ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

Cyber Physical System based Proactive Collaborative Maintenance

D1.2 Consolidated State-of-the-Art of Sensor-based Proactive Maintenance

Appendix 2:

Existing platform architectures and overall designs

Work Package	WP1 - Service platform architecture requirement definition. Scenarios and use cases descriptions
Version	1.0
Contractual Date of Delivery	30/04/2016
Actual Date of Delivery	03/06/2015
Dissemination Level	Public
Responsible	Erkki Jantunen
Contributors	P□l Varga - AITIA, Csaba Hegedus □ AITIA, Bence Petho - AITIA, Istv□n Moldov□n - BME

The MANTIS consortium consists of:

Num.	Short Name	Legal Name	Role	Country
1	MGEP	Mondragon Goi Eskola Politeknikoa J.M.A. S.Coop.	CO	ES
2	MONDRAGON	Mondragon Corporacion Cooperativa S.Coop.	BEN	ES
3	IKERLAN	Ikerlan S.Coop.	BEN	ES
4	TEKNIKER	Fundacion Tekniker	BEN	ES
5	FARR	Fagor Arrasate S.Coop.	BEN	ES
5.1	KONIKER	Koniker S.Coop.	TP	ES
6	GOIZPER	Goizper S.Coop.	BEN	ES
7	ACCIONA	Acciona Infraestructuras S.A.	BEN	ES
8	MSI	Mondragon Sistemas De Informacion S.Coop.	BEN	ES
9	VTT	Teknologian Tutkimuskeskus VTT Oy	BEN	FI
10	LUAS	Lapin Ammattikorkeakoulu Oy	BEN	FI
11	NOME	Nome Oy	BEN	FI
12	FORTUM	Fortum Power And Heat Oy	BEN	FI
13	SQ	Solteq Oyj	BEN	FI
14	WAPICE	Wapice Oy	BEN	FI
15	AAU	Aalborg Universitet	BEN	DK
16	DANFOSS	Danfoss A/S	BEN	DK
17	UNIV	Universal Foundation A/S	BEN	DK
18	HGE	Hg Electric A/S	BEN	DK
19	VESTAS	Vestas Wind Systems A/S	BEN	DK
20	SIRRIS	Sirris Het Collectief Centrum Van De Technologische Industrie	BEN	BE
21	ILIAS	Ilias Solutions Nv	BEN	BE
22	ATLAS	Atlas Copco Airpower Nv	BEN	BE
23	3E	3e Nv	BEN	BE
24	PCL	Philips Consumer Lifestyle B.V.	BEN	NL
25	PHC	Philips Medical Systems Nederland B.V.	BEN	NL
26	PHILIPS	Philips Electronics Nederland B.V.	BEN	NL
27	S&T	Science and Technology B.V.	BEN	NL
28	TU/E	Technische Universiteit Eindhoven	BEN	NL
29	RUG	Rijksuniversiteit Groningen	BEN	NL
30	UNINOVA	UNINOVA - Instituto de Desenvolvimento de Novas Tecnologias	BEN	PT
31	ISEP	Instituto Superior de Engenharia do Porto	BEN	PT
32	INESC	Instituto de Engenharia de Sistemas e Computadores do Porto	BEN	PT
33	ADIRA	ADIRA - Metal Forming Solutions S.A.	BEN	PT
34	ASTS	Ansaldo STS S.p.A.	BEN	IT
35	CINI	Consorzio Interuniversitario Nazionale per l'Informatica	BEN	IT
36	AIT	Austrial Institute of Technology GmbH	BEN	AT
37	HBM	Hottinger Baldwni Messtechnik GmbH	BEN	AT
38	INNOTEC	Innovative Technology and Science Limited	BEN	UK
39	AITIA	AITIA International Inc.	BEN	HU
40	BME	Budaperst University of Technology and Economics	BEN	HU
41	JSI	Josef Stefan Institute	BEN	SI
42	XLAB	XLAB d.o.o.	BEN	SI
43	FHG	Fraunhofer Institute for Experimental Software Engineering IESE	BEN	DE
44	M2X	M2Xpert GmbH & Co KG	BEN	DE
45	STILL	STILL GMBH	BEN	DE
46	BOSCH	Robert Bosch GMbH	BEN	DE
47	LIEBHERR	Liebherr-Hydraulikbagger GmbH	BEN	DE

Document Revisions & Quality Assurance

Revisions:

Version	Date	By	Overview
0.1	20/04/2016	Bence Petho	First Draft
1.0	02/06/2016	Mikel Muxika (MGEP)	Format correction Deliverable info update

Abstract

The purpose of this document is to give a state-of-the-art report on proactive maintenance platform architectures. There are several system management frameworks already available in the telecommunications and more broadly in the ICT sector, as the main competitive edge for network operators is the impeccable network they can provide. These approaches and frameworks (mainly created by/for network operators) might also be useful analogues when defining and designing MANTIS elements, as they have been tested in practice and refined over time.

In this document we will present the reference model created by ITU-T and is under constant research ever since. This service model, system management aspects and framework has been also widely validated and implemented.

Table of Contents

1 Introduction

Users take full advantage of network services nowadays, without even noticing the fact of accessing a globally integrated computer network. Operating and maintaining such geographically diverse network is a quite a challenge under real-life conditions where network elements have limited space for lifecycle change, and numerous errors can occur in the managed network.

ITU-T (the International Telecommunication Union) has basically standardized a business, service, network, and network element management via clear definitions of processes at each level, system management aspects and best practices, technological standards, etc.

