ngmn
the engine of broadband wireless innovation

A Deliverable by the NGMN Alliance

Next Generation Converged Operation Requirements Phase 1

next generation mobile networks

NGCOR

NEXT GENERATION CONVERGED OPERATIONS REQUIREMENTS

by NGMN Alliance

Version: 1.3

Date: 20 May 2012

Version:	**1.3**
Date:	**20 May 2012**
Document Type:	**Final**
Confidentiality Class:	**Public**
Authorised Recipients: (for CR documents only)	

Project:	**NGCOR**
Editor / Submitter:	**Klaus Martiny, Deutsche Telekom**
Contributors:	**T. Benmeriem, FT Orange** **A. Buschmann, Vodafone D2 GmbH** **J.M. Cornily, FT Orange** **M. Geipl, Deutsche Telekom** **M. Mackert, Deutsche Telekom** **K. Martiny, Deutsche Telekom** **P. Olli, Telia Sonera** **B. Zeuner, Deutsche Telekom**
Approved by / Date:	**NGMN Board for Publication**

Abstract: Short introduction and purpose of document

Consolidated document from all requirement documents by the sub tasks GEN; FM; InvM; CON and MT

Document History

Date	Version	Author	Changes
2011/07/18	**V 0.92**	Klaus Martiny, Deutsche Telekom Axel Heck, Deutsche Telekom	1st Distribution to partners
2011/07/29	V 0.93	Andreas Buschman, Vodafone D2 GmbH	Some small changes in the FM section
2011/11/24	V 0.94	Yvonne Doernhofer et al	First compilation of updated sections: - Chapter 1 Introduction K. Martiny / M.Mackert DT - Chapter 2 - GENERIC REQUIREMENTS (GEN) A.Buschmann Vodafone D2 - Chapter 3 - HL REQUIREMENTS for CONVERGED OPERATIONS (CON) T. Benmeriem FT Orange - Chapter 4 - REQUIREMENT MODELING AND TOOLING (MT) B.Zeuner DT - Chapter 5 - REQUIREMENT FAULT MANAGEMENT INTERFACE A.Buschmann Vodafone D2 - Chapter 6 - REQUIREMENTS FOR INVENTORY MANAGEMENT P.Olli Telia, M.Geipl DT, M.Mackert DT - Chapters 7 & 8 – REFERENCES & APPENDIX
2011/11/26	V 0.95	Yvonne Doernhofer, Deutsche Telekom	Editorial Changes
2011/11/27	V 0.959	Manfred Mackert, Deutsche Telekom	Editorial Changes and distribution for review
2011/11/28	V 0.96	Manfred Mackert, Deutsche Telekom	Editorial Changes
2011/11/30	V 0.961	Manfred Mackert, Deutsche Telekom	Update with changes and comments from: • T. Benmeriem for chapter 3 (28.11.2011 and 30.11.2011) • M. Cornily for whole document (28.11.2011) • P. Olli for chapter 6 (30.11.2011)
2011/12/02	**V 0.97**	Klaus Martiny, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Editorial Changes in chapter 6 & Internal Review & Distribution to partners
2012/01/22	V 0.98	Yvonne Doernhofer, Deutsche Telekom	Changes FM (2.02) ,GEN part (1.02), InvM part (1.21), FM use cases, Glossary
2012/01/26	V 0.99	Manfred Mackert, Deutsche Telekom	Updates: Introduction, CON, InvM part (1.25); New: chapters 8.1. & 8.2.; editorial cons.: chapter 7 and complete document; Distributed for Final Review
2012/01/31	**V 1.0**	Klaus Martiny, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Updates from Final Review & Distribution to NGMN TAC for final approval
2012/02/28	**V 1.1**	Yvonne Doernhofer, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Update: Introduction with parts of MT Req abstract, FM chapter 5.5.2, Added comment in CON chapter 3
2012/02/28	**V 1.2**	Yvonne Doernhofer, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Update chapter 1 and 5
2012/04/16	**V 1.3**	Yvonne Doernhofer, Deutsche Telekom	Update REQ-MT (6), REQ-MT (8), REQ-MT (34); Add Editor's note for chapter REQUIREMENTS FOR INVENTORY MANAGEMENT (INVM)

