CASE STUDY – PART I

Network and Service Governance

Abstract

An increasing number of heterogeneous devices are being used from different places to access a myriad of very different services and/or applications. This situation requires a new reliable, dynamic, and secured communication infrastructure with highly distributed capabilities. The autonomic network envisions meeting these features. Although one of the goals of Autonomic Infrastructure is that of self-management, a framework aiming to manage an autonomic network must include tools to facilitate the control and supervision of the network. Network governance is meant to provide a mechanism for the operator to adjust the features of the demanded service/infrastructure using a high level language. These high level directives must be translated into low level policy rules that can be enforceable to control the behaviour of the self managed resources.

This case study describes the use of a network governance framework for the management of IPTV services, deployed either in fixed Fiber-To-The-Home (FTTH) autonomic network or through wireless access. The first part of the case study focuses on a brief description of the case, its methods, concepts and expected innovation.The specific functional, non-functional requirements and the associated problems of this case were presented in the deliverable D4.1 [7]. The prioritization of the problems and functional requirements were presented in deliverable D4.2 [8].

Date of release

17/09/2012

CONTENT

STORY LINE

Telecommunication 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 for which they have been 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.

The Network and Service Governance case 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.

The Network and Service Governance case 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

The case will demonstrate the feasibility of a policy-based management network both on fixed and mobile access, as shown in Figure 1. The mobile network is based on WiFi connection on a DSL network. For the fixed environment, we have chosen one of the technologies used for the delivery of high speed broadband access: Fiber to the Home (FTTH). FTTH rollout is today one of the main drivers of telecom business transformation, encompassing high investments in equipment and systems. While 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 Network and Service Governance case aims to provide a service assurance solution for FTTH environments. The embodiment of functionalities like self-monitoring, self-diagnosis and self-healing into the network elements 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.

