diagnosis solution which is applicable to multiple IMS services (semantic approach) and to diverse technological domains (wireline/wireless, service platform) should also bring economy of scale to the operator, which should add to the OPEX gains (single/shared solution versus services/networks) for service assurance. The main business requirements for UC1 are summarized in the following table:

Table 2 - Use case 1 business requirements

ID	Name
Req_B_1.1	Reduction of time to repair errors/problems
The UMF should enable to decrease the time required to repair problems in the network (this is reducing OPEX).	
ID	**Name**
Req_B_1.2	Reduction of cost per service/per customer
The UMF should enable to decrease the cost per service/per customer of repairing problems in the network e.g. with less calls to the help desk and less required time to repair (this is reducing OPEX).	
ID	**Name**
Req_B_1.3	Increase of efficiency of operating the network and handling errors
The UMF should enable to improve the overall efficiency of network operation as well as handling errors.	
ID	**Name**
Req_B_1.4	Increase of service availability
The UMF should enable to increase service availability by reducing the errors/problems that occur in the network and reducing the time required to repair such errors/problems.	
ID	**Name**
Req_B_1.5	Reduction of churn rate
The UMF may enable to reduce the churn rate by increasing the QoE.	

Use Case #2 - focusing on network stability and performance

In the medium-long term, future networks will become so ubiquitous so as to appear as networks of networks of highly interconnected nodes. As such, if today configuration errors are a large portion of Operators' errors (and in turn the largest contributor to failures and repair time in the medium-long term, configuration problems will exacerbate even more. As a consequence, it appears that reducing human intervention by introducing self-* features in configuration phases shall improve overall efficiency and shall reduce Operators' errors. On the other hand, this will make future networks like large scale complex systems implying intrinsically the existence of multiple phases in their behaviours: this means that in principle identical local dynamics can give rise to widely different global dynamics, with the risk of jeopardizing network performance. For instance the main focus of UC2 is studying the controllability, stability and phase transitions in ubiquitous future networks empowered with self-* features. Operators' trust in autonomics requires solutions allowing both to validate (off-line) the effects of interacting self-* features (e.g. Self Organizing Entities) before provisioning, and continuously monitoring (on line) networks and services stability parameters. This should allow Operators to make cost savings by introducing self-* features, whilst, importantly, keeping full control of network and service dynamics. The main business requirements for UC2 are summarized in the following table:

Table 3 - Use case 2 business requirements

ID	Name
Req_B_2.1	Costs savings due to reduction of configuration mistakes (before provisioning)
Off-line validation of the effects of interacting self-* features (e.g. Self Organizing Entities) before their activation will allow reducing configurations mistakes and network instabilities. This will determine cost savings.	
ID	**Name**
Req_B_2.2	Costs savings due to reduction of unexpected network instabilities (during operations)
On-line validation of the effects of interacting self-* features (e.g. Self Organizing Entities) will allow reducing unexpected network instabilities. This will determine cost savings.	
ID	**Name**
Req_B_2.3	New revenues from "network and service stability" as a service
Assuring network and service stability (with different levels) in an open context (e.g., against diverse internal and external roots of instabilities) can be seen as new advanced service provided by Operators, thus improving competitiveness: this can be considered potentially as a source of new revenues.	

Use Case #3 - focusing on dynamic virtualization and migration of contents and servers

Today, most of network management occurs at the core and users are increasingly communicating with the mobile operator's data centres for their services and application requirements. Hence user traffic has to go through the core/backbone/backhaul resulting in consumption of resources as well as making the service dispensation susceptible to various performance impeding bottlenecks. The effective dispensation of services and efficient utilization of resources becomes all the more important for time/quality sensitive and bandwidth intensive mobile applications such as mobile video traffic (streaming and broadcast). The ubiquitous provisioning of such applications is putting a lot of pressure on mobile network operators and their respective infrastructures (especially the core and backhaul).

In view of this scenario, the main aim of UC3 is to enable the dynamic (on-the-fly and on-demand) realization of services/functions/gateways nearer to the user by leveraging the cloud computing and virtualization techniques to provide true NaaS (Network as a Service). This shall cause most of the user traffic and service demands to get negotiated and managed nearer to the user without having to traverse the core/backbone. This reduction/shifting of load from the core/backbone shall allow the operator to oversubscribe its network resources (bandwidth, processing. storage etc.) and also enhance the utilization of the resources in the backhaul and access. This should translate into increased ROI and revenue base while seeing a corresponding reduction in CAPEX. Additionally, parts of the virtualized operator network may potentially be made available via specific interfaces to 3rd party service providers so that these may optimize their services by taking advanced network and user information from the operator into account. This may also open a potentially new revenue stream for the operator. Finally, UC3 addresses the need to facilitate new service deployments (and therefore the time to market) even for new services from the operator himself in that the operator may be using his own infrastructure cloud and the associated management platform, which has been designed anyway for easy service deployability. The main business requirements for UC3 are summarized in the following table:

Table 4 - Use case 3 business requirements

ID	Name
Req_B_3.1	Increase of ROI
The UMF should lead to the increase of ROI through the reduction/shifting of load from the core/backbone that shall allow the operator to oversubscribe its network resources (bandwidth, processing, storage etc.) and also enhance the utilization of the resources in the backhaul and access (this will determine CAPEX reductions).	
ID	**Name**
Req_B_3.2	Increase of revenue base
The UMF should lead to an increase of the revenue by opening new revenue streams and business models for the operator (e.g. by making available parts of the virtualized operator network via specific interfaces to 3rd party services).	
ID	**Name**
Req_B_3.3	Reduction of churn rate
The UMF may enable to reduce the churn rate by increasing the performance of the network.	
ID	**Name**
Req_B_3.4	Increase of the efficiency of deploying new services
The UMF should enable to facilitate new service deployments.	
ID	**Name**
Req_B_3.5	Decrease of the time required to market (deploy) new services
The UMF should enable to decrease the time to market new services.	

Use Case #4 – focusing on SON and SON collaboration according to operator policies

Future radio access networks, e.g. LTE and LTE-A, will be empowered by self-organizing network (SON) mechanisms that must simplify network management, reduce its cost of operation and increase its performance. In other words, business requirements derived from this use case are related to performance, competitiveness, OPEX and CAPEX. More specifically, coordinated SON functionalities should improve capacity, coverage and QoS performance. Furthermore, the increased performance gain achieved through SON mechanisms may improve the operator ranking, and consequently increase its competitiveness, reduce the churn rate and potentially lead to an increase in the revenues of the operator. In terms of costs, performance gains in certain cases may be translated to delaying or reducing investments in the infrastructure; in other words CAPEX may be reduced. Finally, SON mechanisms should facilitate the decrease of (additional) efforts related to network operation activity of LTE and LTE-Advanced technology to configure, parameterize and optimize the network, thus leading to OPEX reduction. The main business requirements for UC4 are summarized in the following table:

Table 5 - Use case 4 business requirements

ID	Name
Req_B_4.1	Increase of revenues due to improvement of network performance

ID	Name
The UMF should enable to improve capacity, coverage and QoS performance. This will make the network more competitive from a business viewpoint determining an increase of revenues	
ID	**Name**
Req_B_4.2	Improvement of operator ranking
The UMF may enable to improve the operator ranking and consequently increase its competitiveness by improving QoS and QoE provisioning	
ID	**Name**
Req_B_4.3	Reduction of CAPEX
The UMF should reduce CAPEX by delaying or reducing additional infrastructure investments	
ID	**Name**
Req_B_4.4	Reduction of OPEX
The UMF should facilitate the decrease of (additional) efforts related to network operation activity of LTE and LTE-Advanced technology to configure, parameterize and optimize the network. Thus UMF SON mechanisms should lead to OPEX reduction.	
ID	**Name**
Req_B_4.5	Reduction of churn rate
The UMF may enable to reduce the churn rate by improving QoS and QoE for the network users.	
ID	**Name**
Req_B_4.6	Migration to legacy systems
Migration of UMF to legacy systems should take into account economical aspects (e.g. limited impact of UMF cost-of-features and the other costs related to its introduction)	

Use Case #5 – focusing on network morphing

For network operators, that operate multilayer networks (built from different areas of consistent technology, some of which are offering a connectivity/transport service to others), network morphing is an autonomic connectivity management solution that provides a dynamic adaptation of the connectivity to traffic/services demand variations and thus ensures a network configuration whose cost is kept close to the optimal (according to certain cost criteria/policy). Furthermore, network morphing should enable a network operator to maximize the utilization of transport resources over time and adapt to expected and unexpected traffic/services demands and contextual situations. In other words, network morphing should enable the best possible usage of available resources. The main business requirements derived from this use case are related to the reduction of costs required to sustain and operate the network. More specifically, network morphing should enable the decrease of the overall number of resources needed (installed) across the layers in order to ensure the services supported thus implicitly leading to CAPEX reductions. Furthermore, network morphing should decrease the average number of resources in-use across the layers in order to ensure the services supported thus should lead to a reduction of OPEX (Electrical power consumption decrease). The main business requirements for UC5 are summarized in the following table:

Table 6 - Use case 5 business requirements

ID	Name
Req_B_5.1	Reduction of CAPEX
The UMF should facilitate CAPEX reductions through network morphing, which enables the decrease of the overall number of resources needed (installed) across the layers in order to ensure the services supported.	
ID	**Name**
Req_B_5.2	Reduction of OPEX
The UMF should facilitate OPEX reductions through network morphing, which enables the decrease of the average number of resources in-use across layers in order to ensure the services and consequently of leads to the decrease of electrical power consumption.	
ID	**Name**
Req_B_5.3	Reduction of churn rate
The UMF may enable to reduce the churn rate by increasing the performance of the network and consequently the QoE, through adaptation to expected and unexpected traffic/services demands and contextual situations.	

Use Case #6 – focusing on operator-governed, end-to-end, autonomic, joint network and service management

The use case aims at finding solutions that will:

- Enable operators to describe their goals and objectives, through high-level means and govern their network through autonomous operations.
- Achieve policy-based operation of Radio Access Network (OFDMA-based) and Backhaul/Core Network (IP/MPLS-based) segments, which is optimized with respect to QoE/QoS (and energy) efficiency, taking into account metrics derived in network nodes and end-user devices as well as operator objectives.
- Achieve coherence between these segments through cooperation, negotiation and federation.

The autonomous operations targeted in this UC should decrease transaction costs and the need for human intervention, thus lowering OPEX which has become the most important part of a network global cost. Autonomous management should also minimize the error ratio caused by such human intervention. At the same time, network knowledge should enable the optimisation of dynamic allocation and usage of network resources (CAPEX reduction) for example through "cognitive" traffic engineering decisions. Besides, the UC greatly facilitates the deployment and management of new services as network properties required to fulfil that service can be expressed in terms of business metrics. The main business requirements for UC6 are summarized in the following table:

Table 7 - Use case 6 business requirements

ID	Name
Req_B_6.1	Reduction of human intervention
The UMF should enable to reduce the need for human intervention.	
ID	**Name**
Req_B_6.2	Reduction of human error ratio
The UMF should enable to reduce the ratio of errors that occur due to human intervention.	
ID	**Name**
Req_B_6.3	Reduction of time required for service/network configuration
The UMF should enable to reduce the time required for deciding and enforcing changes in the configuration of services and the network.	
ID	**Name**
Req_B_6.4	Increase of the efficiency of deploying new services
The UMF should enable to facilitate new service deployments.	
ID	**Name**
Req_B_6.5	Decrease of the time required to market (deploy) new services
The UMF should enable to decrease the time required to market new services.	
ID	**Name**
Req_B_6.6	Reduction of churn rate
The UMF may enable to reduce the churn rate by increasing the QoE.	
ID	**Name**
Req_B_6.7	Reduction of CAPEX
The UMF should enable to facilitate CAPEX reductions by enabling optimal utilization of resources and delaying or reducing additional investments in the infrastructure.	
ID	**Name**
Req_B_6.8	Reduction of OPEX
The UMF should enable to reduce OPEX by reducing the need for human intervention through autonomic self-management procedures and cognitive "traffic" engineering decisions.	

Use Case #7 – focusing on network and services governance

Telco operators have the need to adapt their operations in order to reduce the time to market and the network maintenance costs, while at the same time increasing the customer satisfaction. There is an agreement in the research community that autonomic networks with self-configuration, self-diagnosis and self-healing capabilities will help in the automation of the provisioning and runtime phases, maintaining the quality of the services committed to the customer with minimal human intervention. These improvements should be accompanied by a transformation in the business definition of services and the actual deployment at the network level. The agreement between a client and a service provider specifies service level objectives, both as expressions of client requirements and as provider's assurances. These objectives are expressed in a high-level, service-, or application-specific manner, but should be translated to the low-level, resource specific language of the network elements. Current (semi-)manual practices must be minimized as much as possible, as they always imply certain delay in the delivery of new services. Furthermore, they require highly specialized technicians for the management of the network.