Contents

Figures

Tables

1 Introduction to NGMN NGCOR

The Telecommunication Market is changing faster and faster. The introductions of new technologies are going shorter and shorter. GSM, HSDPA and UMTS, well understood technologies but good examples regarding the change of customers needs, reflect the change from voice services to the usage of data services. Common to all these technologies is that the network architecture didn't change. The impact onto OSS was low.

With the introduction of LTE the requirements for OSS Capabilities and solutions changed completely. The network architecture became more flat. "Box" monitoring isn't the solution in order to deliver a high service quality to the customer. The challenge is to operate services with high quality, end to end, effectively and efficiently. Additional challenges are monitoring of the service and the introduction of new services. A shorter time to market is always requested.

But, unfortunately, the introduction of LTE as new mobile technology is not the only challenge. The convergence of mobile and fixed networks is another difficulty. The complexity of operating the network will increase dramatically.

Each operator has to consider that - in the same time - the mode of operation is changing. On one hand vendors are offering "Managed Services " and on the other hand sharing of mobile infrastructure between the operators is becoming more popular.

As a summary the challenge for each operator is to operate their networks in the context of:

- Introduction of LTE (architecture change)
- Convergence of mobile and fixed line (considering various technologies e.g. WiFi, DSL, etc.)
- Change of mode of operations (sharing options (e.g. 3GPP TS 23.251), managed services)
- Heterogeneous Networks
- Considerations of currently implemented networks (GSM, UMTS…)
- New mode of operations e.g. Managed Services, Cloud services, Cloud RAN, etc.

This forces operators to start a transformation process.

Considering that OSS solutions, interfaces and models are less standardized as detailed in the following chapter, it is not possible to efficiently and effectively run through this transformation process. Thus a prerequisite is to standardize at least the interface between the element management layer and the OSS layer and to harmonize the information models based on operations requirements.

The target architecture of each operator has to consider:

- Business processes based on industry standards (eTOM/ITIL) see Figure 1. The processes in Figure 1 are used in the project
- Standardized Interfaces
- OSS tools which are designed for operator specific demands
- OSS architecture see Figure 2