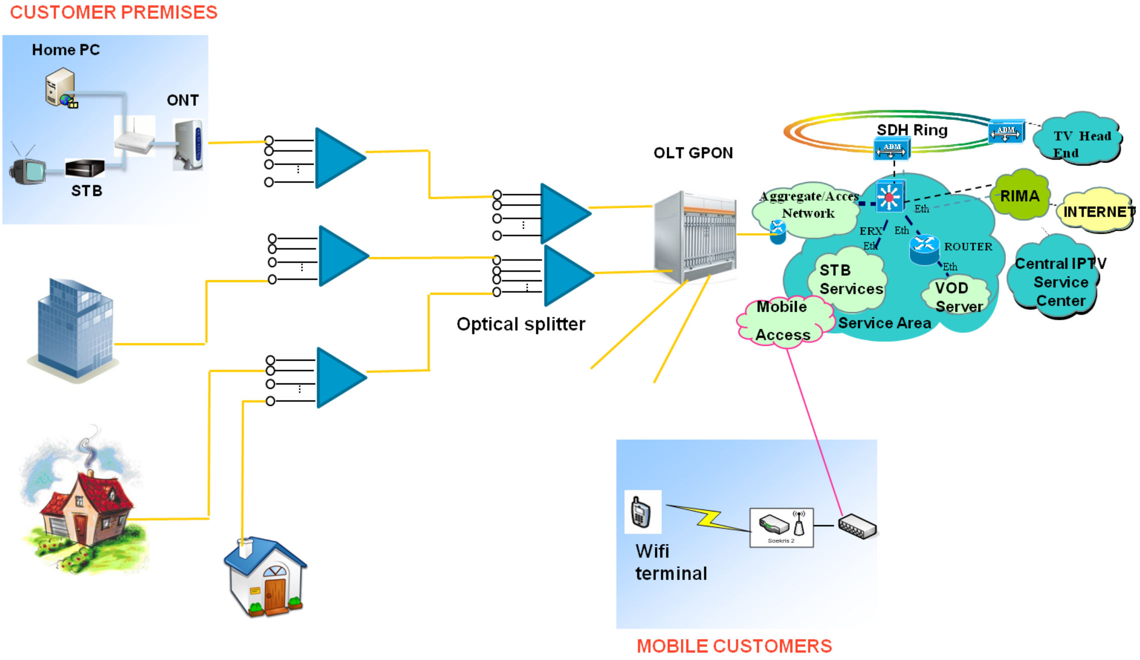

Figure 1: Network topology, showing both FTTH and mobile access

The Network and Service Governance case concerns mainly the deployment and operation phases of services on the network. The activities at the provisioning phase are connected to the Service Configuration & Activation eTOM processes and the corresponding Resource Provisioning process. At the operation phase, the case will perform monitoring and diagnosis, while re-configuration could be invoked for the correction of anomalies. These activities are related to the Service Problem Manager, Service Quality Management processes in eTOM and the corresponding Resource Trouble Management and Resource Performance Management processes.

In summary, the main objectives of this case are:

- Enable operators to describe their goals and objectives, through high-level means and govern their network.
- Application of governance concepts to IPTV services on fixed and mobile networks.
- Implementation of a self-management mechanism for IPTV services. This mechanism will be based on an architecture of distributed agents able to monitor, diagnose and resolve issues.

The rest of this document provides further information about the case. The next section presents a more detailed list of the problems this case aims to solve. Then, the case is modelled in terms of actors, events and functions. Finally, a section is devoted to highlight the innovation concepts introduced in the case.

PROBLEM STATEMENT

Network operators aim to deliver differentiated services driven by business oriented objectives, but the increasing complexity of networks and services makes it difficult to cope with the requirements of managing a network which fulfils business objectives. A current bottleneck in the configuration of large scale communications networks is the manual alignment of network policies to business policies. Realizing business policies requires not only the collaboration of separate constituencies of experts to define the policies, but also the configuration of different devices.

The problem addressed in this case intends to reach the following objective:

Govern FTTH and wireless networks by means of policy-based management network, where operator's requirements are expressed in terms of high-level objectives

This problem can be decomposed into the following sub problems:

Problem 1: Definition of high-level objectives (performance, constraints, priorities…), taking into account business parameters such as the different types of customers and SLAs.

Problem 2: Translation of the high-level objectives to low level network policies, resolution of conflicts that may appear, and guaranty of the integrity of the information stored in the policy server. This implies the use of correlation and filtering techniques to be applied on policies.

Problem 3: Identification of the best solution to be deployed, taking into account the current network context status (topology, devices, their configuration parameters, their current operational status, resource availability, capabilities of each network element, etc.).

Problem 4: Deployment of the selected configuration, which may involve more than one network domain (e.g. radio access network, aggregation or backhaul/core network segments). Coherence should be guaranteed through the different domains, solving any incompatibility that may appear.

Problem 5: Context discovery and monitoring. Network elements in FTTH environments should be able to discover and monitor their operational context using network protocols. External input needed for the operation should be minimized, so as the system does not rely on the heavy inventory systems of the operators.

Problem 6: Performance measurements, diagnosis and self-healing. The objective is to ensure that the desired QoS level is guaranteed during the operational phase of the service. In case of SLA violations, a reconfiguration of network elements may need to be triggered in order to adjust the network configuration parameters following the network conditions with the objective of guaranteeing the committed service level.

The functional and not-functional requirements that derive from this problem statement have been gathered and grouped in Deliverable D4.1. Deliverable D4.1 is a public report available on the project web site: http://www.univerself-project.eu/technical-reports or on request (see Contact section at the end of this document).

MODELLING

In this section the model of the case is presented, in terms of actors who interact with the functionalities of the case, triggers that enable the case functionalities, and phases, each of them corresponding to a specific task that is performed within the case.

Actors

The main actors involved in this case are the Residential Customers, that are the end users of the IPTV services, and human operators who interact with the autonomic infrastructure using the network governance interface. Three different types of operators are usually implicated: the Product Manager, that designs, from a high-level point of view, the service to be offered to customers; the Call Center operator, in charge of the relationships with existing or potential customers, and in this particular case receiving the customer order for contracting a service and triggering the provisioning request ; NOC (Network Operation Center) operator, in charge of supervising the status of the network. These three types of operators work in different departments of the telecommunications company that is delivering the services.