UC7 focuses on mechanisms that address the gap between high-level specification of client performance objectives and existing resource management infrastructures. Such mechanisms should provide operators with means for decision oriented operational tasks based on the use of policies rather than low level command execution, thus should decrease the human intervention required for deploying new services, configuring and operating the network. This should lead to reduction of time to market as well as OPEX. Furthermore, network and service governance should enable improved QoS/QoE and consequently should lead to reduced churn rate and potentially increased revenues. UC7 will demonstrate the feasibility of a policy-based management network on top of one of the technologies for the delivery of high speed broadband access: FTTH. Currently, telecommunication operators are making huge investment efforts in fibre-to-the-home deployments, which is consider the network of the future in fixed access segment, able to support ultra-broadband speeds.

Traditional service provider operations support system (OSS) infrastructures and organizations often lack the end-to-end processes necessary to assure the quality of the new IP services. The real challenge for operators, if they aim to handle broadband growth for millions of subscribers, is to develop optimized operational models introducing efficient service management and operational processes across the network and converged services architecture. The measurement of the QoE is an essential part of a service provider's competitive strategy for offering future services. UC7 aims to provide a service assurance solution for FTTH environments, providing the network elements with self-monitoring, self-diagnosis and self-healing possibilities. These functionalities will enable the early detection and resolution of network, QoS, and QoE problems with limited or no customer impact. As a consequence, network and service governance applied on FTTH networks should enable improved QoS/QoE and therefore should lead to reduced churn rate and potentially increased revenues. The main business requirements for UC7 are summarized in the following table:

Table 8 - Use case 7 business requirements

ID	Name
Req_B_7.1	Reduction of human intervention
The UMF should enable to decrease the human intervention required for the deployment, configuration and operation of new services on FTTH networks	
ID	**Name**
Req_B_7.2	Reduction of high specialized personnel in maintenance tasks
The UMF should enable to decrease the needed of high specialized technicians for purely maintenance of the network, that could be easily managed and supervised through the Governance framework.	
ID	Name
Req_B_7.3	Reduction of time required for service/network configuration
The UMF should enable to decrease the time required for the deployment, configuration and operation of new services on FTTH networks.	
ID	**Name**
Req_B_7.4	Reduction of the downtime of a service
The UMF should enable to decrease the service downtime, thanks to the proactive self-monitoring, self-diagnosis and self-healing capabilities.	
ID	**Name**
Req_B_7.5	Reduction of OPEX
The UMF should enable to reduce OPEX by reducing the need of highly specialized technicians through autonomic self-management procedures applied to FTTH network elements.	
ID	**Name**
Req_B_7.6	Increase of the efficiency of deploying new services
The UMF should enable to facilitate new service deployments through the use of the Network Governance Framework, which allows the automatic translation from high-level business requirements to network policies.	
ID	**Name**
Req_B_7.7	Decrease of the time required to market (deploy) new services
The UMF should enable to decrease the time required to market new services, through the use of the Network Governance Framework, which allows the automatic translation from high-level business requirements to network policies.	

ID	Name
Req_B_7.8	Reduction of churn rate
The UMF may enable to reduce the churn rate by increasing the QoE of the FTTH customers.	

5 Functional Requirements

This section describes the use case functional requirements, as derived from the analysis of the UniverSelf use cases. Such requirements highlight key features of the UMF and Network Empowerment solutions that are necessary to provide solutions to specific technical problems.

Table 9 - Use case 1 functional requirements

ID	Name
Req_F_1.1	Access mechanism to raw Service data
UMF shall give access mechanisms to any raw service data (Performance indicators, Services alarms, Services configuration, Services semantic, Services messages)	
ID	**Name**
Req_F_1.2	Access mechanism to raw Network data
UMF shall give access mechanisms to any raw network data (Alarms, Protocols configuration, Protocols semantic, Protocols messages, Hardware parameters, Performance indicators)	
ID	**Name**
Req_F_1.3	Elaborated Data/Context Management
UMF shall give a method to access context database for obtaining/storing/updating context information	
ID	**Name**
Req_F_1.4	Knowledge Data Management
UMF shall give a method to access knowledge base for obtaining/storing/updating knowledge information	
ID	**Name**
Req_F_1.5	Topology information Monitoring
UMF shall give a method for monitoring any topology information data.	
ID	**Name**
Req_F_1.6	Contextual data translation
UMF shall give a method for the translation of contextual data (upper layers to lower layers in the hierarchy).	
ID	**Name**
Req_F_1.7	Contextual data filtering/pre-processing
UMF shall give a method to perform filtering and pre-processing to contextual data (lower layers to upper layers in the hierarchy).	
ID	**Name**
Req_F_1.8	Diagnosis Embodiment
UMF must enable embodiment of the proactive diagnosis mechanism	
ID	**Name**
Req_F_1.9	Root cause analysis from alarms
UMF should be able to pinpoint the root cause among many alarms and identify the problems that need to be fixed	
ID	**Name**
Req_F_1.10	Horizontal data correlation
UMF must give a method to correlate Intra/Inter-Domain data.	
ID	**Name**
Req_F_1.11	Vertical data correlation
UMF must give a method to enable Cross-Technological and Cross-Organizational correlation.	
ID	**Name**
Req_F_1.12	Time scale data correlation
UMF must Give a method to enable a Time scale data correlation.	
ID	**Name**
Req_F_1.13	Model for Anomaly Prediction pattern data exchange
UMF must provide model to exchange prediction pattern	
ID	**Name**
Req_F_1.14	Model for Normality Prediction pattern data exchange
UMF should provide model to exchange prediction pattern	
ID	**Name**
Req_F_1.15	Model for Anomaly diagnosis exchange
UMF must provide model to exchange anomaly detection.	

ID	Name
Req_F_1.16	Model for Normality diagnosis exchange
UMF should provide model to exchange Normality detection.	
ID	**Name**
Req_F_1.17	Model for Complex data
UMF should provide Key Performance Indicator models.	
ID	**Name**
Req_F_1.18	Model for Complex data exchange
UMF should provide models to exchange KPI	
ID	**Name**
Req_F_1.19	Data sharing exchange methods
UMF must provide data sharing methods between self-x enabling elements.	
ID	**Name**
Req_F_1.20	Mitigation policies exchange
UMF should provide mitigation policies for each predicted event.	
ID	**Name**
Req_F_1.21	Interface with NMS
UMF shall provide Interface with NMS for upstream data exchange (raw data coming from monitoring, event reporting, evaluation of the system after a mitigation/ reparation plan) and downstream data exchange (high level data monitoring such as KPI or aggregated data, data to be monitored and re-configuration actions)	
ID	**Name**
Req_F_1.22	Predicted event reporting to Human
UMF should provide Self-x enabling elements and Network (NMS) to human interfaces (OSS) for event detection reporting.	
ID	**Name**
Req_F_1.23	Predicted event reporting to Network
UMF must provide Self-x enabling elements to Network entities (NMS) interfaces to share detection reports.	
ID	**Name**
Req_F_1.24	Predicted event reporting to Self-x enabling element
UMF must provide interfaces to share detection reports between Self-X enabling elements	
ID	**Name**
Req_F_1.25	Triggered Mitigation reporting to Human
UMF should provide Self-x enabling elements and Network (NMS) to human(OSS) interface for mitigation triggering reporting	
ID	**Name**
Req_F_1.26	Triggered Mitigation reporting to Network
UMF must provide Self-x enabling elements to Network (NMS) interface for mitigation triggering reporting.	
ID	**Name**
Req_F_1.27	Triggered Mitigation reporting to Self-x enabling element
UMF must provide interfaces to share mitigation triggering reports between self-x enabling elements.	
ID	**Name**
Req_F_1.28	Event prediction algorithms Coordination
UMF must allow algorithm coordination between multiple event prediction nodes.	
ID	**Name**
Req_F_1.29	Data Aggregation
UMF should aggregate the monitored data in order to reduce the amount of data to be analyzed	
ID	**Name**
Req_F_1.30	Traffic Anomaly Detection
UMF must provide methods for the detection (proactive or reactive) of events such as network traffic anomalies, faults and congestion.	
ID	**Name**
Req_F_1.31	NMS function to NMS function Interfaces

UMF must provide interfaces for exchanges between NMS functional blocks such as Situation Analysis/ Diagnosis, Candidate Solution Computation and Solution Selection and Elaboration or NMS functionalities.	
ID	**Name**
Req_F_1.32	OSS Interface to NMS
UMF must provide interface for communicating operator's goals to NMS so as to be taken into account for the selection of the mitigation/ reparation plan (human to network interfaces for inserting business goals to be translated into policies).	
ID	**Name**
Req_F_1.33	EMS to OSS interface
UMF must provide Network (EMS) to human interface (OSS) for reporting failure of re-configuration actions.	
ID	**Name**
Req_F_1.34	Human to Network Interface
UMF must provide H2N Interface for reporting users' problems and evaluation of the system.	

Table 10 - Use case 2 functional requirements

ID	Name
Req_F_2.1	Active Self-Monitoring
UMF shall have a feature for active self-monitoring (i.e. sending events and/or probe packet(s) into the network and measuring responses, e.g. in terms of QoS parameters)	
ID	**Name**
Req_F_2.2	Passive Self-Monitoring
UMF shall have a feature for passive self-monitoring (i.e. capturing data as it passes by)	
ID	**Name**
Req_F_2.3	Network Knowledge Extraction
UMF shall have features to collect, filter and elaborate monitored data and events in order to extract network knowledge.	
ID	**Name**
Req_F_2.4	Network Stability Models
UMF shall have a set of network stability models with the related indicators to be used for proactive and reactive network stabilization actions.	
ID	**Name**
Req_F_2.5	Proactive Self-Stabilization
During Operations, UMF shall allow proactive self-stabilization actions (e.g. prediction and preventive actions)	
ID	**Name**
Req_F_2.6	Reactive Self-Stabilization
During Operations, UMF shall allow reactive self-stabilization actions (e.g. detection and corrective actions)	
ID	**Name**
Req_F_2.7	Human de-activation of self-* features
During Operations UMF shall allow humans (e.g. through a specific interface) to take actions to deactivate "autonomic and self-*" features	
ID	**Name**
Req_F_2.8	On-line self-prevention actions
During Operations, UMF shall allow to take on-line self-prevention actions (e.g. coordination, conflict resolution of self-* features)	
ID	**Name**
Req_F_2.9	External knowledge
UMF shall allow to exploit also external knowledge (e.g. vulnerable state descriptions)	
ID	**Name**
Req_F_2.9	Validation of self-* features
During Planning, UMF shall allow to validate the activation of self-* features (e.g. though simulation and to prediction of network dynamics using off-line tool)	
ID	**Name**
Req_F_2.10	Orchestration of self-* features
During Operations, UMF shall orchestrate self-* features to assure network stability and performance.	
ID	**Name**
Req_F_2.11	Map of self-* features
UMF shall have a map (e.g. repository) about all self-* features deployed into the network (Operators may wish to have a full control how and where self-* features are deployed)	
ID	**Name**

Req_F_2.12	Human Interface for on-line
UMF shall have a human interface to assess on-line network stability and to de-activate self-* features	
ID	**Name**
Req_F_2.13	Human Interface for off-line
UMF shall have a human interface to assess off-line validation of self-* features	