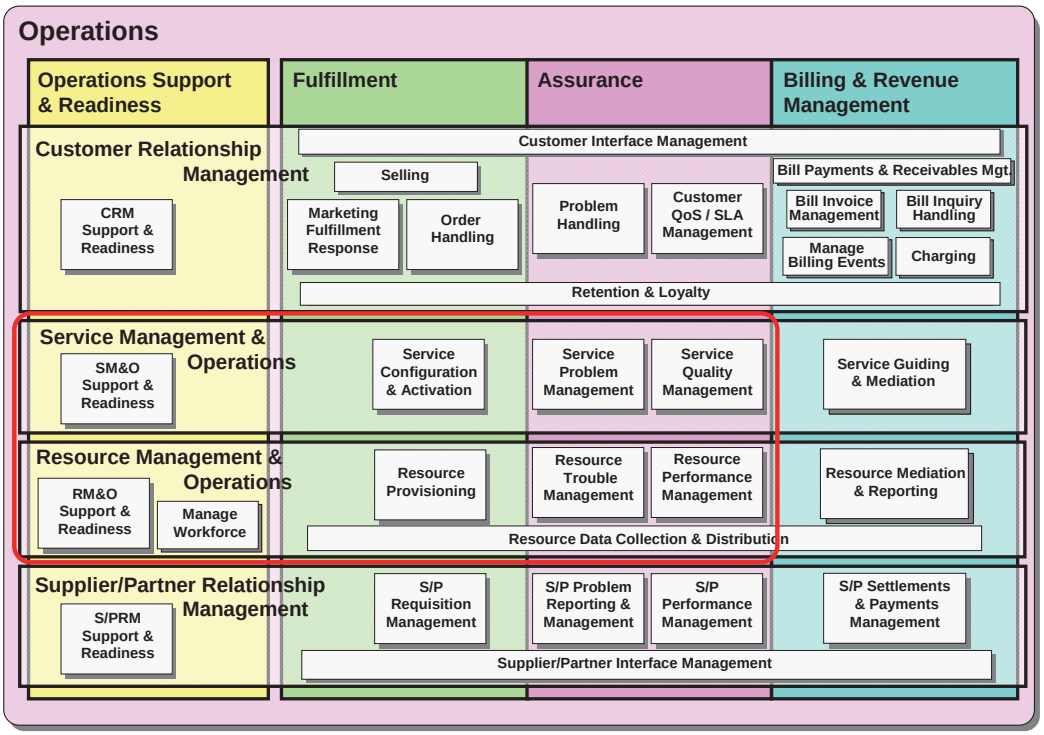

Figure 1: Business processes

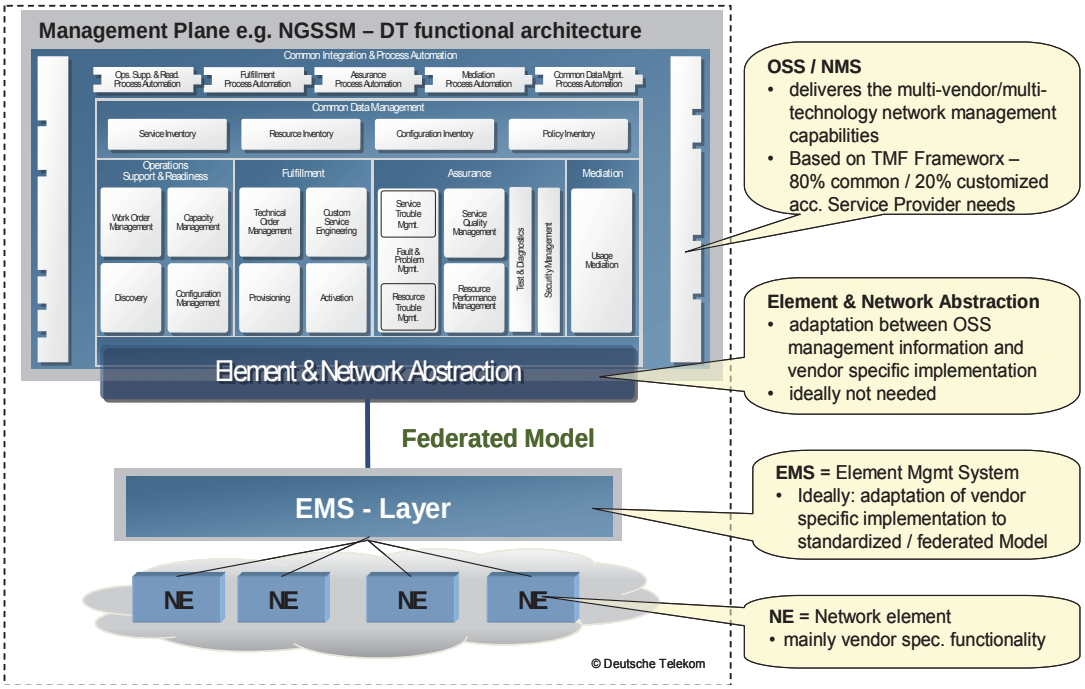

Figure 2: OSS architecture - agreed OSS Architecture: 80% based on Frameworx, 20% operator specific

Figure 3 defines the complexity of the project.