Triggers

The operator manages the autonomic network by means of high-level objectives expressed through the network governance tool. Triggers for the operator consist of:

- New high level objectives that need to be set to the network elements. These objectives may refer, for instance, to the deployment of a new service, or to the monitoring of existing ones.
- Provisioning request, for the actual deployment of an already defined service to a given customer.
- In the opposite direction, network elements send notifications to inform about the status of the network and services: anomalous conditions, SLA violations, self-adjustments of the network configuration parameters made autonomously by the network elements or alarms to inform about an unusual situation that could not be handled autonomously by the network. This runtime information is shown to the operator through the human-to-network user interface.

Phases

The solutions to the problems identified in the previous section can be decomposed in several phases. The sequence of the phases conforms to the lifecycle of an IPTV service, from the definition to the runtime phase. This section describes in detail the different phases and its sequence. For the description of the phases, a distinction is made between the Service Definition stage and the Service Provisioning & Runtime stage. For each of these stages, a subset of phases has been identified.

During the Service Definition stage, the Product Manager defines the high level objectives (HLOs) that drive the operation of the network. These HLOs defined in Phase A are based on the requirements of the services that are/will be deployed in the network, relevance of the users, timely planned behaviour of the network and information provided from the human operator. The service profiles produced in this first place are matched in phase B with customer profiles. This functionality will enable the operator to perform more efficient and intelligent network planning and dimensioning. Furthermore, this allows the operator to define specific services to be offered to specific customers (i.e. services with different quality could be offered for new customers, self-employees or VIP customers). In phase C the mapping of abstract service requirements to technical requirements takes place. The QoS requirements specified for a service need to be translated to network parameters, such as jitter, packet error rate, etc. Then, phase D is triggered, where the outcome of the previous phases is combined and policy rules are generated based on the specific low-level mechanisms and languages. The generated policies may be conflicting since they were generated for different network domains that are governed with different scopes. In order to avoid inconsistencies and incoherence in the network, policies conflicts are resolved in phase E. Finally, phase F maintains the new policies and the existing ones in a policy repository.

After phases A-F have been executed, a new service is defined and ready to be used. When one customer contacts the Call Center and decides to contract the offered service, the operator will trigger a provisioning request through the governance interface. This triggers phase G, where a network context analysis takes place, aiming to determine the current context condition associated with the network. The network context can be defined as a set of parameters that identify the network (e.g. the topology, devices, and its configuration parameters). This analysis takes into account existing knowledge that has already been extracted from raw monitoring data. The output of this phase is a set of possible deployment configurations. In phase H, the most suitable configuration is chosen, based on the parameters acquired from previous phases and technical investigation into the operator's network architecture, which is composed, by the network profile, service profile of the deployed services and the user profile of the customers. The selected configuration feeds Phase I, where the actual configuration on the network is performed.

Once the provisioning state has succeeded, phase J is triggered, where continuous monitoring of the network is performed by collecting measurements. The objective is to ensure that the desired QoS level is guaranteed during the operational phase of the service. When phase J finds that a given network element is not working properly, triggers phase K to evaluate the impact of this malfunctioning on the deployed services. Phase K does this by comparing the current network real situation with the desired value associated with the governance policies. The output of this phase feeds Phase L, so actions can be triggered in order to adjust the network configuration parameters following the network and service conditions. The network automatically plans and executes the needed actions as re-routing, policies changes, etc. to avoid the services being impacted. The first objective is to guarantee the committed service level, which sometimes implies a workaround instead of a definitive solution. Performance problems usually require changes on network and service resources, which could require stock management, workforce assignment, network upgrading, etc. Phases J-L also notify the NOC operator about the current status of the network and the actions that may have been triggered.

The case actor, the triggers and the phase sequence are presented in the Case Concept Map in Figure 2.