In this document we will present these models of the ITU and their basic principles that can be useful for MANTIS: the Telecommunications Management Network (TMN); the Fault, Configuration, Accounting, Performance and Security Management (FCAPS); and the Enhanced Telecom Operations Map (eTOM). Based on the framework of these models, we will also present an existing architecture for managing Ethernet networks which can be a take-off point for MANTIS.

2 ISO Telecommunications Management Network Model

In general, assuring that the service is available for the users in at least a certain, agreed level of quality (agreed upon in Service Level Agreements SLAs) is the responsibility of the service provider. Though, Service Level Specifications (technical specs derived from business SLAs) do not define prevention, observation or elimination of service degradation definitions, keeping the agreements (SLAs) is the service providers responsibility.

The Telecommunications Management Network is a protocol model defined by ITU-T. It is the part of the ITU-T Recommendation series M.3000 and is based on the OSI management specifications in ITU-T Recommendation series X.700 [1].

It incorporates three aspects of network management, as shown in Figure 1.

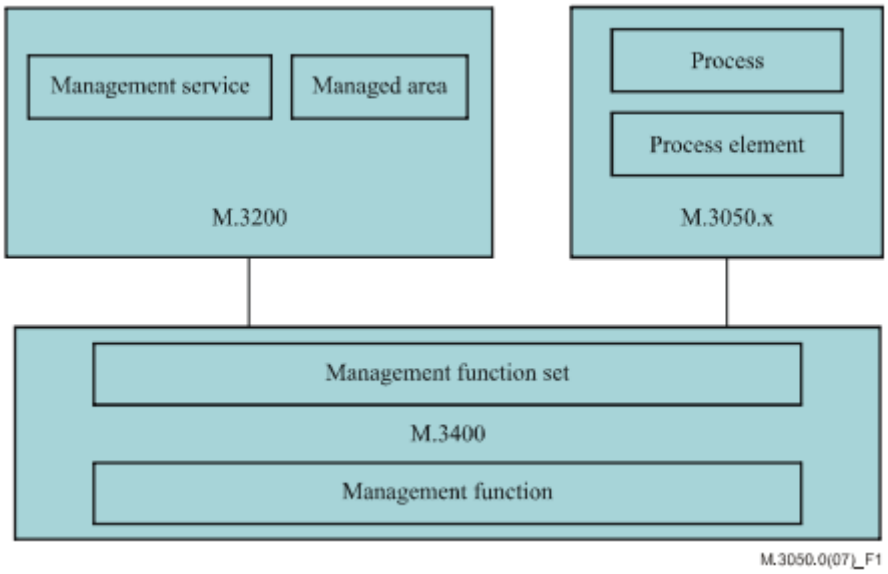

Figure 1. The structure of the ITU-T M.3000 Recommendation series. (Source: [2], p. 10.)

These three aspects will be discussed in the following sub-sections:

Recommendation	Name	Function
M.3200 Series	ITU-TMN Model [3]	Service Providers Operation Levels
M.3050.X Series	eTOM [2]	Business Process Standardization
M.3400 Series	FCAPS [4]	Network-centric Approach for Service Providers

Table 1. The Telecommunications Management Framework by ITU-T

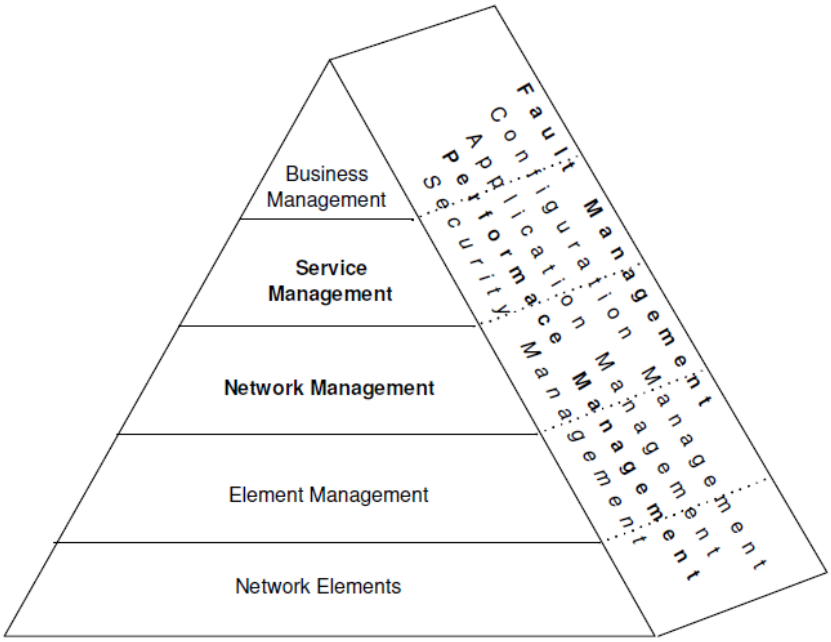

Figure 2. The FCAPS and TMN Model structure.

Although FCAPS and the TMN model both define different aspects and functions for a management system, these definitions complete each other, and can be understood form two different dimensions, as seen in Figure 2.

2.1 FCAPS

The traditional network management functions are defined by ITU-T in [1]. These may be grouped into five distinct areas, namely fault management, configuration management, accounting management, performance management and security management. This model is lately called □FCAPS□.