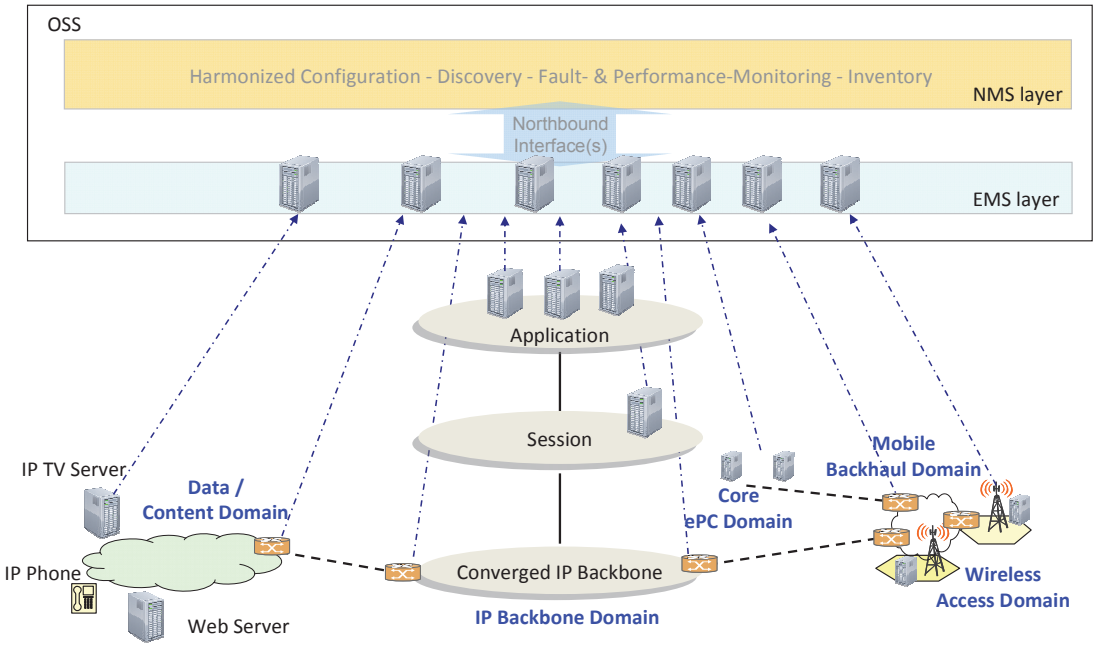

Figure 3: Operator's harmonized OSS, end-to-end network multi-domain, multi-technology management view

1.1 The current situation around standards for converged operations

3GPP WG SA5 has specified detailed Network Resource Models (NRMs) [13] for the management of mobile networks, plus a Generic Network Resource Model [9].

TM Forum has done the same for the management of various kinds of fixed networks, as well as a Shared Information & Data (SID) Model [25] providing a "common reference model for enterprise information that service providers, software providers, and integrators use to describe the network data", i.e., also generic definitions for network and service management aspects.

As a consequence the resulting models are different.

Parallel to 3GPP und TM Forum other Standards Development Organisations (SDOs) and organisations such as the Internet Engineering Task Force (IETF), International Telecommunications Union – Telecommunication Standardization Sector (ITU-T), Broadband Forum (BBF), Metro Ethernet Forum (MEF), etc., have defined different management standards/ recommendations for mobile and fixed networks.

Because all sets of specifications have been specified independently, the management of the mobile part and the fixed part is currently structured along silos with different management interfaces, information models, management architectures, and management workflows.

All these different Standards (from SDOs/ organisations) and proprietary solutions (from vendors) use different modelling/tooling, therefore the CAPEX and OPEX for network operators and integrators to integrate all these interfaces have increased dramatically. This heterogeneous modelling/tooling also has a massive influence to scalability, time to market, complexity, and applicability of these standards in OSS.

The convergence of mobile and fixed networks requires the convergence of the mobile and fixed OSSs.

1.2 The NGCOR Project and its Objectives

The Next Generation Converged Operations Requirement (NGCOR) project is approved by the board of NGMN.