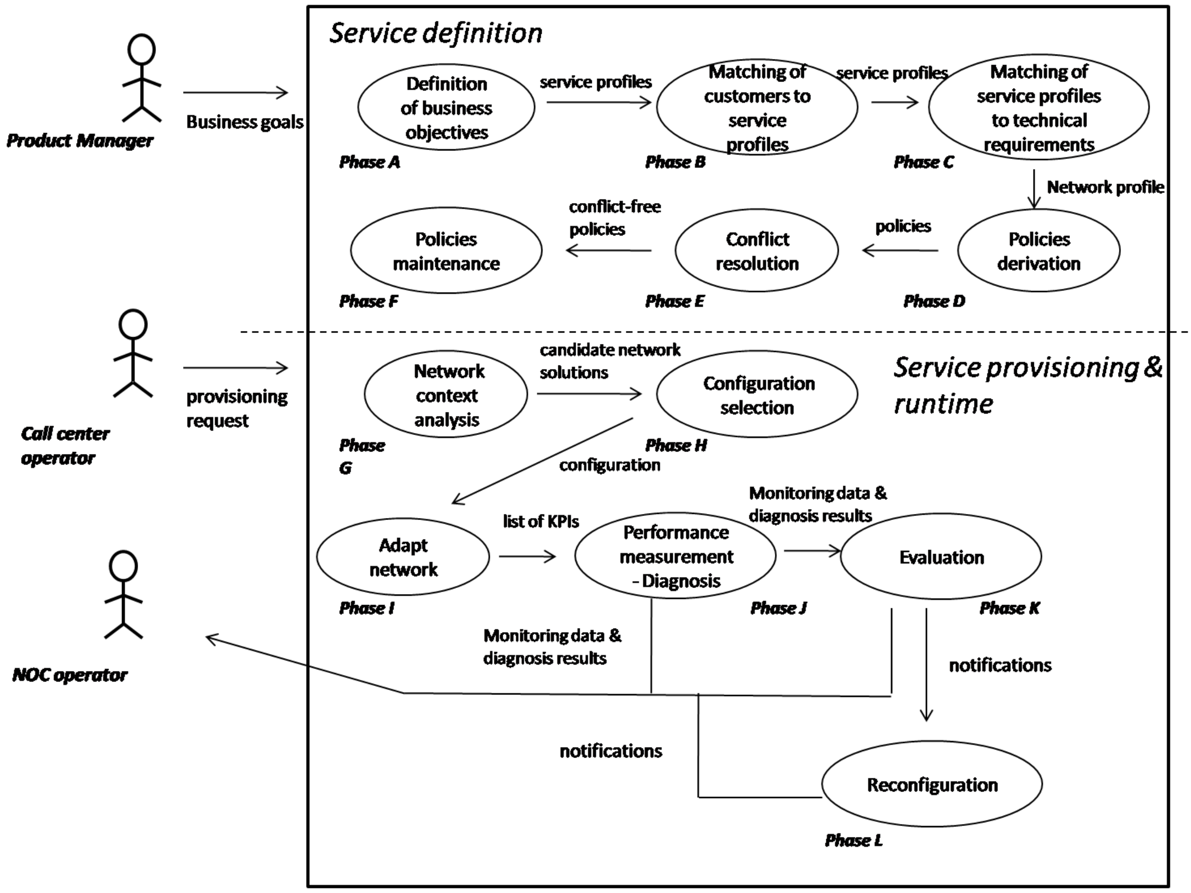

Figure 2: Case Concept Map

INNOVATION

This section tries to highlight the innovative ideas behind this case, differentiating them from the state of the art and emphasizing the benefits the case provides.

Enabling concepts and mechanisms

The innovations in this case focus on three different aspects: Network Governance and self-management in fixed FTTH and wireless environments.

With respect to Network Governance, the case aims to design and implement a goal-based management system for the governing of the whole lifetime of the services. In order to demonstrate the utility of such a governance framework, it will first be applied to current services and networks. IPTV has been chosen as the service to be deployed.

Network governance is meant to provide a mechanism for the operator to adjust the features of the demanded service/infrastructure using a high level language. In order to achieve this objective a business language may be required that will help the operator to express what is needed from the network. These high level directives must be translated into low level policy rules that can be enforceable to control behaviour of self managed resources. Reasoning is also an important challenge in the scope of network governance, as it can be exploited for the mediation and negotiation between separate federated domains. In other words, to allow interoperability between semantically equivalent, but differently instantiated models, it is required to cover multiple standards instead of relying on a single information model. This leads to the use of ontologies for allowing semantic fusion and reasoning with knowledge extracted from data/information.