The FCAPS model identifies the five main elements (functions) of network (system) management. FCAPS is an acronym of the tasks that such system has to serve:

- Fault Management
- Configuration Management
- Accounting / Administration
- Performance Management
- Security Management

When focusing on service availability and quality, the misbehaviour of various objects both in the managed network and service context is being analyzed constantly. In order to keep up-to-date status of the managed system, permanent evaluation of the network elements is unavoidable. This is the main task of performance management (PM). Keeping track of the hardware and software configuration changes in the managed network □ as well as the changes of the service □ is the main function of configuration management (CM). Fault management (FM) encompasses the detection, isolation and correction of abnormal operation of the managed objects (network elements, service applications, etc.). This is only efficient if the operator has up-to-date status information (provided by PM) and interconnection information (provided by CM) about the objects. Intrusions and frauds are to be prevented by security management (SM), which also covers the detection, handling and logging of such activities. Accounting management addresses important issues, these, however, have minor effect on service quality and performance, hence we do not discuss them here.

FCAPS is widely used in telecom network management systems; see Section 4 as an example.

2.2 ITU TMN Model

The FCAPS approach is highly technical and defines the functionalities for an automated network management system and does not give any guidelines on how this task can be implemented in a functioning organization. This is done by the TMN Model, which therefore defines a different aspect of service management: business and organizational behaviour.

This framework identifies four logical layers of network management. This gives a guideline for network operators to create complex services and back them up with proper organizational and network structures.

The general TMN model is traditionally pictured as a triangle with a perspective. The triangle represents the various management levels from business processes to the network elements, whereas the perspective of the triangle suggests that the FCAPS tasks should be taken care of at each level, as seen on Figure 2.

These logical layers are the following:

Layer	Concerned with
Business Management Layer	high-level planning, budgeting, goal setting, executive decisions, business-level agreements
Service Management Layer	• uses information presented by Network Management Layer to manage contracted service to existing and potential customers; • this is the basic point of contact with customers for provisioning, accounting, QoS expectations and fault handling; • it maintains statistical data (accounting and administration)
Network Management Layer	• the Network Management Layer has visibility of the entire network based on information provided by the Network Element Layer; • coordinates all network activities and supports demand of the Service Management Layer
Network Element Layer	manages each network element: element activity; configuration, logs
Network Elements	switches, routers, service endpoints

Table 2 The ITU TMN Model (Source: [5], p. 9.)

This is a top-down framework, where the top two levels are mostly business-oriented and the bottom levels are customized to the current business needs and business service models.

The top two elements are further helped by ITU-T business process standardization efforts which culminated in eTOM, discussed in the following sub-section.

2.3 eTOM

The Enhanced Telecom Operations Map (eTOM) was created by ITU-T in 2003. It is a comprehensive business process framework for service providers (but not a business model itself). It contains an industry-agreed set of integrated business process descriptions. It is deeply embedded with and extends the TMN and FCAPS models. It is also a part of NGOSS (New Generation Operations Systems and Software) program.

"The eTOM framework can serve as the blueprint for standardizing and categorizing business activities (i.e. process elements) that will help set the direction and the starting point for development of business and operations support systems." (M.3050.0 p. 11. in [2])

It describes and analyses different levels of enterprise processes according to their significance and priority for the business. The framework is defined as generically as possible so that it remains organization-, technology-, and service-independent. It also provides a neutral reference point for internal business process reengineering needs, partnerships, alliances, and general working agreements with other companies [6]. This results in a clear definition of an organization like in Figure 3 or Process Flow descriptions like in Figure 4.