The project is a continuation of the projects SON and NGMN Top OPE Recommendations from 2010. SON was focused on radio capabilities of a mobile network, NGMN Top OPE Recommendations specified operations requirement for mobile networks.

Converged operation is one key issue for each operator and service provider because the services will be delivered via a common infrastructure. There is no differentiation which platform (wireline or wireless) is delivering the service.

The current situation is caused by the fact that OA&M capabilities for wire line and wire less network elements are implemented by various different not harmonized standards or aren't standardized at all. Results are huge invests, high operational cost and slow time to market. The expected results from a standardization and unification of interfaces and information models are reduced OPEX and CAPEX and significantly shortened time to market. Without a higher grade of standardization an optimization of commercial figures isn't possible.

The results of both activities are considered in the NGCOR project since these results are essential for the converged management of a next generation mobile networks.

NGCOR is an enhancement of OPE because NGCOR details specifications of operations requirements for both wire line and wireless networks. It is obvious that both networks will be merged in the near future. NGCOR is describing requirements for converged operations. It is not the intention to specify the convergence of wireline and wireless networks.

There is a need to define converged OA&M requirements to ensure that the operational activities within the converged networks perform optimally. The project has the claim to give guidance to SDOs and industry bodies (e.g. 3GPP or TM Forum) in order to prioritize the work. Developing solutions for the most important requirements is the first and specifying the recommendations for the best solutions is the second target.

"An increasing number of service providers (SP) have to operate a variety of network and service production infrastructures, from mobile and fixed network environments up to converged networks and services across many countries. The increasing demand to maintain and improve customer experience requires full end-to-end service management and hence, multi-technology and multi-vendor network management capabilities. On the other hand, financial downturn has put even more pressure on operational efficiency improvement."
[Source: Deutsche Telekom (DT), France Telecom (FT), Vodafone (VF), BT, Portugal Telecom (PT)]

1.3 Expected benefits and commercial Impact

Currently Operators yearly spend millions of Euros for the adaptation and integration of the element managers with the OSS layer. The commercial impact is huge; from CAPEX- and OPEX-point of view, from an effort point of view to maintain the processes that are - caused by a low level of standardization - more complex as needed, and also from lost revenue due to long time to cash for new services.

One of the most significant changes in software development and procurement practice over the past decade is the greatly increased emphasis being placed on building O&M systems incorporating COTS software in order to keep overall development and maintenance costs as low as possible. Source of COTS software are the

equipment vendors and OSS vendors who can supply off-the-shelf or COTS components that can be plugged into a larger software system to provide capabilities that would otherwise have to be custom built.

The rationale for building OSSs based on standardized interfaces and COTS OSS components is that they will involve less development time by taking advantage of existing, market proven, vendor supported products, thereby reducing overall system development costs and time to market for new services.

Having implemented the NGCOR project's main goal - the standardization of the interfaces between the element management layer and the OSS layer and the harmonization of the information models - a cost reduction of up to 70% is achievable. Not to mention the reduction of effort to maintain the OSS landscape and the reduction of process time.

The estimation of the savings from this way of system development and integration considers costs such as

- Requirements definition,
- Effort needed to understand and select the COTS software,
- Pre-integration assessment and evaluation - standardized and vendor specific,
- Design, code, test design and test - standardized and vendor specific,
- Post-integration certification of compliance with mission critical or safety critical requirements,
- Licensing and royalties and
- Software maintenance.

Savings are rapidly growing in a multi domain and multi vendor environment with a massively reduced number of integration points.