Table 11 - Use case 3 functional requirements

ID	Name
Req_F_3.1	H2N interface
The UMF shall provide a H2N Interface to insert high level goals, to deliver control and management and to feedback system checks	
ID	**Name**
Req_F_3.2	Policy language translation
The UMF shall provide translation of operator specified Policies into clear configuration and management actions	
ID	**Name**
Req_F_3.3	Data Monitoring
The UMF shall provide/support means for the monitoring of access/backhaul networks (nodes and links).	
ID	**Name**
Req_F_3.4	Mobility Management
The UMF shall support QoS aware mobility management (incl. movement detection and handover execution)	
ID	**Name**
Req_F_3.5	Data processing
UMF shall provide tools and means for aggregation & processing of monitored data	
ID	**Name**
Req_F_3.6	Network Monitoring
UMF MUST provide means to monitor and evaluate for End-to-End (E2E) connection/session status/statistics	
ID	**Name**
Req_F_3.7	Conflict management
UMF SHOULD have some degree of Conflict resolution (signalling vs. performance)	
ID	**Name**
Req_F_3.8	Platform management
The UMF MAY support Multi-homed/multi-interface devices for effective load balancing (e.g., flow mobility) and efficient resource management (e.g., capacity increase).	
ID	**Name**
Req_F_3.9	Capabilities discovery
UMF shall discover Service/network capabilities (e.g., bandwidth, error rates, modulation, energy, processing power, storage, transcoding abilities etc.)	
ID	**Name**
Req_F_3.10	Route management
The UMF may support routing strategies for Route optimization	
ID	**Name**
Req_F_3.11	Fault tolerance
The UMF shall provide necessary context information with global-scope for Load balancing (i.e., congestion control/fault tolerance) – in backhaul and access networks. The load balancing strategy will be used to circumvent failed/congested/non-optimum nodes/paths.	
ID	**Name**
Req_F_3.12	Resource management
The UMF shall provide methods for autonomic resource management (& allocation) – incl. tunnel management	
ID	**Name**
Req_F_3.13	Virtualization Management
The UMF MAY provide control and management methods for content/function/gateway virtualisation/migration	
ID	**Name**
Req_F_3.14	Service data Monitoring
UMF shall Give a method to access in monitoring purpose to any service data (Performance indicators, Services alarms, service’s configuration, services semantic, services messages).	
ID	**Name**
Req_F_3.15	Network data Monitoring

UMF shall give a method to access in monitoring purpose to any network data (e.g., alarms, protocol configuration/semantics/messages, hardware parameters, performance indicators etc.)	
ID	**Name**
Req_F_3.16	Elaborated Data/Context Management
UMF shall give a method to access context base for obtaining, storing and updating context information.	
ID	**Name**
Req_F_3.17	Knowledge Data Management
UMF shall give a method to access knowledge base for obtaining, storing and updating knowledge information.	
ID	**Name**
Req_F_3.18	Topology information Monitoring
UMF shall give a method to access in monitoring purpose to any topology information data.	
ID	**Name**
Req_F_3.19	Contextual data translation
UMF shall give a method for the translation of contextual data (upper layers to lower layers in the hierarchy).	
ID	**Name**
Req_F_3.20	Contextual data filtering/pre-processing
UMF shall give a method to perform filtering and pre-processing to contextual data (lower layers to upper layers in the hierarchy).	
ID	**Name**
Req_F_3.21	Information flow management
The UMF shall provide interfaces for communication, between Knowledge repository and decision engine, between SON entities and Governance tool, and also amongst different SON entities.	

Table 12 - Use case 4 functional requirements

ID	Name
Req_F_4.1	H2N interface
UMF shall provide a H2N/GUI interface for inserting operator targets and policies	
ID	**Name**
Req_F_4.2	Information for self-X operation
UMF shall provide Information for operating SON functionalities (network topology including the location of self-X entities, traffic characteristics, performance and QoS indicators)	
ID	**Name**
Req_F_4.3	Interfaces for self-X governance
UMF shall provide Interface between governance tools and self-X entities, to allow to insert, modify, interact with and monitor self-X processes	
ID	**Name**
Req_F_4.4	Interfaces for self-X operation
UMF shall provide interface for communication between SON entities and between SON entities and the network	
ID	**Name**
Req_F_4.5	Policy repository
UMF shall provide policy repositories for storing the defined policy rules.	
ID	**Name**
Req_F_4.6	Policy language
UMF shall provide policy language to allow operating self-X functions	
ID	**Name**
Req_F_4.7	Policy generation
UMF should allow generating policies using a tool accessible via H2N interface	
ID	**Name**
Req_F_4.8	Self-X triggers
UMF shall define triggers of self-X functions. Triggers should include events in time, periodic and manual activation, for a predetermined duration	
ID	**Name**
Req_F_4.9	Policies for self-X operation
UMF shall provide rules/policies for operating self-X entities (to identify the involved self-X entities; to activate / deactivate self-X functions, to transfer high level goals to low level operation of self-X entities; to provide information to - and from self-X algorithms; to allow the interaction between self-X entities, and between self-X and other network entities; to resolve conflicts between running self-X processes when coordination fails)	

<table>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_4.10</td><td>Self-X monitoring</td></tr>
<tr><td colspan="2">UMF shall allow monitoring network performance and parameters (including indicators related to- and parameters modified by SON running processes)</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_4.11</td><td>Self-recovery</td></tr>
<tr><td colspan="2">In case of human intervention in the autonomic system (policy modification, deactivation, update/evolution of monitored KPI set), the system should return smoothly and quickly to the autonomic process</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_4.12</td><td>Policy adjustment</td></tr>
<tr><td colspan="2">UMF shall allow adjusting policies according to feedback from running self-X processes</td></tr>
</table>

Table 13 - Use case 5 functional requirements

<table>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.1</td><td>Knowledge data management</td></tr>
<tr><td colspan="2">UMF must provide features to store and retrieve past observations, states and decisions, such as past traffic measurements, bandwidth estimations, network configurations</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.2</td><td>Traffic data monitoring interface</td></tr>
<tr><td colspan="2">UMF must provide interfaces for monitoring packet traffic data inside network equipments</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.3</td><td>Traffic aggregation</td></tr>
<tr><td colspan="2">UMF must provide features to aggregate network core traffic data in quasi real-time with control over the aggregation process.</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.4</td><td>Aggregated traffic data interface</td></tr>
<tr><td colspan="2">UMF must provide interfaces for monitoring aggregated traffic data in a streaming fashion with periodical or on-demand export.</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.5</td><td>Bandwidth estimation</td></tr>
<tr><td colspan="2">UMF must provide methods to estimate bandwidth needs from aggregated traffic data.</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.6</td><td>Bandwidth estimation data interface</td></tr>
<tr><td colspan="2">UMF must provide interfaces to access the bandwidth estimations (either in pull or push mode)</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.7</td><td>Network parameter monitoring</td></tr>
<tr><td colspan="2">UMF must provide features to monitor network parameters, such as link capacity, network load, traffic flows between segments, delay, jitter, energy consumption.</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.8</td><td>Network parameter monitoring interface</td></tr>
<tr><td colspan="2">UMF must provide interfaces for monitoring network parameters</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.9</td><td>Network topology model</td></tr>
<tr><td colspan="2">UMF must provide an abstraction of the network topology for routing optimization</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.10</td><td>Implementing routing optimizations and load balancing</td></tr>
<tr><td colspan="2">UMF must provide interfaces for implementing routing optimizations and load balancing on involved network elements for MPLS.</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.11</td><td>Policy rules for routing table updates</td></tr>
<tr><td colspan="2">UMF must provide features to define policy rules that trigger updates on network elements routing tables</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.12</td><td>Distribution of policy rules for routing table updates</td></tr>
<tr><td colspan="2">UMF must provide features to distribute policy rules among network elements to enforce the routing path update</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_F_5.13</td><td>Triggering routing optimization</td></tr>
<tr><td colspan="2">UMF must provide decision mechanisms to specify when MPLS optimized routing paths should be computed (offline, online)</td></tr>
<tr><th>ID</th><th>Name</th></tr>
</table>

Req_F_5.14	Network configuration sharing
UMF must provide mechanisms to collect and aggregate network configuration, responding to requests of route descriptions for given traffic descriptions (input/output/bandwidth/type/QoS)	
ID	**Name**
Req_F_5.15	Alternative configuration suggestion
UMF must provide mechanisms to suggest alternative network configurations to handle a given traffic (described by input/output/bandwidth/type/QoS)	
ID	**Name**
Req_F_5.16	Configuration costs sharing
UMF must provide mechanisms to collect and aggregate network configuration costs, responding to requests of (i) cost description for given traffic or route descriptions, (ii) cost of configuration changes/updates.	
ID	**Name**
Req_F_5.17	Apply network configuration changes
UMF must provide mechanisms to apply a configuration change in the network, treating a sequence of atomic actions, being able to handle configurations described by IDs.	
ID	**Name**
Req_F_5.18	Human enhancement of bandwidth estimation
UMF should allow network operators to support/enrich the bandwidth estimation mechanisms with inputs of seasonal or event-related traffic fluctuations	
ID	**Name**
Req_F_5.19	Generation of connectivity configuration changes
UMF must provide mechanisms to generate configuration changes, based on traffic knowledge, current configuration state and available configuration states	
ID	**Name**
Req_F_5.20	SLA compliance monitoring
UMF must provide mechanisms for monitoring SLA compliance, e.g. target data rate	
ID	**Name**
Req_F_5.21	SLA compliance monitoring interface
UMF must provide interfaces to the SLA compliance monitoring	
ID	**Name**
Req_F_5.22	SLA and configuration commands manipulation
UMF must provide H2N interfaces to edit SLAs and configuration commands	

Table 14 - Use case 6 functional requirements

ID	**Name**
Req_F_6.1	H2N interface for request and goals expression
UMF SHOULD provide the means (H2N interface with appropriate GUI) for the operator to express requests and goals	
ID	**Name**
Req_F_6.2	Policies derivation
UMF should provide functionality for the derivation of policies based on operator's requests and goals	
ID	**Name**
Req_F_6.3	Policy conflict resolution
UMF should provide functionality for policy conflict resolution	
ID	**Name**
Req_F_6.4	Business goals to policies translation
UMF should provide functionality for translation of business goals to policies	
ID	**Name**
Req_F_6.5	Policy rules distribution
UMF should enable distribution of policy rules among network elements to enforce policy decisions (e.g. routing path update)	
ID	**Name**
Req_F_6.6	Business level entries/request analysis
UMF should provide functionality for analyzing the business /service level requirements and derive (translate them to) technology (network) specific requirements	
ID	**Name**
Req_F_6.7	Candidate solutions discovery/determination
UMF should provide functionality for discovering/determining the candidate solutions (networks) that can satisfy the derived network requirements	
ID	**Name**

Req_F_6.8	Candidate solutions reasoning
UMF should provide functionality for reasoning with the candidate solutions (networks)	
ID	**Name**
Req_F_6.9	QoS optimization function
UMF should provide a mechanism that optimizes the provided QoS based on the resource consumption in the RAN	
ID	**Name**
Req_F_6.10	RAN management function
UMF should provide an autonomic RAN management mechanism to find the optimal RAN deployment configuration using information.	
ID	**Name**
Req_F_6.11	Applied policy translation to traffic engineering compatible commands
UMF should provide modules to translate the instructions from the applied policy to traffic engineering (e.g. DiffServ/MPLS) compatible commands	
ID	**Name**
Req_F_6.12	Collaboration and negotiation
UMF should provide collaboration and negotiation functions for the establishment of agreements and federation between and network segments (RAN & Backhaul/Core), domains, operators and service providers	
ID	**Name**
Req_F_6.13	Conflict resolution mechanisms
UMF should provide mechanisms for on-line conflicts and dependencies resolution for different self-optimization and/or self-healing actions	
ID	**Name**
Req_F_6.14	RAN & Backhaul/Core Network monitoring
UMF should provide functionality for monitoring RAN & Backhaul/Core Network parameters (e.g. Capacity, Network Load, traffic Flows between segments) to be taken into account in the load optimization	
ID	**Name**
Req_F_6.15	Conversion of generic configuration into technology-specific configurations
UMF should provide functionality for converting instances of a generic configuration model into technology-specific configurations	
ID	**Name**
Req_F_6.16	Autonomic functions for (self-)optimization actions
UMF should provide autonomic functions that will trigger the appropriate (self-)optimization actions	
ID	**Name**
Req_F_6.17	Policy repositories
UMF should provide policy repositories	
ID	**Name**
Req_F_6.18	Policy repository interface
UMF should provide interfaces for accessing policy repositories	
ID	**Name**
Req_F_6.19	Policy Models
UMF should provide policy models (network policies, routing update policies…)	
ID	**Name**
Req_F_6.20	Information and knowledge storage
UMF should provide storage for information and knowledge on SLAs, Applications, User classes, RAN (network, resources, configuration), Backhaul /Core (network, resources, configuration), Traffic mobility requirements, and Traffic demand descriptions	
ID	**Name**
Req_F_6.21	Information and knowledge retrieval
UMF should provide interfaces for retrieving information and knowledge on SLAs, Applications, User classes, RAN (network, resources, configuration), Backhaul /Core (network, resources, configuration), Traffic mobility requirements, and Traffic demand descriptions	
ID	**Name**
Req_F_6.22	RAN QoS level related offers
UMF should provide interfaces for requesting/receiving QoS level related offers from RAN (responsible RRMs)	
ID	**Name**
Req_F_6.23	RAN measurements collection
UMF should provide interfaces for collecting RAN measurements	
ID	**Name**
Req_F_6.24	Backhaul/core networks QoS level related offers