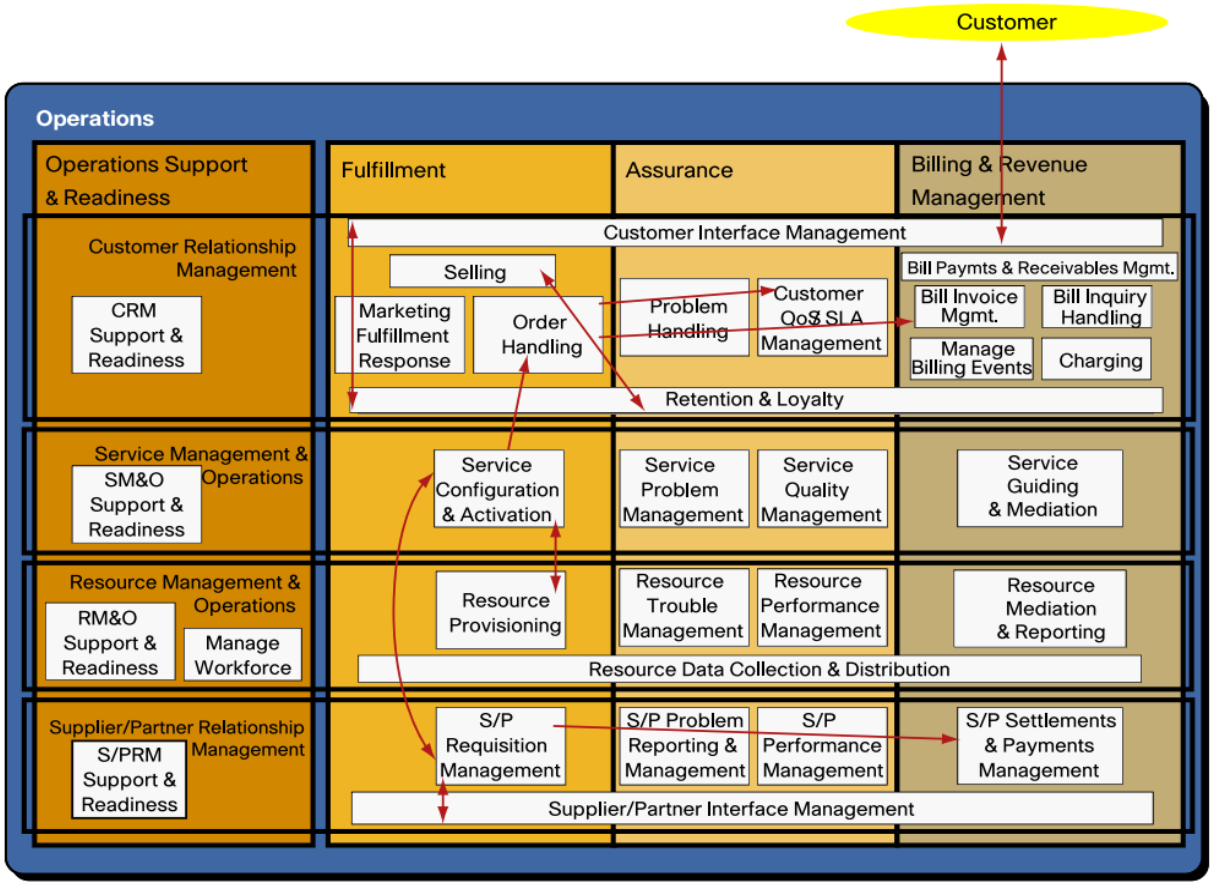

Figure 3. Exemplary outcome of using the eTOM Framework for process definitions [6]

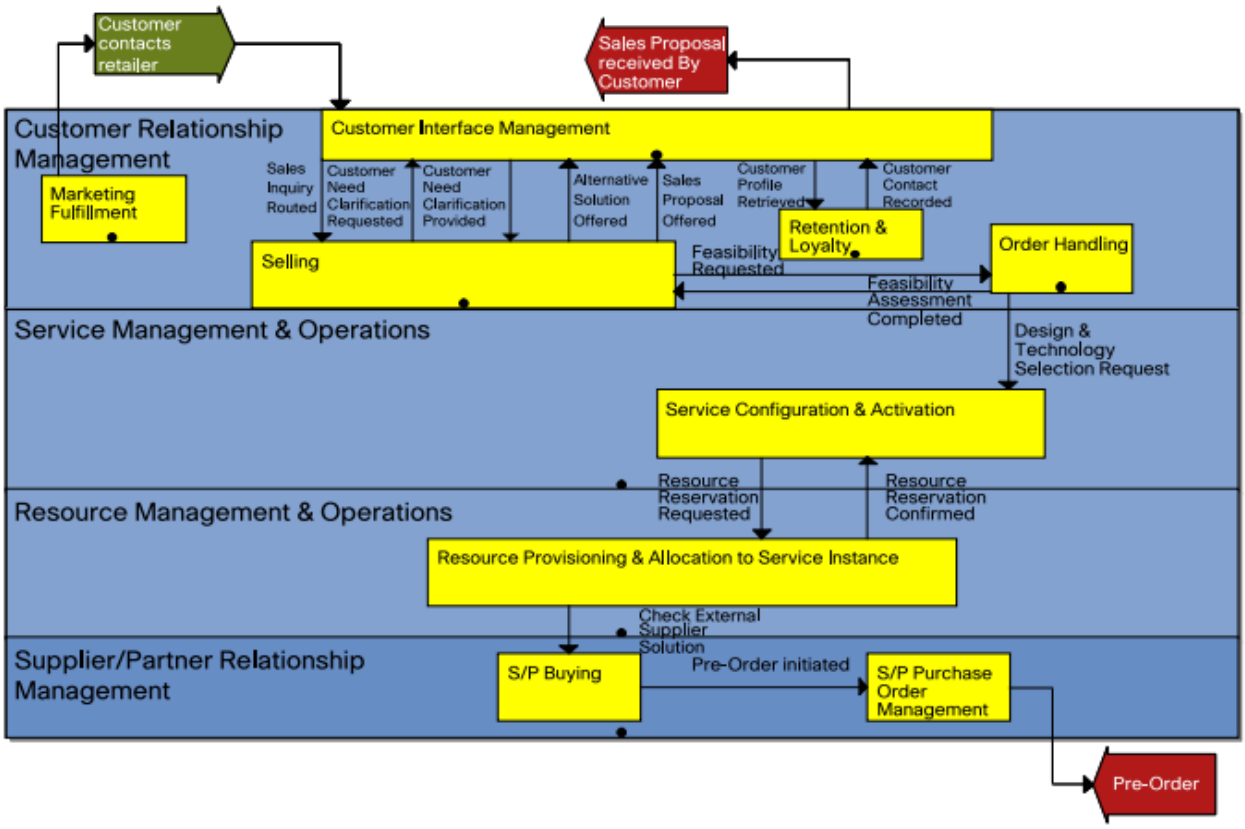

Figure 4. Example Process Interaction Flow [6]

Rich further work has been done on eTOM as well, several case studies and extensions are available. For example, [7] explores the advantages of adding an organization level approach to eTOM, as it might further support scaling and handling large telecom company operations by helping managers to have an overview of the processes involved.

Other IT service management frameworks are ITIL, COBIT, PRINCE2 and Learn IT [8].

2.4 Relevance to MANTIS

Based on this framework (and telecom industry best practices) it might be viable for the project to put quite an emphasis on how a MANTIS framework would be implemented in real business environments and in a pre-existing corporation. This can be achieved by defining and describing the relevant business processes (business process standardization) to proactive maintenance, asset management or even asset procurement as well. After that, the business environment should also be modelled as well by asking questions like these:

- How deep can the suppliers be embedded in the company□s asset management? (e.g. long term contractual terms, guarantee obligations are industry standard)
- How rigid is the production of vendors? (e.g.: How long does it take for replacement parts to arrive after the order is placed?)
- Therefore, how deep are the IT systems interconnected? (e.g. if MANTIS is required to have ERP and automatic order placement capabilities based on its asset wear forecasts)
- What are the typical software frameworks, UI arrangements, etc. used?
- With these reference business models, processes and practices, the MANTIS framework HMI, ERP interfaces can be tailored to the needs.