Moreover, policies are inherent to network governance. Policies specify rules that should govern the behaviour of the managed elements. In particular, network governance is almost always interwoven with policies lying at the highest level of the so called policy continuum. In network governance, policies are required for the selection of the optimal configuration of a service and for the translation from business level policies to low level policies. Finally, configuration enforcement mechanisms are necessary in order to apply the configuration decision. First, it is required to identify concerned equipments and request each of them to perform the appropriate configuration actions. Then, each of the targeted equipments has to translate and enforce the decision. The term configuration implies self-configuration and also includes reconfiguration actions (re-optimizations). Reconfiguration actions can be triggered in order to adjust the configuration parameters following network, service and customer conditions.

Regarding the self-management in fixed FTTH environments, the case will provide the network elements with context discovery, probabilistic self-diagnosis and self-healing capabilities. FTTH rollout is today one of the main drivers of telecom business transformation, encompassing high investments in equipment and systems. In traditional copper-based DSL services, the network structure was relatively simple, with a relation one-to-one between the ports at the Central Office (CO) and at the customer premises. But Passive Optical Network (PON) has a tree layout, with different levels of splitting. Failures in the branches of this tree cannot be located easily even with sophisticated optical testing techniques, such as reflectometric procedures. In addition, new equipments are located on both sides (OLT (Optical Line Termination) at Central Office, ONTs (Optical Network Terminations), routers, set top boxes or IP phones at home). These devices provide useful information, of heterogeneous nature and format, through different interfaces and using a variety of protocols, information that need to be evaluated in order to find the root cause of a failure. The case aims to research a service assurance solution for FTTH environments, providing the network elements with self-* features. These functionalities will enable the early detection and resolution of network, QoS, and QoE problems with limited or no customer impact.

Traditional telecom networks management relied on big inventory systems where all the network elements were stored, and on the assumption that the state of every entity was precisely known at any instant. Classical Operating Support Systems were therefore built as large centralized systems, able to deal with huge amounts of information [1] [2] and find the root cause of failure, but unable to provide a solution when only partial data were available. Today the introduction of new technologies and the popularity of broadband-based services have produced an important growth in the number of managed entities, which complicates the labour of centralized solutions. Topology and inventory data are scattered among multiple systems and it is not always complete neither consistent. The complexity of the network environment makes very difficult to observe certain aspects of the domain, and moreover, the relationships between domain events are not always deterministic. Besides, it is often impractical to model and analyse explicitly all the dependencies. Moreover, the explosion of new devices makes difficult the gathering of all the needed monitoring information, and when it is feasible to get it, sometimes it is inaccurate or vague. Therefore, uncertainty in data has become a main source of problems for network operators. To overcome the above described problems, the Network and Service Governance case will deploy a distributed set of agents for the self-management of FTTH network elements. The agents will monitor the current network status and derive a probabilistic diagnosis through the use of inference on Bayesian Networks. Bayesian Networks [3][4] are probabilistic graphical models able to represent the knowledge and reasoning under uncertainty conditions.

With respect to wireless networks, there already exist strict requirements for specific levels of network QoS in terms of changing load conditions. The work in this case includes dynamic route adaptation techniques and handover/self-healing/load-balancing actions as derived actions of Governance framework. The dynamic route adaptation of individual traffic flows, together with new Traffic Engineering optimization techniques, allows the utilisation of underutilised resources and improves the system performance. The work in this case provides solutions to these problems using evolutionary algorithms and more specifically Genetic Algorithms. The algorithms find near optimal flow patterns for a given set of requests, given the network topology. As a result, feasible requests are routed on a path from the source node to the destination node along which capacity constraints are satisfied, minimizing the congestion and maximizing the potential for traffic growth. The load-balancing actions include handover decision algorithms triggered by the Governance framework in order to conserve the QoS/QoE experienced by the user under specific QoS thresholds defined by SLAs. The self-healing actions are triggered in case of cell outage and target on decreasing the connection loss rate and QoS degradations during a cell outage incident by increasing the transmission power of neighbouring cells.