UMF should provide interfaces for requesting/receiving QoS level related offers from backhaul/core networks	
ID	**Name**
Req_F_6.25	Packet marking
UMF should provide modules and interfaces for packet marking in the backhaul/core segment. I.e. Mark packets in order to construct and control traffic classes (profiles) and indicate congestion levels.	
ID	**Name**
Req_F_6.26	Traffic monitoring in backhaul/core segment
UMF should provide interfaces for monitoring the traffic in the backhaul/core segment. I.e. Measure the provided QoS and the resources that are consumed (Energy, Green concept, etc)	
ID	**Name**
Req_F_6.27	Information & knowledge dissemination among segments
UMF should provide interfaces for enabling dissemination of information & knowledge between network segments (RAN & Backhaul/Core)	
ID	**Name**
Req_F_6.28	Network segments collaboration and negotiation
UMF should provide interfaces for collaboration and negotiation between network segments (RAN & Backhaul/Core)	
ID	**Name**
Req_F_6.29	Interface with network information
UMF should provide interfaces with network information. Network information may contain link status, link utilization, network loads, traffic Flows between segments	
ID	**Name**
Req_F_6.30	Interface with performance related information
UMF should provide interfaces with performance related information	
ID	**Name**
Req_F_6.31	Routing optimization interfaces
UMF should provide interfaces for implementing routing optimization on involved network elements	
ID	**Name**
Req_F_6.32	Network Parameters monitoring
UMF should monitor network parameters (e.g. Capacity, Network Load, traffic Flows between segments) to be taken into account in the load optimization	
ID	**Name**
Req_F_6.33	Network model information provision
UMF should provide network model information: provide network topology abstraction for routing optimization	
ID	**Name**
Req_F_6.34	Self-configuration functions
UMF should provide functions (at network and node level) to download the new configurations and perform diagnostic self-tests to make sure that the process is successfully completed or exceptions are identified.	
ID	**Name**
Req_F_6.35	Network device configuration interfaces/protocols
Interfaces and protocols for installing, manipulating and deletion of configuration of network devices	
ID	**Name**
Req_F_6.36	Online conflict resolution
Mechanisms for on-line conflicts and dependencies resolution for different self-optimization and/or self-healing actions	

Table 15 - Use case 7 functional requirements

ID	Name
Req_F_7.1	Information model
UMF must provide an information model that allows the representation of all the elements involved in the lifecycle of a service, starting from the business goals down to the network elements	
ID	**Name**
Req_F_7.2	Knowledge base
UMF must include a knowledge base to store all the relevant information for the modelling, provisioning and runtime phase of a service	
ID	**Name**
Req_F_7.3	Knowledge base management
UMF must provide mechanisms for the insertion, removal and modification of the information stored in the knowledge base	
ID	**Name**

Req_F_7.4	Business goals language
UMF must incorporate a language to express high-level business goals.	
ID	**Name**
Req_F_7.5	H2N interface
UMF must incorporate a H2N graphical interface to insert high level business goals	
ID	**Name**
Req_F_7.6	Business goals translation
UMF must provide mechanisms for the translation of high level goals to specific policies of network entities	
ID	**Name**
Req_F_7.7	Policy language
UMF must incorporate a policy language to provide information and allow communication between the autonomic entities	
ID	**Name**
Req_F_7.8	Interfaces for policy management
UMF must define interfaces between governance tools and autonomic entities, to allow the insertion, modification, and dissemination of policies.	
ID	**Name**
Req_F_7.9	Policy conflict resolution
UMF should provide mechanisms for policy conflict resolution	
ID	**Name**
Req_F_7.10	Policy dissemination
UMF must provide mechanisms for the dissemination of policies to the network elements	
ID	**Name**
Req_F_7.11	Network context monitoring
UMF must provide mechanisms for the individual autonomic nodes to monitor their operational status (QoS parameters should include BER, Jitter, Access Delay, Throughput, Delay)	
ID	**Name**
Req_F_7.12	Self-diagnosis
UMF must provide mechanisms for the individual autonomic nodes to self-diagnose themselves based on their current operational status.	
ID	**Name**
Req_F_7.13	Self-healing
UMF must provide the individual autonomic nodes with self-healing capabilities	
ID	**Name**
Req_F_7.14	QoS calculation
UMF must provide mechanisms for deriving the QoS based on the monitoring data collected from the autonomic elements	
ID	**Name**
Req_F_7.15	Behaviour assessment
UMF must provide feedback mechanisms to assess that the behaviour of the running autonomic entities is the one that correspond to the high level goals set by the human operator	
ID	**Name**
Req_F_7.16	Self-optimization/ adjustment
UMF should provide mechanisms for handling network performance degradation. For example: Incorporation of scheduling actions and mechanisms for policy-based self-optimisation/adjustment of resources to handle the network performance degradation, or suboptimal allocation of network resources to different nodes (e.g. selfish nodes).	
ID	**Name**
Req_F_7.17	Context discovery
UMF must provide mechanisms/algorithms for the network elements to self-discover their neighbours, using network protocols.	
ID	**Name**
Req_F_7.18	Policy-based trust management mechanisms
UMF must incorporate trust management schemes for detection of faulty/malicious behaviours of network elements based on operator policies.	
ID	**Name**
Req_F_7.19	Network to human notifications
UMF must define interfaces between autonomic entities and governance tools to allow the communication of collected monitoring, information, notification of results of diagnosis processes, notification of self-healing actions, notification of alarms	
ID	**Name**

Req_F_7.20	Information retrieval
UMF must define interfaces between governance tools and autonomic entities to allow the query of: current status of network elements, configuration information, historical monitoring information, historical diagnosis results, historical self-healing actions, historical notifications	
ID	**Name**
Req_F_7.21	Real time monitoring
Real time monitoring data and status of the network elements SHOULD be made available to the operator on the fly.	

6 Non - Functional Requirements

This section describes the use case non-functional requirements, as derived from the analysis of the UniverSelf use cases. Such requirements highlight the expected performances, properties or behaviours the UMF and Network Empowerment solutions shall exhibit when solving the that specific technical problems.

Table 16 - Use case 1 non-functional requirements

ID	Name
Req_NF_1.1	Adaptability to Operators topology changes
UMF must take into account the topology change and /or the configuration change and should be adjustable to the adding or deleting of a component.	
ID	**Name**
Req_NF_1.2	Adaptability to end to end management (Horizontal and vertical)
UMF must be applied for cross-layer and end to end perspective, both media and signalling, facing multiple network domains and technologies.	
ID	**Name**
Req_NF_1.3	Adaptability to operator organization
UMF must respect present operator's tools, processes and human organization and ensure its evolution.	
ID	**Name**
Req_NF_1.4	Reflexivity
Management Framework should support reflexivity. i.e., Management Framework should expose information regarding managed network and service infrastructures at an abstract level (information related to the identification of the network and service resources, connections, dependencies between services and needed resources for use or QoS)...	
ID	**Name**
Req_NF_1.5	Real time data acquisition
UMF must acquire real time data on-the-fly from the monitored network	
ID	**Name**
Req_NF_1.6	Event prediction algorithms Adaptability
UMF must allow algorithm Adaptability to face network/context constraints.	
ID	**Name**
Req_NF_1.7	Event prediction algorithms Robustness
UMF should allow algorithm Robustness to face: Missing data in monitoring processes, Time fluctuations in monitored data analysis.	
ID	**Name**
Req_NF_1.8	Event prediction algorithms scalability
UMF must allow algorithm scalability to face: multiple prediction time scale, Network/Context data amount, complexity, and changes, Topology changes, Organization structure evolution.	

Table 17 - Use case 2 non-functional requirements

ID	Name
Req_NF_2.1	Network Stability visual representation
UMF shall should be able to provide a visual representation of the network stability (e.g. with different levels of details) which is easy to be read and understood.	
ID	**Name**
Req_NF_2.2	Performance in self-stabilization
UMF shall actuate self-stabilization actions within a time scale to avoid that instabilities jeopardize network performance.	
ID	**Name**
Req_NF_2.3	Interoperability with legacy network management systems
UMF shall be compatible with legacy network management systems during Operations and Planning.	
ID	**Name**
Req_NF_2.4	UMF supportability
UMF shall be easily updated to accommodate/adapt usage in diverse network and service scenarios (for instance, it should be easy to add new self-* features in the framework for improving stability).	

<table>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_2.5</td><td>Security of network and services stability control</td></tr>
<tr><td colspan="2">UMF shall have the ability to prevent and/or forbid access to a system by unauthorized parties.</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_2.6</td><td>Resilience of network and services stability control</td></tr>
<tr><td colspan="2">UMF shall be redundant so to provide and maintain an acceptable level of stability control in face of faults and challenges to normal operations.</td></tr>
</table>

Table 18 - Use case 3 non-functional requirements

<table>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_3.1</td><td>Stability of network planning and configuration</td></tr>
<tr><td colspan="2">The UMF shall ensure uniformity and stability across network segments in terms of high level network planning and configuration.</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_3.2</td><td>Migration Management</td></tr>
<tr><td colspan="2">The UMF shall ensure that migrations (e.g., of servers, functions, services, content etc) are stable and optimised in terms of configurable policies</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_3.3</td><td>Network Survivability</td></tr>
<tr><td colspan="2">The UMF should ensure support survivability and maintenance of necessary resources during active sessions against any adverse situation e.g., by providing redundancy and/or failure recovery mechanisms.</td></tr>
</table>

Table 19 - Use case 4 non-functional requirements

<table>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_4.1</td><td>Scalability of Self-X</td></tr>
<tr><td colspan="2">Self-X functions shall be scalable to allow good operation in large number of network nodes (e.g. self-optimization functions in eNodeBs of a LTE network, including adjacent nodes)</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_4.2</td><td>Robustness of Self-X</td></tr>
<tr><td colspan="2">Self-X functions shall be robust: QoS/performance deterioration shall be limited to a pre-defined threshold in any self-X process</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_4.3</td><td>Time scales</td></tr>
<tr><td colspan="2">Time scales of Self-X functions for converging to a new stable state should be known to allow coordination of running Self-X processes</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_4.4</td><td>Convergence time</td></tr>
<tr><td colspan="2">Convergence time of SON mechanisms to reach a desired stable state (individually or jointly –in case of SON coordination) should be minimal</td></tr>
</table>

Table 20 - Use case 5 non-functional requirements

<table>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_5.1</td><td>Scalability to network size</td></tr>
<tr><td colspan="2">The methods provided by UMF must be scalable to network traffic with > 100000 hosts (IP addresses)</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_5.2</td><td>Scalability to network traffic</td></tr>
<tr><td colspan="2">The methods provided by UMF must be scalable to network traffic with gigabit per second bandwidth</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_5.3</td><td>Robustness towards short-term traffic fluctuations</td></tr>
<tr><td colspan="2">The methods provided by UMF must be robust towards short-term traffic fluctuations (short-term increases of bandwidth)</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_5.4</td><td>Time scale of traffic monitoring</td></tr>
<tr><td colspan="2">UMF methods for data monitoring should allow monitoring on a time scale of around 5 minutes.</td></tr>
<tr><th>ID</th><th>Name</th></tr>
<tr><td>Req_NF_5.5</td><td>Time scale of network configuration computation</td></tr>
<tr><td colspan="2">UMF methods for the computation of new network configuration should have an expected run time in the order of seconds.</td></tr>
</table>

ID	Name
Req_NF_5.6	Performance of MPLS routing optimization
UMF methods should enable MPLS routing optimization to increase overall system performance in terms of link utilization and convergence to the optimal solution	

Table 21 - Use case 6 non-functional requirements

ID	Name
Req_NF_6.1	H2N GUI friendliness
The H2N GUI should be human friendly for facilitating the expression of the requests and goals	
ID	**Name**
Req_NF_6.2	Optimized performance of load allocation to ingress/egress nodes
UMF should enable optimized load allocation to ingress/egress nodes	
ID	**Name**
Req_NF_6.3	Accuracy of load allocation to ingress/egress nodes
UMF should ensure that the proposed mechanisms for routing optimization/load allocation to ingress/egress nodes converges to optimal solution	

Table 22 - Use case 7 non-functional requirements

ID	Name
Req_NF_7.1	Governance Tool Usability
The system through the H2N interface should allow network operators to operate networks with a reduced human effort, without requiring specialized knowledge of the network behaviour and with reduced configuration errors.	
ID	**Name**
Req_NF_7.2	Success of high level goals
The system should enable H2N GUI to improve the success of high level goals through fine tuning based on feedback mechanisms which monitoring the underlying networks.	
ID	**Name**
Req_NF_7.3	Adaptability
Self-Diagnosis and self-healing processes should be dynamic and adjustable, following changes in the network context.	
ID	**Name**
Req_NF_7.4	Performance of Trust management
The application of trusted network behaviour should not have an important impact in the performance of the system.	