3 Service Assurance Framework

This section describes a general framework for Service Assurance (SA) functions, methods and activities, for further work see [9]. In this section a generalized meaning of Service Assurance is used, namely: it covers all the functions that help assuring fluent services over, for example Ethernet, managed networks.

The proposed Service Assurance framework should be considered as an umbrella, utilizing beside others Connectivity Fault Management (CFM), Performance Monitoring (PM) and SLA Verification tools, methods and metrics. The event notifications generated by these subsystems are analyzed by Fault Management FM functions, which are also part of the SA framework.

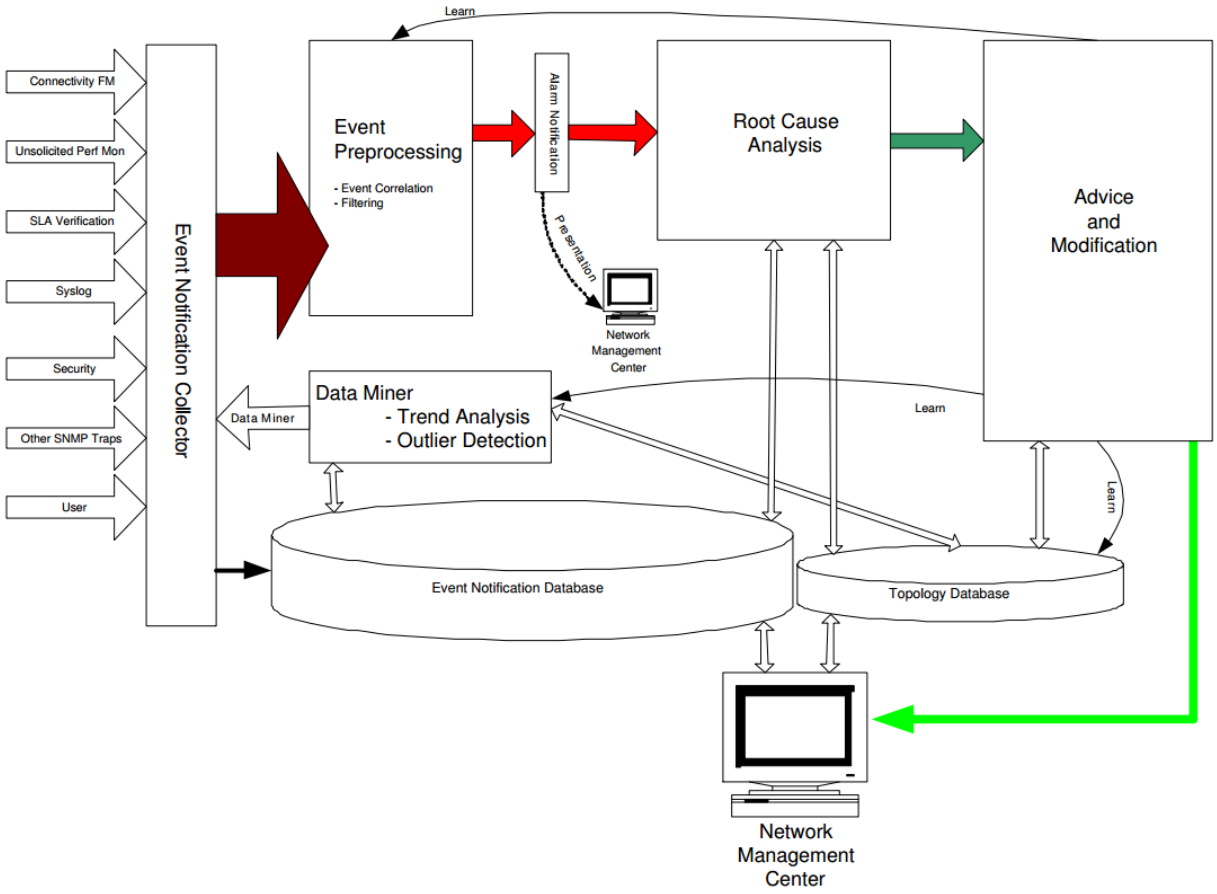

Figure 5. Connection of elements of the event processing and alarm handling model

In this framework, fault localization means the process of identifying the location of the original fault [10]. We refer to the passive filtering and correlation of events as event correlation [11]. Finally, we use root cause analysis as a more general term for finding the location of a fault, and the actual cause of this fault, utilizing regular monitoring and active investigation checks. We refer to event notifications as events, being sometimes alarming, sometimes informative. An alarm is an event with a severity over a certain threshold. Alarms must be acted upon immediately. Fault management and performance monitoring information can be collected in different manners. A classic typology distinguishes polling from push [12].

As Figure 5 suggests, events arrive to the event processing and alarm handling model from various sources. The Event Notification Collector maps these to a standard format, then sends them to Event Pre-processing and stores them into the database. The Data Miner works on the stored events (seeing more historical events as well), and generates a new event when necessary. Once the events get correlated and filtered, only those alarms get presented to the NMC (Network Management Centre), which should be acted upon. The Root Cause Analysis (RCA) for these alarms starts immediately. When

the root cause is found, a fault description gets forwarded to the Advisor Module. This decides whether the corrective actions should be taken automatically, or only the advice (and the log about the tests carried out during RCA) should be forwarded to the human operator. The operator then decides what to do and he/she is also able to check if the automatic corrections taken were appropriate. The model includes learning mechanisms as well, which are indicated in Figure 5, too.