> Vodafone estimates that after the TM Forum Interface Program's RAM interface is adopted by the industry, it will save up to 68 percent in integration costs compared with vendor-specific integration.
>
> *TM Forum Case Study Handbook 2012*

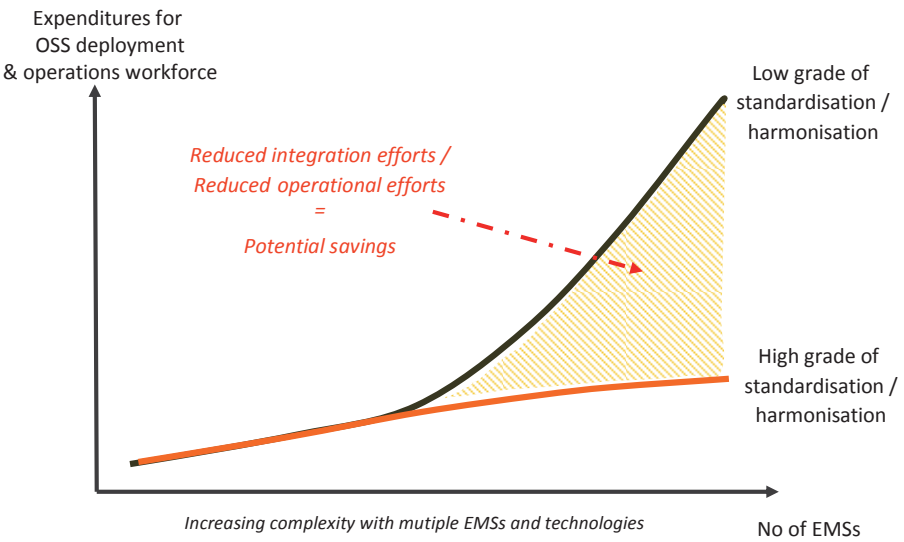

Figure 4: Savings through Interface standardisation and Information Model harmonisation

1. Benefits from converged Fault-Management process

- reduced OPEX and improved service quality through improved fault qualification
- reduce time & efforts for network diagnosis, repair, extension and swap
- enable cross domain fault correlation and RCA
- shortened network outage time

2. Benefits from converged process for Inventory Mgmt. / Discovery / Reconciliation

- avoid time-consuming manual data collection process to represent “the truth” (Manual audits and commissioning are leading cause of rollout delays)
- Streamlined planning and decision making through complete and real-time visibility of multi-vendor / multi-technology network infrastructure
- reduce the no of “stranded” assets & circuits and costly investments
  RHK study: Typical Capacity Utilization is less than 70% (RHK),
  Recent Tier I audit: 16% of all routers in inventory were de-commissioned, redeployed, or non-existent
- faster time to market for new services
- avoid inflated maintenance charges from key hardware vendor, based on inaccurate installed base view (purchase records vs. actual ‘in use’ inventory)
- a proper inventory data base is a prerequisite for financial processes. Like depreciation, warranty management, etc. The management of financial processes based on proper inventory is crucial for each operator.

1.4 Methodology

The methodology applied to derive and deliver business requirements in NGCOR is relying on a requirements life cycle.