7 Design information gained from requirements definition

7.1 Synthesis: the global picture

As mentioned in section 3, in the context of the task 4.1 activities, the use cases definition started from the three reference scenarios identified during the proposal preparation, which are reflecting the stakeholders needs and requests for networks and service in the short-medium and long terms. As such, the overall approach adopted aims at defining the functions or features satisfying these needs and requests through a detailed description of use cases with the related business implications.

The seven use cases are descriptors of a set of precise problems to be solved by the UMF and the Network Empowerment mechanisms. The related functional and non-functional requirements have been derived and developed: this problem-oriented approach meets very well the current issues network operators are facing in their deployed infrastructures, and at the same time outlines the research directions set for future networks, service-oriented computing and networking, and the Future Internet themes.

This section is presenting a synthesis of the information gained from the use case problems analysis and requirements definition whilst pursuing a bottom-up engineering process of requirements (which will be completed in deliverable D4.2).

The emerging global picture is characterized by a list of "condensed" technical issues[1] which are potentially impacting existing and future networks and services domains; the list includes:

- **Optimisation of resources** – there are the issues concerning optimizing on demand allocation, insulation, sharing and use of (real and virtual) partitions of infrastructure resources (communication, storage, processing, control) with consideration to various physical resource limitations and assurances in multi-technology / multi-layer networks as well as in a wide variety of ICT networked services. Mechanisms and APIs are required for the use and change/configuration of infrastructure resources.
- **Improving effectiveness of management** - there are the issues of enabling self-management functions and their integration (i.e. self-discovery, self-diagnosis, end-to-end self-monitoring, self-configuration, self-optimization, self-organization, self-healing, self-protection, self-awareness, self-governance, self- testing, self-control, self-adaptation) improving effectiveness of main areas of management (such as fault, configuration, performance and security) through exploitation of a "cross-layer knowledge and context"; this knowledge can be extracted from network, user and service data (both numeric and semantic);
- **Integrated use of context and knowledge** - there is the issue of bringing together (for system use) widely distributed data/context/knowledge/information entities (sources and clients) for collection, filtering, adaptation, storage, optimisation, as well as management of knowledge and context quality and distribution; optimal and efficient handling and retrieving of huge amounts of data and information regardless of their location in the networks and/or services;
- **Control and orchestration** - there is the issue of controlling and coordinating autonomic, self-* functions (e.g. closed control-loops) to assure stability, convergence and performance;
- **Validating and assessing stability** - there are the two issues of: 1) making offline validation of self-* features (before the real deployment) and 2) assessing online network and service stability in order to allow, in case of instabilities, human deactivation of self-* features;
- **Service self-manageability across lifecycle** - there is the issue of accommodating seamless manageability (i.e. self-deployment, self-monitoring, execution, assurance, QoS, SLAs, self-optimisation and triggers, rooming, accounting, agile deployment of new services etc) of ICT networked services without drastic increases in deployment and operational costs as the number, range and qualities of services is expected to explode in the future creating the opportunity for new revenue streams for infrastructure operators;

[1] The term condensed issue refers to an issue, which is common in different use-cases, and as such it shows different facets being covered by the different use-cases.

- **Governance** - there is the issue of improving network and service governance, through high-level means, goals and objectives; governing by means of high level policies triggering monitored and coordinated self-organizing networks functionalities, and resolving possible incompatibilities with backhaul/core segments;
- **Network empowerment** - there is the issue how to embed intelligence into the systems and network equipments that constitute the infrastructure and support service delivery;
- **Improving networks/services flexibility and elasticity** - there is the issue of how to extend and enable extensibility in order to add or change functionality without affecting the integrity and stability of the full system through Plug_and_Play / Unplug_and_Play/ dynamic programmability approaches;
- **Global integration** - there is the issue of enabling systemic integration of all functionality (i.e. integration and interworking of all self-x functions, coordination and interworking of all closed control loops in the managed systems, integration and interworking of heterogeneous managed objects) and a uniform set of interworking interfaces between management functions that permits introduction and migration of new functions, and between management functions and control functions;
- **Environment bearing** - there is the issue of enabling a number of environmentally friendly designs aimed to minimize UMF operations' environmental impact;
- **Migration and interworking with legacy** - there is the issue of defining migration paths to support the progressive introduction of autonomic and new management and control features in the existing legacy of management and managed systems.

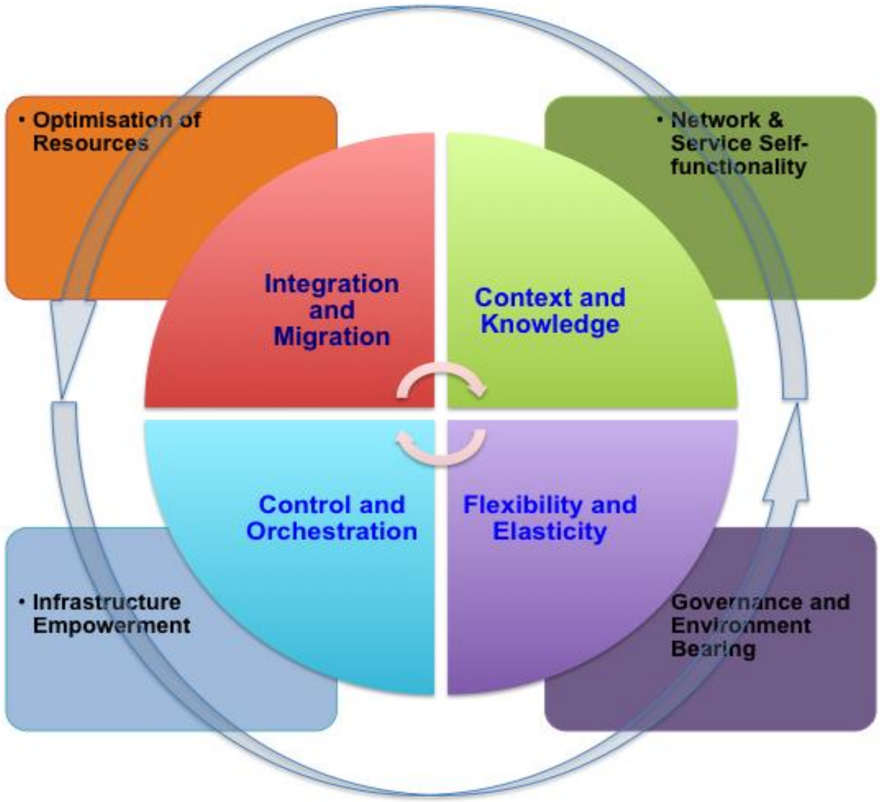

Figure 3 - Synthesis of use case problems analysis and requirements derivation

These "condensed" issues are showing interesting inter-relations between them. This is leading to a systemic perspective of what features are mainly expected to be achieved by UMF and Network Empowerment, as from the use case perspective. For instance:

- end-to-end self-monitoring features of real and virtual managed entities;

- self-monitoring (on-line) features of network and services in order to assess network stability;
- self-configuration features, e.g. SON capabilities, or control-loops capable of actuating control changes in real and virtual entities;
- self-optimization features, methods for optimizing allocation and use of (real and virtual) network resources (communication, storage, processing) in multi-technology / multi-layer networks;
- capabilities for off-line validation of self-configuration and self-optimization features;
- self-discovery features;
- self-diagnosis features;
- capabilities for orchestrating self-* features;
- etc.

This list provides just a sketch of the UMF and Network Empowerment features from a use cases perspective, which is merely intended to convey an intuitive understanding; as such this overview is not intended to provide formal sophistication and details of their successful application in the UMF design and demonstration. On the other hand the picture is leveraging the lessons learnt from the use case development.

At the end of the day, UMF and Network Empowerment requirements will describe the functionality needed to meet stakeholder's requests or user needs (a.k.a. "user requirements"). In this sense the totality of the use cases requirements and of the top-down requirements will identify the necessary attribute, capability, characteristic, and quality of the UMF and Network Empowerment solutions. The requirements together as a set, blending of the top-down and bottom-up processes, will provide (also through the next releases of deliverables D4.1 and D2.1) what distinguishes UniverSelf from earlier network and service management technologies and what the UniverSelf project intends to design and deliver.

7.2 Exploitation in the project

The Description of Work has already described the process of the exploitation in the project of the information gained from the use cases definition and requirements derivation. Specifically, this information has been (is being continuously) transferred to WP2 and WP3 in charge, respectively, of the design of UMF and Network Empowerment. This section is reporting some consideration and examples how this transfer has taken/is taking place. For example there is a clear link between the UC requirements reported in deliverable D4.1 and how they transform, in D2.1, into bottom-up design blocks (UMF), and further the mapping back to the UC view.

At the same time, each use case being a specific, real-life problem, WP3 has been the first recipient of all use cases problems, with the goal of contributing to meeting them with appropriate algorithms/methods/mechanisms.

7.2.1 WP2 perspective

This deliverable provides a synthesis of the functional, non-functional and business requirements derived from the selected use cases that were defined and developed so far within WP4.

One of the goals of WP2 is to address those requirements by carefully analysing them so as to identify a first functional view (functional components) of the UMF. At the end of this process, there is a list of functional components, i.e. functions and models per use case corresponding to those requirements. In the next step, the functional components (from all use cases) that exhibit similar a purpose/goal and/or similar inputs and outputs or operation are developed and they are grouped into a set of functional blocks. The functional blocks are accordingly conceptual entities that group functional components with commonalities and irrespectively of the use case to which they belong. Thus, a functional block can serve many use cases, achieving a first level of integration and unification (as in ***Unified*** Management Framework).

In addition to these requirements, the top level requirements identified as part of the top-down approach and reported in deliverable D2.1, need also to be taken into account in the UMF design. Some of them are already captured by the functional blocks of the bottom-up approach. Some others that may not be explicitly covered by the existing functional blocks are used to amend and enhance the bottom-up based design so as to provide a more complete UMF design that will fulfil all the objectives of UniverSelf towards the autonomic management and control of legacy and future networks. Finally, the functional blocks are aggregated into functional groups, in consistency with the bottom-up approach but also in a way that satisfies the top-level requirements. Each functional group realizes higher level management and control functionality.

After the derivation of functional blocks and functional groups, a mapping to the network elements takes place so as to start delineating a system view of the UMF design. The network topology targeted in each use case has been used. This mapping constitutes a first step forward for the identification of the needed interfaces and content exchanges in the network layout. Therefore, at this point, there is a return in use case requirements to identify interfaces, messages and parameters but also to verify the result on a use case level. The mapping can be done in terms of either functional blocks or high level functional groups depending on the level of detail that is required. If a detailed description is needed, the functional blocks are also depicted inside the functional groups, in order to show the interactions between functional blocks that are mapped into the same network element and belong to the same functional group. Having mapped the functional blocks and/or groups to the network topology and using the way that they interact (which block/group sends information to which and where do the inputs of the block/group originate from, i.e. inputs and outputs) are sufficient for the identification of the first interfaces and content exchanges between the elements. At this stage, an implicit verification is done on a use case level, since it is more easy to identify if a missing requirement exists which leads to missing functional component, input and output.

Since the intention is the UMF design, and use cases have only an assistant role to identify through the requirements all these functional components, an aggregation per network segment, namely wireless access, wireline access, backhaul/core, Network Management System (NMS)/ Operational Support System (OSS), service and future networks, takes place. The aim is to exploit functional blocks and functional groups for identifying common interfaces and content exchanges per segment.

Other business and non-functional requirements are used to judge the UMF in terms of usability by network operators, feasibility by the solution providers and extensibility for tackling new scenarios. In addition, they will also have a certain impact on the system view of UMF e.g. by driving decisions with respect to the level of distribution of specified functions among the management systems or network elements, which in essence may result in different levels of performance.

7.2.2 WP3 perspective

The following table illustrates the interaction between WP4 and WP3 (Network Empowerment). The left column reflects the problems derived from the use cases whereas the right column indicates what task force in WP3 will address the tools, techniques and algorithms related to the UCs' problems.[2]

Currently, the names of the task forces in WP3 are:

- TF3.2.A: SON Interaction
- TF3.2.B: Random elements
- TF3.2.C: Governance
- TF3.2.D: Load balancing
- TF3.3.A: Patterns in operators' data
- TF3.3.B: Context
- TF3.3.D: Anomalies
- TF3.3.E: Learning
- TF3.4.A: Trust in SON
- TF3.4.C: Distributed traffic engineering
- TF3.4.D: Closed loop interaction

In principle, all problems are addressed at the methodology level with the exception of Problem UC6-1 (use case 6-1). In this particular case, the problem describes actions that must be performed off-line using some tools and databases that are outside of the network. The problem is thus not part of Network Empowerment.