There are two basic communication protocols for managing networks: the Simple Network Management Protocol (SNMP) [13] and the Syslog [14] protocol. The former provides a way to verify the network element configuration, read basic statistics, and also provides an alarming functionality via configurable traps and the latter is the de facto standard for forwarding log messages in an IP network.

4 Related project platforms

4.1 Arrowhead[1]

The Arrowhead project is aimed to provide an intelligent middleware that can be used to allow the virtualization of physical machines into services. It includes principles on how to design SOA-based systems, guidelines for its documentation and a software framework capable of supporting its implementations. The design guidelines provide generic □black box□ design patterns on how to implement application systems to be Arrowhead Framework compliant. Moreover, it already solves relevant issues regarding interface, protocol and semantic interoperability. As a matter of fact, one of the main challenges of the Arrowhead project is the design and development of a framework to enable interoperability between systems that are natively based on different technologies. One main objective is to achieve that, thus keeping the advantages of SOA, e.g., the flexibility obtained by the loose coupling. The strategy to meet that objective is to identify what are the least common denominators needed and select the most suitable common solutions. The Arrowhead proposed approach is shown in Figure 6.

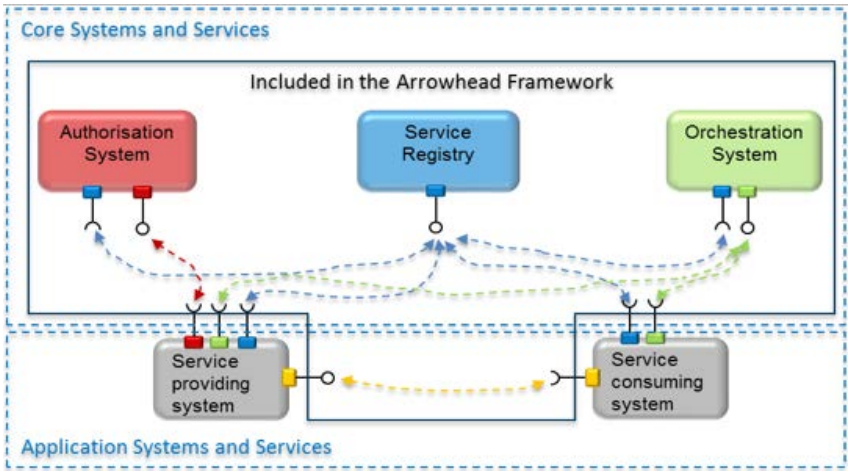

Figure 6 □ The Arrowhead framework: proposed approach

4.2 IMC-AESOP

The IMC-AESOP project is aimed to use the existing basic SOA and cloud technologies (normally used in several applications and contexts different from manufacturing production asset) and prove that they can be used to create new solutions in industrial and infrastructural environments [15]. In particular, the main idea is to take advantage by the wide dissemination of the internet-based technologies in almost all the levels of the automation pyramid (ISA-95 model) for applying the DPWS (Device Profile for Web Services □ OASIS standard) as the reference implementation technology to enable virtualization of physical entity (ex. CNC machine, robot, etc.) in terms of services. The usage of DPWS will enable cross-layer integration inside ISA-95 manufacturing enterprise model. The application of a common technology to all the levels of a manufacturing company from shop floor to business management passing through operation management is the approach used in the IMC-AESOP project to solve relevant issues regarding interface, protocol and semantic interoperability (everything is normalized according to the DPWS standard). The IMC-AESOP proposed approach is shown in Figure 7.

[1] http://www.arrowhead.eu

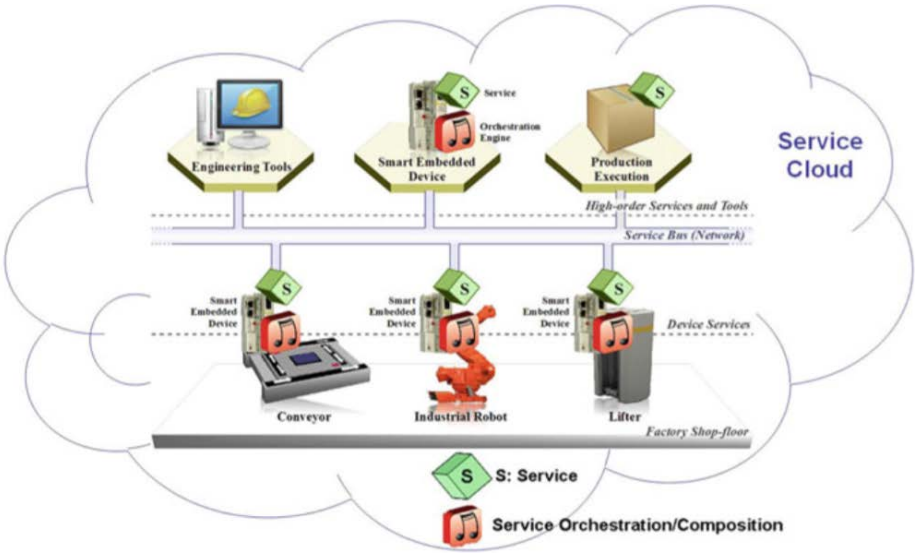

Figure 7 – The IMC-AESOP framework: proposed approach [15]

4.3 PRIME[2]

The PRIME project is aimed to design and develop new solutions for the deployment of highly adaptive, reconfigurable self-aware plug and produce assembly systems, which will use multi-agent control, dynamic knowledge sharing, integrated monitoring, and innovative human-machine interaction mechanisms. The PRIME project main result is an agent-based intelligent middleware for advanced monitoring of manufacturing production systems. Within the PRIME agent-based middleware, each physical entity (ex. CNC machine, robot, etc.) is virtualized as an agent that brings into the system a set of capabilities, i.e. provides to the others agents – that are registered into the PRIME Framework – a set of technical abilities that can be use to execute an operation [16]. The middleware also provides mechanisms to discover agents and invoke their capabilities. The communication between agents is based on the FIPA[3] standards that defines standard message exchange patterns and basic semantic. The PRIME proposed approach and architecture is shown in Figure 8.