The above mentioned algorithms have been implemented as a set of Network Empowerment Mechanisms or NEMs[1], namely the FTTH Bayesian Diagnosis NEM , the Routing for MPLS Traffic Engineering NEM and the Self-Healing Mechanism for Cell Outage Management NEM.

Differentiation from the state of the art

Although already elaborated in the previous section, the main progresses with respect to the state of the art are summarized here:

- Governance of network and services from a high-level point of view, with automatic translation of business objectives to network policies. Current procedures in network operators involve the manual derivation of the network configuration that involves very specialized technicians. This approach leads to a bottleneck in the configuration process when deploying new services.
- Policy-management framework allowing the enforcement of operator's directives to the network elements.
- End-to-end service and resource management for FTTH environment, based on distributed agents gathering monitoring information. The use of distributed agents helps to address the scalability and complexity inherent to the current and future networks. Agents continuously monitor and diagnose the network conditions, triggering a self-healing process when degradation in the QoS is detected.
- Optimization of traffic based on evolutionary algorithm techniques facilitating dynamic route adaptation of individual traffic flows at a network environment with rapidly changing load conditions.

[1] *NEM = a functional grouping of objective(s), context and method(s) where "method" is a general procedure for solving a problem. A NEM is (a priori) implemented as a piece of software that can be deployed in a network to enhance or simplify its control and management (e.g. take over some operations). An intrinsic capability of a NEM is to be deployable and interoperable in a UMF context (in a UMF-compliant network).*

Impacts and benefits

Autonomic management in general and this case in particular, are expected to impact business metrics as follows:

- OPEX reduction, by reducing the need of highly specialized technicians through autonomic self-management procedures applied to network elements.
- Reduction of human intervention – reduction of efforts required for the deployment, configuration and operation of new services on FTTH and wireless networks
- Reduction of high specialized personnel in maintenance tasks. The use of the governance framework should decrease the need of high specialized technicians for purely maintenance of the network.
- Reduction of downtime of a service, thanks to the proactive self-monitoring, self-diagnosis and self-healing capabilities.
- Reduction of churn rate, by increasing the QoE of IPTV customers.

In general, self-management capabilities in network elements will help to optimize the effort in operations. By enabling end to end diagnosis and healing procedures, it will decrease the number of customer complaints and reduce network management effort.

On the other hand, the deployment of these autonomic procedures implies the evolution of the network elements, which undoubtedly will impact CAPEX.

TO BE CONTINUED

This document is the first part of the Network and Service Governance case study that is published in the UniverSelf project and covers the introduction, general description, problem statement and innovation of this case. During the lifetime of this project other Network and Service Governance studies (and non case study documents) will be published that will provide more detailed information, results and innovations of this case study. Readers should keep in touch to get premium access to these high-quality reports!

REFERENCES

[1] ITU-T (1989), Principles for a Telecommunications Management Network, Recommendation M.3010, 1996.

[2] M. Creaner, J. Reilly (2005). NGOSS Distilled – The Essential Guide to Next Generation Telecoms Management. The Lean Corporation, August 2005.

[3] Pearl, Judea. Bayesian Networks: A model of self-activated memory for evidential reasoning. Cognitive Science Society, 1985.

[4] Pearl, Judea , J.H. Kim. A computational model for causal and diagnostic reasoning in inference systems. Proceedings of the 8th International Joint Conference on Artificial Intelligence (IJCAI), 1983.

[5] Jacobson Ivar, Christerson M., Jonsson P., Övergaard G., Object-Oriented Software Engineering - A Case Driven Approach, Addison-Wesley, 1992

[6] Cockburn, Alistair. Writing Effective Cases. Addison-Wesley, 2001.

[7] "Synthesis of case requirements" - Deliverable 4.1, August 2011, http://www.univerself-project.eu/technical-reports

[8] "Synthesis of case requirements – Release 2" - Deliverable 4.2, April 2012, http://www.univerself-project.eu/technical-reports

CONTACT INFORMATION

For additional information, please contact: Beatriz Fuentes, fuentes@tid.es or Carolina García-Vázquez (cgv@tides); or consult www.univerself-project.eu

UNIVERSELF CONSORTIUM