[2] The task force organization is informal and dynamic and may continue to evolve in the course of the project. This is also the reason why some consecutive task force numbers are missing here.

Table 23 – Problem-Task force mapping

Use Case	UC problems domain	Task Forces in charge of the tools, techniques and algorithms related to the UCs' of the problem
UC1 - Self-diagnosis and self-healing for IMS VoIP and VPN Services	Problem UC1-1: To develop algorithms and models to support reusable end to end cross-layer and local self-diagnosis related to networks and services. They should be able to provide macro/micro granularity for the end to end view and for local view or subscriber's view. Self-modelling will be investigated to create models related to managed objects topology (and interaction) and related behaviours, associated with correlation algorithms. Defined models and methodology should be compatible with other management functions (e.g. configuration).	TF3.3.A is in charge of pattern based diagnosis. Data modelling will define reusable event patterns, for micro or macro events. Event/parameter correlation algorithms are the key of such a process. TF3.3.E is in charge of the identification of learning techniques related to fuzzy logic and reinforcement learning and the extraction of event identification schemes.
	Problem UC1-2: Enabling end to end and local self-Proactive and reactive diagnosis, including the detection, estimation of possible anomalies/issues/problems before occurring (proactive), known and occurring anomalies (reactive) or unknown anomalies. It also includes the analysis and qualification of incidents and related causes. Knowledge must be built from service and network data, alarms and events	TF3.3.A is in charge of pattern based diagnosis. From well known problems, recurrent or not, it sets up a pattern and a detection algorithm to diagnose them. TF3.3.B is in charge of 1) Diagnosing proactively and predicting network faults or congestion on the one hand, while also context (anomalies, faults, loss or lack of resources) on the other hand. 2) Diagnosing malfunctions of network elements and service weaknesses. 3) Employing a) algorithms needed for data mining and knowledge extraction, b) methods for processing monitored data and generating Context. TF3.3.D is in charge of detecting anomalies and vulnerabilities in an integrated manner. This detection is based on both internal knowledge and external knowledge. TF3.3.E is in charge of the identification of learning techniques related to fuzzy logic and reinforcement learning. Mechanisms for reactive diagnosis based on network key performance indicators will be proposed. Evolution of the self diagnosis mechanisms based on the network's performance.
	Problem UC1-3: Based on diagnosis and defined mitigation & reparation plans, self-healing is enabled by applying the correct mitigation or reparation plan based on business goals	TF3.3.D is in charge of preventing anomalies/vulnerabilities in VoIP infrastructures by selecting/executing suitable corrective configuration operations.

	Problem UC1-4: Self-Diagnosis/healing functions should be triggered by network/service events but also by subscriber events (in the case of a subscriber signalling). Validation by human operators of diagnosis should be possible, reporting of mitigating/reparation actions should be done. Link with configuration processes is tight.	It is one of the targets of TF3.3.B to develop active self-diagnosis algorithms for both network and IMS services running on top of them. Here the notion of "context" is understood as the physical and functional architecture of the system to supervise. This comprises the network topology (access and aggregation segments, and core network), the functional architecture deployed over them (subsystems and their functions), plus the parameterization of these elements. In TF3.3.B it is planned to address the diagnosis problem as requests sent to a generic context model in order to explain a given observed symptom or alarm (e.g. no ability to make calls for a given user). This comprises the automatic instantiation of the part of the model that is necessary to answer this query (i.e. determining the necessary context for the problematic user), and the associated collection of observations. This process will probably be iterative: explore/build the context, draw a set of possible explanations, then refine the context (possibly instantiating extra elements of model) to discard some explanations and refine others, etc.
UC2 - Network Stability and Performance	Problem UC2-1: To develop (leveraging prior-art) continuous and/or discrete models and related open source tool-boxes for simulations and emulations of stability and performance of networks with (large) number of nodes embedding self-configuration mechanisms/control-loops. Modelling includes network segments, nodes, control-loops rules and mechanisms (e.g. monitoring/actuation), etc. and their interactions in wide areas.	TF3.3.E is in charge of distributed node level decision making mechanisms based on Fuzzy-logic and Reinforcement learning techniques in a large scale network. TF3.3.F is in charge of defining continuous and/or discrete models and open source tool-boxes for systems, nodes, networks and processes. This task force will also develop a handbook on said modelling, methodologies, open source tool-boxes (with related recommendations for future reuse and extensions) and will define concepts, metrics and ways to estimate “network stability”.
	Problem UC2-2: To make simulations and emulations about stability and performance of networks in presence of various potential roots causes of instability (as identified in this and other UCs, if requested)	TF3.3.E is in charge of the identification of learning techniques related to fuzzy logic and reinforcement learning. The relations between instability and the learning schemes need to be identified; the metrics shall be extracted, as well as the corresponding remedy actions. TF3.3.E will support Task 4.2 in making simulations/emulations of a large scale network with self-* mechanisms and/or optimization algorithms
	Problem UC2-3: To define the necessary and sufficient level of “cross-layer knowledge of the network” to be monitored and controlled (e.g. order and control parameters) to predict behaviour and assure network stability and performance	TF3.3.F will define concepts, and models correlating “network stability” with “cross-layer knowledge of the network” (e.g. rippling effects). TF3.3.B employs 1) methods for generating context, and adding this to the simulation/ emulation model and 2) learning mechanisms for predicting the traffic of the network after a (re-)configuration, and for predicting the stability of the network based on data that have derived from simulations/

		emulations.
	Problem UC2-4: To define the most effective and low-cost network decision logic distribution to assure network stability and performance.	TF3.3.F will define concepts, and models correlating "network stability" with "network decision logic". TF3.4.C will develop decentralized mechanisms that realize in-network self-configuration to guarantee network performance through dynamic resource management based on the run-time state of the network. TF3.4D will develop techniques that allow the co-existence and inter-operation of multiple control loops. Coordination mechanisms will harmonize distributed decision making and will guarantee network stability.
UC3 - Dynamic Virtualization and Migration of Contents and Servers	Problem UC3-1: To develop strategies that would reduce the load (traffic, processing, signalling etc.) on the core network segments and data centres for efficient delivery of data/service/application to the mobile user. This would be achieved by decentralizing and migrating frequently used/critical resources/functions/services from the core/data centres towards the access and backhaul network nearer to the user. This issue will be studied and analysed with respect to the best practice solutions of network virtualization techniques for enabling dynamic migration of functions and resources.	TF3.2.D: Load balancing will develop algorithms for resource optimization (i.e. load balancing) for both service and network levels. TF3.4.C will develop co-operation strategies when (different) load balancing algorithms are used simultaneously for service and network resources
	Problem UC3-2: Specifying the resources and functions used (or required) by a mobile user (with varied mobility patterns) for accessing commonly used network services and applications (real time and non-real-time) in the context of 3GPP network architectures. Specifying the KPI for each of these services and applications and defining network/configuration/performance parameters for the commonly used services. Identifying the functional and operational enhancements of existing segments at the access/backhaul for supporting and hosting the migrated resources/functions/services).	TF3.3.B will develop 1) movement detection, 2) auto discovery and selection of best network(s) and service(s), 3) proper knowledge building schemes enabling the optimization of the event identification and decision making mechanisms, 4) filters for extracting the relevant data, 5) Interfaces for inserting the data in the knowledge mechanisms, 6) builders of knowledge about traffic demand according to user and service data, 7) interfaces for communicating the acquired knowledge to the decision making mechanisms
	Problem UC3-3: Develop algorithms that would leverage the virtualization techniques and cloud concepts for seamless migration of resources/services/functions context. Develop novel techniques and algorithms for enabling the seamless mobility of resources/services/functions virtual clouds in sync with the user mobility.	TF3.2.D will develop algorithms for service/resource adaptation and migration. TF3.4.C will develop a framework needed to support distributed load balancing algorithms using information from and acting in different layers (network nodes, services).

	Problem UC3-4: Develop simulation models to understand the implication of decentralizing the resources/functions/services from the core and migrating them towards the access and backhaul segments and their impact on the network architecture and the corresponding network entities.	TF3.2.D will develop simulation models to evaluate the adaption/migration algorithms. TF3.3.F is in charge of defining continuous and/or discrete models and open source tool-boxes for systems, nodes, networks and processes. It will also develop a handbook on said modelling, methodologies, open source tool-boxes (with related recommendations for future reuse and extensions).
UC4 - SON and SON Collaboration according to Operator Policies	Problem UC4-1: Design of distinct SON functionalities in network nodes to efficiently self-configure and self-optimize network resources. The SON functionalities at a given node (e.g. base station) should allow self-adapting to varying operation conditions, in the presence of other self-organizing neighbouring nodes, to assure stability and scalability.	TF3.2.B will develop SON algorithms that adapt wireless network parameters in response to changing traffic and environment conditions. TF3.2.D will design algorithms dealing with: a) the efficient learning-based mechanisms for resource management of control plane data and optimization of load balancing requests, b) AP Dynamic Activation/De-activation mechanisms for the assessment of network capacity and APs overlapping coefficient on a specific geographical area. TF3.3.E is in charge of the identification of learning techniques related to fuzzy logic and reinforcement learning. Develop efficient learning techniques for SON mechanisms encompassing self optimization and self-healing. Both distributed (scalable) and robust solutions are targeted. Robust solutions allow minimizing performance and QoS degradation and instabilities in the learning phase. TF3.3.F will define concepts, metrics and ways to estimate "network stability".
	Problem UC4-2: Design of different SON functionalities operating simultaneously to achieve one or several performance objectives. The solutions should guarantee coordinated operation of the SON functionalities, while avoiding or solving conflicts between conflicting objectives.	TF3.2.A addresses the smooth interaction of SON use cases such that they can operate simultaneously while avoiding conflicts. TF3.2.B. will develop techniques that optimize radio network configurations that try to balance different conflicting objectives in small cell/femtocell coverage problems. TF3.4.D will develop a management framework that allows the coordinated operation of the SON entities, by means of orchestration of multiple control loops but also policies (e.g. hierarchy) in order to resolve conflicts, instabilities, etc. according to operator goals
	Problem UC4-3: Govern radio access networks by means of high level policies triggering coordinated SON functionalities. Definition of objectives and rules in the different network levels from the OAM till the SON algorithms embedded in the radio access nodes. Monitor the full SON processes to provide assurance.	TF3.2.B will provide feedback on the low-level objectives and provide guidance on how these link to high-level policies. TF3.2.D will work on policy-based scheduling techniques for the application of load balancing mechanisms complementing problem UC4-1. TF3.4A will develop a network governance framework, that using semantic technologies, allows the translation of high-level goals to policies that could

		be applied on the network elements.
UC5 - Network Morphing	Problem UC5-1: To adapt traffic routing configuration of the network consequently to monitored traffic evolutions in order to ensure a low cost of the traffic routing configuration	TF3.3.B develops 1) the mechanism for incorporating the service level agreements (SLA) and user information in the packet without human intervention, 2) the mechanism for monitoring SLA compliance. The target data rates, which these mechanisms have to be able to process, can be derived after the corresponding SLA parameters identification from T4.1 (in "Collecting new SLA inputs" phase), 3) mechanism for Building SLA knowledge (online and/or offline functionality), 4) mechanism for transforming information related to SLA compliance per link to SLA compliance per route.
	Problem UC5-2: To enrich traffic variations with self-built knowledge of probabilistic traffic trends -> Pro-activity in routing adaptation to traffic. Traffic can be either monitorable IP traffic or sets of services demands	TF 3.3.E: identification of learning techniques related to fuzzy logic and reinforcement learning. Optimization and learning algorithms are related to the improvement performance of control loops (controlling radio resource management (RRM) functions in the network) on the one hand, and to achieving high performance SON functionalities on the other.
UC6 - Operator-governed, End-to-end Autonomic joint Network and Service Management	Problem UC6-1: To enable operators to describe their goals and objectives in high-level terms (H2N interface). To derive policies according to the higher level goals, to provide constraints and priorities. The assess the derived policies against existing goals/policies so as to identify and resolve conflicts (in fact, conflicts can arise if the defined goal/objective/policy are antagonist with respect to previous goals or the impact of these goals on already deployed services)	*(not treated as part of the WP3 task forces)*
	Problem UC6-2: Analysing the business request to elaborate the inputs/requirements derived from the business entry and to correlate them together with pertinent knowledge stemming from user & service raw data so as to derive technology specific (network-specific) requirements.	TF3.3.B and TF3.3.A can contribute to extract useful knowledge and feed knowledge-bases with respect to users and services, thus assisting in providing faster decisions.
	Problem UC6-3: Determination of candidate solutions to determine (reason with) the candidate solutions (networks) that can satisfy the derived network requirements. The candidate technologies and networks, which can contribute to this satisfaction need to be, discovered also taking into account existing knowledge that was extracted from raw network data to knowledge.	TF3.3.B and TF3.3.A can contribute to extract useful knowledge and feed knowledge-bases with respect to networks, thus assisting in providing faster decisions.