[2] http://www.prime-eu.com

[3] http://www.fipa.org

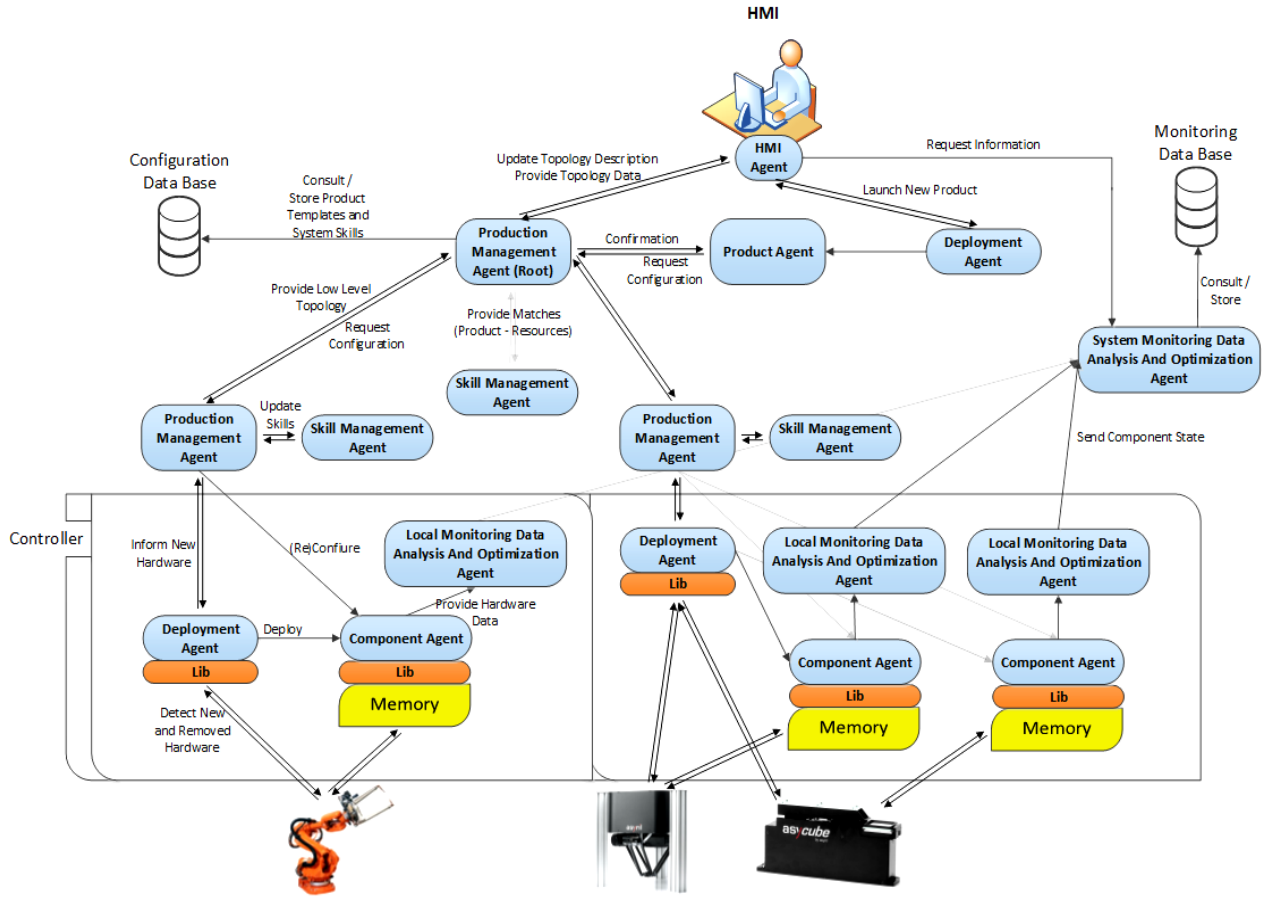

Figure 8 □ The PRIME framework: proposed approach [17]

4.4 IoT-A[4]

The IoT-A project is aimed to design and define an architectural reference model and related reference architecture for IoT systems. The IoT-A Architectural Reference Model (ARM) is an effort to handle the emergence of a variety of communication solutions and plethora of a cost-effective, rapidly evolving connected devices. In particular, the ARM enables for higher degree of interoperability between IoT applications by standardizing and characterizing the IoT domain while assuring a common understanding. The IoT-A ARM building blocks together with the typical process of using the IoT-ARM to derive concrete compliant IoT architectures are shown in Figure 9.

[4] http://www.iot-a.eu/public

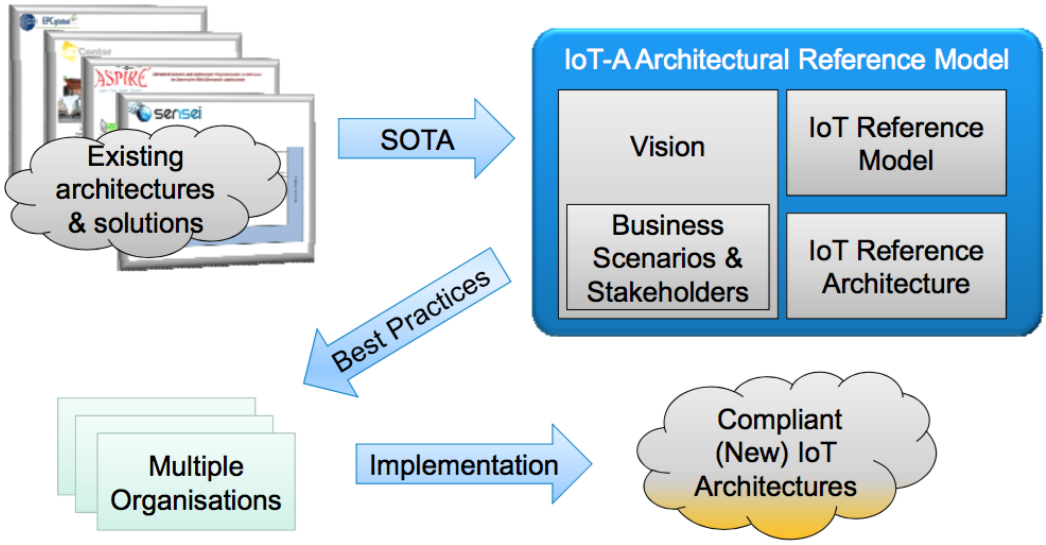

Figure 9. IoT-A architectural reference model building blocks [18]

4.5 ProaSense

4.6 IDEAS

4.7 Self-Learning

4.8 SOCRADES

4.9 MIMOSA

5 Conclusion

In this deliverable, we presented the approach of the telecom industry to system (network) management, both in the business and technical sense with the ITU-TMN model. We emphasized the importance of the actual business processes and practices when creating MANTIS elements.

Finally, we have provided a reference management system architecture that might be useful for MANTIS overall system design.

6 Related standards

- ITU-T Std. X.700, Management Framework for Open systems Interconnection (OSI) for CCITT Applications, 1992
- ITU-T: The M.3050 Recommendation Series
- ITU-T: The M.3200 Recommendation Series
- ITU-T: The M.3400 Recommendation Series
- OASIS Devices Profile for Web Services (DPWS) Version 1.1

7 References

[1] X.700 - *Management Framework for Open systems Interconnection (OSI) for CCITT Applications*, ITU-T Std. X.700, 1992.

[2] ITU-T: *The M.3050 Recommendation Series*. Available: https://www.itu.int/rec/T-REC-M.3050.0-200407-S/en Accessed: 2015. 08.21.

[3] ITU-T: *The M.3200 Recommendation Series.* Available: https://www.itu.int/rec/T-REC-M.3200/en Accessed: 2015. 08.21.

[4] ITU-T: *The M.3400 Recommendation Series.* Available: https://www.itu.int/rec/T-REC-M.3400/en Accessed: 2015. 08.21.

[5] The International Engineering Consortium: *Telecommunications Management Network Web ProForum Tutorials*. Available: http://www.hit.bme.hu/˜jakab/edu/litr/TMN/tmn.pdf Accessed: 2015. 08.21.

[6] Cisco (2009): *Introduction to eTOM.* White Paper, Available: http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white˙paper˙c11-541448.html Accessed: 2015. 08.21.

[7] J. Wen, et al. (2008): *Research on the Expanded TMF eTOM Framework and Case Study.* 2008. IEEE International Conference on Service Operations and Logistics and Informatics (SOLI), 2008. Oct., Beijing, pp. 718-721.

[8] A. Tanovic (2012): *Improvement of the eTOM standard through the comparsion with ITIL V3 best practices.* IEEE 20th Telecommunications Forum (TELFOR), Belgrade, 2012. Nov., pp. 36-39.

[9] P. Varga, I. Moldov□n (2007): *Integration of Service-Level Monitoring with Fault Management for End-to-End Multi-Provider Ethernet Services.* IEEE Transactions on Network and Service Management, Vol. 4, No. 1, June 2007.

[10] M. Steinder and A. Sethi, □*A survey of fault localization techniques in computer networks,*□ Science of Computer Programming, Special Edition on Topics in System Administration, vol. 53, no. 2, pp. 165□194, Nov. 2004

[11] G. Jakobson and M. Weissman, □*Real-time telecommunication network management: extending event correlation with temporal constraints,*□ in Proc. 4th IEEE/IFIP International Symposium on Integrated Network Management, IM□95, A.S.Sethi, Y. Raynaud, and F. FaureVincent, Eds. Chapman and Hall, May 1995, pp. 290□301.

[12] J. P. Martin-Flatin, *Web-Based Management of IP Networks and Systems*. Wiley, 2003.

[13] RFC 1098 (1990): *The SNMP Protocol*. Available: https://www.ietf.org/rfc/rfc1157.txt Accessed: 2015. 08.24.

[14] RFC 5424: *The Syslog Protocol*. Available: https://tools.ietf.org/html/rfc5424 Accessed: 2015. 08. 24.

[15] A. Colombo, T. Bangemann, S. Karnouskos, J. Delsing, P. Stluka, R. Harrison, F. Jammes, and J. L. Lastra, Eds., *Industrial Cloud-Based Cyber-Physical Systems: The IMC-AESOP Approach*, 2014 edition. New York: Springer, 2014.

[16] ESPRIT Consortium AMICE, Ed., *CIMOSA: Open System Architecture for CIM*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993.

[17] A. Rocha, G. di Orio, J. Barata, N. Antzoulatos, E. Castro, D. Scrimieri, S. Ratchev, and L. Ribeiro, □An agent based framework to support plug and produce,□ in *2014 12th IEEE International Conference on Industrial Informatics (INDIN)*, 2014, pp. 504□510.

[18] IoT-A, □Initial Architectural Reference Model for IoT,□ D1.2, Jun. 2011.