	Problem UC6-4: To invoke the selected RANs and request for an offer in terms of the quality which the RAN can provide. Then, RAN investigates way to accommodate the request (anticipated load). In OFDMA-based (LTE) case this may result in problems related to radio resource allocation, Admission/Congestion control and scheduling, relay selection in case of multi-hop networks, link positioning, compensation by means of SON mechanisms etc.	TF3.2.C is in charge of the autonomic management of OFDM-based segments - Access network parameter optimization based on operator policies - Stochastic optimization methods/algorithms and meta-heuristics (simulated annealing, genetic algorithms, swarm intelligence and other bio inspired like ant-colony optimization) - Game theoretic approaches - Application to OFDM(A) resource allocation, relay link positioning in multi-hop cellular OFDM networks
		TF3.2.B studies genetic-based methods/algorithms to solve the autonomic, policy-based optimization of OFDM(A)-based segments. Research findings from T3.2.B can be used to guide these methods/algorithms. TF3.3.B will define a model for data collection and elaborate to organize the incremental knowledge derived from terminal and radio access network node measurements to give proper diagnosis and prediction mechanisms to be used in TF3.2.C for QoS related RAN government.
	Problem UC6-5: Invocation of backhaul/core segment * /The backhaul/core segment is triggered and the problem aims at finding the best configuration and accordingly offer of quality, so as to support the solution (offer) provided previously by RAN. The backhaul/core investigates way to accommodate the request. At the backhaul side, this may involve LSP configuration in IP/MPLS case. At the core side, it also involves GW (e.g., SGW, PDN-GW) (re)selection/configuration, GW migration/dimensioning.	TF3.2.C is in charge of the autonomic management of MPLS-based segments - Route optimization & Ingress/Egress node selection based on operator policies - MPLS parameter optimisation: Load aware and optimal routing algorithms & protocols/Maximum-flow/Graph-theory - Policy-based, green traffic engineering - Bio-inspired approaches
		TF3.2.D will have load balancing as one of the main objectives for the case of autonomic management of MPLS-based segments (e.g. allocation of radio access network nodes to ingress nodes/ingress nodes to egress nodes (gateway) etc.). Research findings within T3.2.D can be used to guide these methods/algorithms.
	Problem UC6-6: The problem here is to resolve possible incompatibilities between the offered QoS from RANs and backhaul/core segments, respectively. For that reason, some sort of negotiation and cooperation between segments is needed that will be used to fine-tune the resulting offers from the underlying segments, in order to achieve coherence.	TF3.4.C will develop a collaborative vertical traffic engineering framework between core network segments and overlaying specialized service/content networks. This task force will also cover protocols and strategies for negotiation and cooperation between the OFDM(A)-based RAN and the MPLS-based backhaul/core segments, respectively. A cooperation framework between OFDMA access network and MPLS core segments running individual traffic engineering optimizations will be designed.

	Problem UC6-8: To ensure the designated QoS levels by means of corrective actions and by issuing alarms and warnings to the upper layers in case these corrective actions cannot remedy the problematic situation.	TF3.2.D will develop admission control functions as means of corrective actions to ensure the designated QoS levels. The functions will be fuzzy logic and reinforcement learning based and the specific related implementation issues will be addressed in TF3.3.E. TF 3.3.E: identification of learning techniques related to fuzzy logic and reinforcement learning. Application of respective solutions to improve the robustness and performance of flow-based resource management mechanisms.
UC7 - Network and Services Governance	Problem UC7-1: To enable operators to describe their goals and objectives, through high-level means and govern their network. Derivation of network policies from the business goals through the use of semantic techniques.	TF3.4.A deals with the development of a network governance framework, that using semantic technologies, allows the translation of high-level (business) goals to policies that could be applied on the network elements.
	Problem UC7-2: Evaluation of the network governance tool, in terms of examining whether the generated policy rules and the applied configuration actions meet the initial business requirements. This evaluation will be realized through a feedback loop procedure that will realize the following actions: a) evaluation of the applied configuration actions in the infrastructure part and generated policy rules and b) evaluation of the business requirements through examining how well the specific goal is met.	TF3.2.D will work on linking the network governance mechanisms and its resulting load-balancing actions (e.g. SON related configuration actions). TF3.4.A will do research on how, based on network monitoring data, trust can be established among network elements in order to ensure the reliability of information exchanged.
	Problem UC7-3: Implementation of algorithms so that the network elements in FTTH environments can self-discover their context, through the use of network protocols.	TF3.3.B is in charge of developing mechanisms for local context discovery, contributing then in the development of knowledge for increasing system efficiency.
	Problem UC7-4: Implementation of self-monitoring algorithms in network elements in FTTH environments.	TF3.3.B will develop mechanisms for context diagnosis which will contribute in decisions regarding self-configurations and self-healing and in self-awareness
	Problem UC7-5: Probabilistic self-Diagnosis functions should be implemented in the network elements, based on their own state and their operational context.	TF3.3B will develop mechanisms for context diagnosis based on Bayesian networks.
	Problem UC7-6: Decision making processed based on semantic models and inference engines must be supported for self-healing purposes.	TF3.2.D will work on linking the network governance mechanisms and its resulting self-healing actions related to load balancing (e.g. SON related configuration actions). TF3.3B covers the development of mechanisms that enable proactive diagnosis of congestion/ faults, taking as inputs the monitoring parameters, to be fed in the self-healing mechanisms

7.3 Exploitation towards standardization

The functional, non-functional and business requirements have been identified and listed in this document. Then, their subsequent analysis allowed gaining relevant design information to feed the project activities. Indeed, the primary purpose of the bottom-up analysis of use case requirements is to enrich the UMF design process and focus the technical reference problems to be addressed by the network empowerment taskforces.

Besides this, another important exploitation of the identified use case requirements is their use to feed the project standardization activities. The scope of this exploitation in standards, which concerns mainly the requirements and not the expected project results, is twofold: (1) driving the work of selected standardization groups with relevant requirements in order to strengthen the project impact; and (2) juxtaposing the project and external requirements for refinement purposes.

The first targeted group is the ETSI AFI which is an Industry Specification Group aiming to develop pre-standard specifications for Autonomic Network Engineering for the Self-Managing Future Internet [11]. The first work item (WI#1), currently active within this group, targets the description of scenarios, use cases, and definition of requirements for the Autonomic/Self-Managing Future Internet [7]. Scenarios and use cases are intended to reflect real-world problems, which can benefit from the application of Autonomic/Self-Management principles. This purpose is in line with the use case definition, requirement identification and analysis that have been achieved within UniverSelf and reported in this document. The current release of WI#1 provides a rather consolidated set of scenarios and requirements that have been identified by ETSI AFI stakeholders; it covers auto-configuration, fault management, monitoring, coordination of multiple self-* mechanisms, among other functions, and it addresses legacy and emerging technologies. In this context, the plan for the exploitation of the use case requirements towards ETSI AFI consists in two steps that shall be taken:

- First, the requirements extracted from UniverSelf use cases will be juxtaposed and thoroughly compared with the current AFI list of requirements in order to refine the UniverSelf ones and identify gaps within AFI requirements.
- Then, based on this analysis, a contribution will be prepared and provided in order to enrich WI#1 and, by the same, to participate in driving the second AFI work item (WI#2 - Generic Autonomic Network Architecture), and the technology-specific work items (WI#3) on applicability of the generic architecture to specific environments.

Besides ETSI AFI, potential contributions towards other relevant standardization groups are currently investigated and discussed. These initiatives include:

- **LCCN BoF initiative at IRTF:** The Learning-Capable Communication Networks (LCCN) initiative aims to combine insights of several communication networking use cases involving application of various learning techniques [12] [13]. This scope is in line with numerous requirements, extracted from UniverSelf use cases that identify the need for learning capabilities within communication networks and express the expected behaviour of such capabilities.
- **NMRG Group at IRTF:** As stated in its charter, the Network Management Research Group (NMRG) provides a forum for researchers to explore new technologies for the management of the Internet [14]. Besides, NMRG has recently updated its charter, which offers an opportunity to influence shaping (self-) management solutions for future networks on topics such as safe configurations, stability or trust with appropriate problem statement and requirements drafts.
- **3GPP:** The requirements addressing novel SON functionalities, SON coordination and related policy management, which have been identified within UniverSelf use cases (e.g. mainly UC4), are in the scope of future 3GPP releases.
- **ITU-T FG FN**: The requirements addressing novel Future Networks functions and related management operations, which have been identified within UniverSelf use cases (e.g. mainly UC2 and UC3), are in the scope of future releases of FN recommendations.

8 Conclusion

Deliverable D4.1 provides the synthesis of the requirements collected via the use cases defined in the WP4 (Deployment and Impacts) of the UniverSelf project. According to the project lifecycle, the requirements have been transferred to WP2 to guide the design of the Unified Management Framework (UMF), to WP3 to guide the design of the methods and algorithms of the Network Empowerment solutions, and to other tasks of WP4 for the implementation and validation of the integrated solutions, the business impact analysis and the trust development and evaluation.

In the UniverSelf project, a use case is a descriptor of a (set of) precise problem(s) to be solved, in a given technological context.

Use cases definition started from the three reference scenarios identified during the project proposal preparation, i.e. Scenario 1 - Operators' Service and Data Management, Scenario 2 - SON for Radio Access and Core Networks, and Scenario 3 - Future Internet Services Management and Network Resource Optimization (see Annex A). These three reference scenarios reflect the network operators needs of reducing the total cost of ownership, exploiting new revenue streams and improving the return on investment for network equipment and infrastructures; furthermore many problems such as fault diagnosis, misconfigurations, performance degradation, etc. are still open problems and, will become even more pressing with the developing trends and scale of future networks. Seven use cases have been identified, whose descriptions are reported in corresponding white papers. The first series of use case white papers cover the use case story line, problem statement, modelling, and innovation parts of the use case template. The white papers are available on the project web page at the following link: http://www.univerself-project.eu/white-papers.

The use cases are:

1. Self-diagnosis and self-healing for IMS VoIP and VPN services
2. Network Stability and Performance
3. Dynamic Virtualization and Migration of Contents and Servers
4. SON and SON Collaboration according to Operator Policies
5. Network Morphing
6. Operator-governed, End-to-end, Autonomic, joint Network and Service Management
7. Network and Services Governance

At the 1st release of Deliverable D41 in the project, it appeared reasonable that UC#5 might be merged with another use case such as UC#3 or UC#6. After some investigations, the decision was made (at PMT17 meeting on 7/07/2011), in consensus of all partners involved and of the PMT members, to actually merge the content of UC#5 with UC#6. The numbering of the use case has not been changed to preserve consistency across the current and following documents. As a direct result of this decision, the project is now studying 6 use cases as initially planned.

Main achievements reported in this deliverable include:

- The telecommunication industry perspective, based on the views of the project industrial partners, in terms of what are the technical and business problems that the ICT industry is willing to solve thanks to the development and adoption of UMF and Network Empowerment technologies developed in the context of UniverSelf;
- A detailed list, an analysis and a synthesis of the functional, non-functional and business requirements of the seven use cases;
- Some considerations on how this process of use case requirements expression and analysis have been (and are being continuously) exploited within the project activities (e.g. with particular reference to the work package 2 and work package 3) and towards relevant standardization bodies, are also given.

There is a clear link between the UC requirements reported in this report .1 and how they transform (in D2.1) into bottom-up design blocks (UMF), and further the mapping back to the UC view. At the same time, each use case being a specific, real-life problem, WP3 has been the first recipient of all use cases problems, with the goal of addressing their algorithmic/methodological aspect.

Coherently with the requirements process shown in Figure 2, the next immediate step is to classify the requirements in order to align priorities for the UMF design (WP2) and the related technical development from algorithms (WP3) to experimentations (WP4). A requirement classification based on internal and external stakeholder's viewpoints will be conducted to trigger the priorities and related work planning.

References

[1] V. D. Blondel, A. Megretski (Eds), Unsolved Problems in Mathematical Systems and Control Theory, Princeton University Press, 2004

[2] Mendler, C., Evaluating the Benefits of Carrier Outsourcing, 2008, Yankee Group, http://www.scribd.com/doc/8572879/Evaluating-the-Benefits-of-Carrier-Outsourcing-2008-Yankee-Group.

[3] Daniels, J., Werner, P. W., and Bahill, A. T. (2001). Quantitative methods for tradeoff analyses. Syst. Eng. 4(3):190–212.

[4] Andrew P. Sage,William B. Rouse, Handbook of Systems Engineering and Management, Wiley Series (2009)

[5] Smith, E. D., Son, Y. J., Piattelli-Palmarini, M., and Bahill, A. T. (2007). Ameliorating mental mistakes in tradeoff studies. Syst. Eng. 10(3):222–240.

[6] Bahill, A. T. and Dean, F. F., Discovering system requirements, Chapter 4 in Handbook of Systems Engineering and Management, A. P. Sage and W. B. Rouse (Eds.), second edition, John Wiley & Sons, pp. 205-266, 2009.

[7] ETSI GS AFI 001 V1.1.1 (2011-06), Group Specification, Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet

[8] Writing Effective Use Cases, Alistair Cockburn, 2000, (ISBN 0-201-70225-8)

[9] IETF RFC2119 Key words for use in RFCs to Indicate Requirement Levels, http://tools.ietf.org/html/rfc2119

[10] ETSI drafting rules, Special Report, ETSI SR 001 262 V1.8.1 (2003-12) – in particular Section 23

[11] ETSI AFI Group, Website: http://portal.etsi.org/portal/server.pt/community/afi/344

[12] Learning Capable Communication Network (LCCN) problem statement, IRTF Internet-Draft, http://tools.ietf.org/html/draft-tavernier-irtf-lccn-problem-statement-01

[13] Learning-Capable Communication Networks Group, Website: https://sites.google.com/site/lccngroup/

[14] Network Management Research Group (NMRG), Website: http://irtf.org/nmrg

Abbreviations

3GPP	3rd Generation Partnership Project
3GPP LTE	3GPP Long Term Evolution
3GPP SAE	3GPP Service Architecture Evolution
AFI	Autonomic network engineering for the self-managing Future Internet
AP	Access Point
API	Application Programming Interface
BoF	Birds-of-a-Feather
BSS	Business Support System
CAPEX	Capital Expenditures
DiffServ	Differentiated services
DoW	Description of Work
E2E	End-to-End
EMS	Element Management System
eNodeB	Evolved NodeB
ETSI	European Telecommunications Standards Institute
FG-FN	Focus Group – Future Networks
FMC	Fix Mobile Convergence
FTTH	Fibre To The Home
GUI	Graphical User Interface
GW	Gateway
H2N	Human-to-Network
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IRTF	Internet Research Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IRTF	Internet Research Task Force
IS	Information System
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union – Telecommunications standardization sector
KPI	Key Performance Indicator
LCCN	Learning-Capable Communication Networks
LE	Large Enterprises
LSP	Label Switched Path
LTE	Long Term Evolution
LTE-A	LTE Advanced
MPLS	Multi Protocol Label Switching
NaaS	Network as a Service
NMRG	Network Management Research Group
NMS	Network Management System
OAM	Operations Administration and Maintenance
OFDM	Orthogonal Frequency-division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access

OPEX	Operational Expenditures
OSS	Operations Support System
PDN-GW	Packet Data Network Gateway
QoE	Quality of Experience
QoS	Quality of Service
ROI	Return of Investment
RAN	Radio Access Network
RRM	Radio Resource Management
SGW	Serving Gateway
SME	Small and Medium Enterprises
SLA	Service Level Agreement
SON	Self Organized Networks
TCO	Total Cost of Ownership
TMF	TeleManagement Forum
UC	Use case
UMF	Unified Management Framework
VoIP	VoIP - Voice over IP
VPN	Virtual Private Network

Definitions

Business requirements – *it is a description in business terms of what must be delivered or accomplished to provide value.*

Business bottlenecks – *any bottlenecks that may impact the business adoption of a new product/system/service by the market.*

Business opportunities - *main opportunities and relevancy of introducing a product/service in the market.*

Compliance - *the conformance to a rule, such as a specification, policy, standard or regulatory.*

Extensibility - *the ability to extend a system and the level of effort and complexity required to realize an extension. Extensions can be through as the addition of new functionality, new characteristics or through modification of existing functionality/characteristics, while minimizing impact to existing system functions.*

Functional requirement – *it is a description of a function, or a feature of a system, or its components, capable of solving a certain problem or replying to a certain need/request. The set of functional requirements present a complete description of how a specific system will function, capturing every aspect of how it should work before it is built, including information handling, computation handling, storage handling and connectivity handling.*

Interoperability - *the ability of diverse systems and subsystems to work together (inter-operate).*

Network Governance – *a framework which enables operators to describe their goals and objectives, through high-level means and govern their network. Include the derivation of network policies from the business goals through the use of semantic techniques.*

Non-functional requirement – *it is a description of how well a system performs its functions, it represents an attribute that a specific system must have. The non-functional requirements are controlled by other aspects of the system.*

Performance - *it describes the degree of performances a system (according to certain predefined metrics, e.g. convergence time).*

Privacy - *the ability of system or actor to seclude itself or information about itself and thereby reveal itself selectively.*

Operability - *the ability to keep a system in a safe and reliable functioning condition, according to pre-defined operational requirements.*

Reliability - *the degree to which a system must work. Specifications for reliability typically refer to stability, availability, accuracy, and maximum acceptable bugs.*

Requirement – a *requirement can be defined as a statement that identifies a capability or function that is needed by a system in order to satisfy its customer's needs. Actually before effectively discovering and developing requirements, well-defined and well-stated problems should be identified. The problems must be stated in a clear, unambiguous manner: they should explain the customer's needs (in case of UniverSelf, the network operators' needs).*

Resilience - *the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.*

Safety - *conditions of being protected against different types and the consequences of failure, error harm or any other event, which could be considered non-desirable.*

Scalability - *the ability of a system to handle growing amounts of work or usage in a graceful manner and its ability to be enlarged to accommodate that growth.*

Security - *the ability to prevent and/or forbid access to a system by unauthorized parties.*

Stakeholder - *a person, group or organization with an interest in something. The term stakeholder includes anyone who has a right to impose requirements on the system. This includes end users, operators, maintainers, owners, regulatory agencies, sponsors, etc. In the UniverSelf project analysis, example of stakeholders includes end users (residential, SME, LE), network operators and service providers, solution and technology providers, regulatory bodies.*

Supportability - *a system's ability to be easily modified or maintained to accommodate usage in typical situations and change scenarios. For instance, how easy should it be to add new blocks and/or subsystems to the support framework.*

Usability - *the ease with which a system performing certain functions or features can be adopted and used.*

Use Case – *it is a descriptor of a set of precise problems to be solved. It describes steps and actions between stakeholders and/or actors and a system, which leads the user towards a value added or a useful goal. A UC describes what the system shall do for the actor and/or stakeholder to achieve a particular goal. Use cases are a system modelling technique that helps developers determine which features to implement and how to gracefully resolve errors.*

Viewpoint - *It is a representation of a whole system from the perspective of a related set of concerns.*

Annex A – Scenarios as per the Description of Work

To achieve its objectives, UniverSelf uses not only purely technical work packages. Transverse investigations are also carried out, based on "Scenarios", of which each includes at least 2 use cases. The motivation to create industry impacting results, guided the UniverSelf consortium to implement a scenario-driven approach. In UniverSelf, a scenario is defined as a network context containing pre-identified management operations that could be solved more cost-effectively (when compared to current solutions) by applying autonomic principles).

The scenarios identified will be used during the project life to provide a bridge between the theoretical approaches, concepts, algorithms and the practical deployment. They also serve to ensure that UniverSelf research will be in line with open, real-life, fundamental technical problems faced by current and future networks. Finally these scenarios will also provide a "use life-cycle" to the project, thereby initiating continuous synchronization between the different RTD activities.

During project proposal building, the consortium worked on the definition of three exemplary scenarios for the main problems faced in the deployment and operation of complex and heterogeneous networks. The concerns of the network operators (FT/Orange, Telecom Italia and Telefonica I+D) were essential in the elaboration of these scenarios - namely "Operators' Service and Data Management", "SON for Radio Access and Core Networks Scenario" and "FI Services management and network resources optimization".

Scenario 1: Operators' Service and Data Management

Today telecommunications operators handle huge amounts of data, either collected during their daily operations or provided directly by customers: in addition to the data in personal profiles, operators have records of the communications (phone calls, messaging, and chats) among end-users, logs of the registration of mobile terminals on the mobile stations, visited URLs, etc. Ultimately, all these processes today already result in hundreds of databases with relevant data. ! Looking at the future, networks will be more and more pervasive and at the same time highly adaptive to changes in conditions: this growing complexity and "adaptivity" will generate a further exponential increase of data. Managing such data flows is a challenging task: the amount of data daily generated, with databases containing billions of records, is so large that manual analysis is practically impossible. In the past, the need to handle such large volumes of data led to the development of knowledge-based expert systems. The problem with this approach is that it is time consuming (the so-called "knowledge acquisition bottleneck"). The advent of data mining technology promised some more appropriate solutions to these problems, but even such techniques are still limited for the purpose of creating global network knowledge.

UniverSelf approach will help solving the following still-existing problems:

- The lack of a global end to end view of all data (both Users and net data), especially in NGN networks
- Lack of mappings/views correlating these data to services at different levels
- Cross-layer network data are not used for optimising use of network resources (e.g. allocation, cross layer traffic engineering, dynamic load balancing, etc)
- Cross-layer network data are not used for optimising the management (many alarms are still uncorrelated, we work out overlapping solutions to the same problem).
- No means of using data flows for enabling new business opportunities, one of which is the possibility of brokering specific data to Third Parties

Scenario 2: SON for Radio Access and Core Networks Scenario

This scenario demonstrates how both fixed/mobile operators and customers can benefit from the technologies that UniverSelf will bring into the real world. The former will benefit from reduction of their management and operational expenditures, as well as (in certain cases) infrastructure costs whilst operators' customers will benefit from an enhanced quality of service. The scenario describes a situation where the marketing unit of the Operator has launched a "video on demand" service on the LTE advanced network which complements the existing "mobile TV" MBMS service. Due to the success of the campaign, a peak of demand has to be handled to guarantee good network operation and QoS provisioning to the desired levels. With current technologies most O&M activities are performed manually, but a UniverSelf enabled framework allows the operator to just introduce its high level business and operating objectives into the Policy Manager. The Policy Manager derives and activates the operating policies into Self-Organizing Network (SON) mechanisms (Self Configuration and Self-optimization, monitoring and self-healing) and instructions to coordinate SON entities. In the end the complexity of the situation is hidden to the operator who may concentrate on the required business level actions.

The UniverSelf approach will help solving the following existing problems:

- Evolving the management plane to allow the introduction of high level policies
- Representing, abstracting and mapping etc.
- Enhancing cognitive capabilities in SON enabled network elements, including learning, decision making and knowledge sharing geared towards enforcing policies
- Develop a framework, ranging from algorithms to technological implementation, for coordinated SON mechanisms and entities to enforce policies

Scenario 3: Future Internet Services Management and Network Resource Optimization

Future Internet services will incorporate high multimedia flow demands, support of service continuity, and dynamic customization over heterogeneous and hybrid access and core networks. Legacy and new services will be combined in order to provide new forms of communication services. In particular, the considered FI services include Real-time Experience Social networking services and Global Inter-Connectivity and cooperation services (e.g., online real-time interconnected schools around the globe). Legacy and new services will be combined in order to provide new forms of communication.

The focus of the scenario is to configure and manage the necessary number of network components, e.g. Base Stations, access points, and routers with the least possible human intervention, for the purpose of setting up a temporary network for a Music Festival and of managing the load fluctuation generated by this subset, considering the supported FI services. The introduction of new demanding services on one side and the integration of different networking technologies on the other side will place new problems on the network operators. This scenario requires the evolution of network management and system configuration mechanisms, providing features such as dynamic self-organization of network clouds, fault management, optimization of resource usages in the context of either/both multiple networks or/and multi-layers.

Role of the Scenarios

The three scenarios introduced above are further explained in the appendix **Error! Reference source not found.** of this document according to a template defined in the ETSI AFI. Because they may not sufficiently cover the evolutions in network use and market trends that will occur along the project early stage (before kick-off and first half, UniverSelf may identify the need for defining one or two additional scenarios during the first half of the project. After this period, there would be no value in modifying the scenarios description, as time would be insufficient to transform these scenarios into solutions. Along the life of the project scenarios will be used:

- As warrant of the industrial focus of UniverSelf work.
- As operator-oriented playground for all the activities related to testing and assessment of UniverSelf solutions.
- As vectors between the Work Packages tasks, thanks to their conveying of requirements between the different steps of their life-cycle. In this sense, they provide a time-structure to UniverSelf.
- As a pool of use cases.