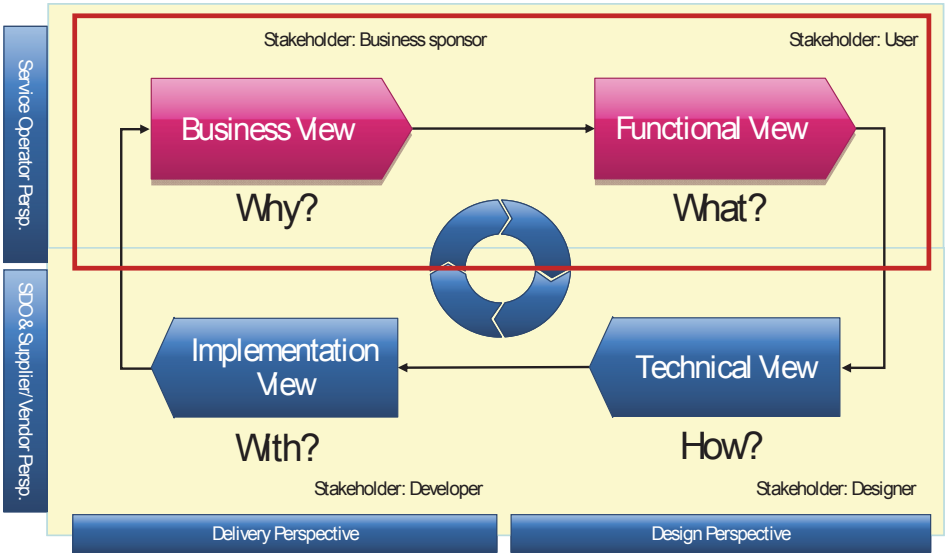

Figure 5: Requirements life cycle adopted in NGCOR & NGCOR focus area

Two responsibility areas / perspectives are defined in this life cycle:

- Service Operators perspective - focussing onto the business & functional view
- SDOs & Organizations - focussing onto the technical & implementation view

with a clear split between the service operator's perspective and the SDO & standardization perspective.

The requirements delivered by the NGCOR project are based on the business view (Why?) and the functional view (What?) of the lifecycle. The implementation and technical view isn't in the scope of the project.

The NGCOR requirements aren't independent from each other. The understanding how they are linked to each other is defined in the "business pyramid". The pyramid is shown in Figure 6: Business pyramid (general view).

- Business scenarios are the basis for architecture scenarios
- Inventory management is the common information base for the FCAPS processes
- For each process use cases are developed which are the basis for the requirements
- Inventory Management has a link to all Operations Processes

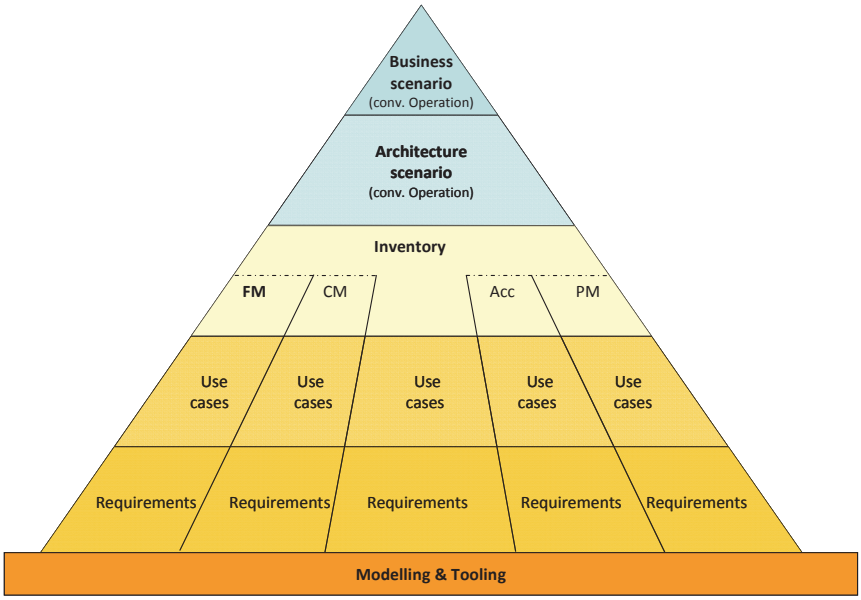

Figure 6: Business pyramid (general view)

The use cases are based on a template derived from the use case template defined in ITU-T M.3020 Management interface specification methodology.

Usage Scenario Id	<US_<SDO>_DDD_N>
Usage Scenario Name	
Summary	
Actor(s)	
Pre-Conditions	
Begins When	
Description	<Step 1> <Step 2> … <Step n>
Ends When	
Post-Conditions	
Exceptions	Put a reference here to a document or a separate table which lists all the exceptions. Specific exceptions will be explicitly listed in the Description clause.
Traceability	Hyperlinks to the associated requirements

where:

- <SDO> denotes the SDO / organisation
- DDD denotes the specification
- "N" is a 4 digits integer (e.g. 0012).

1.5 Project scope

The answer to the question "what is in and what is out of the project's scope" is highlighted in Figure 7

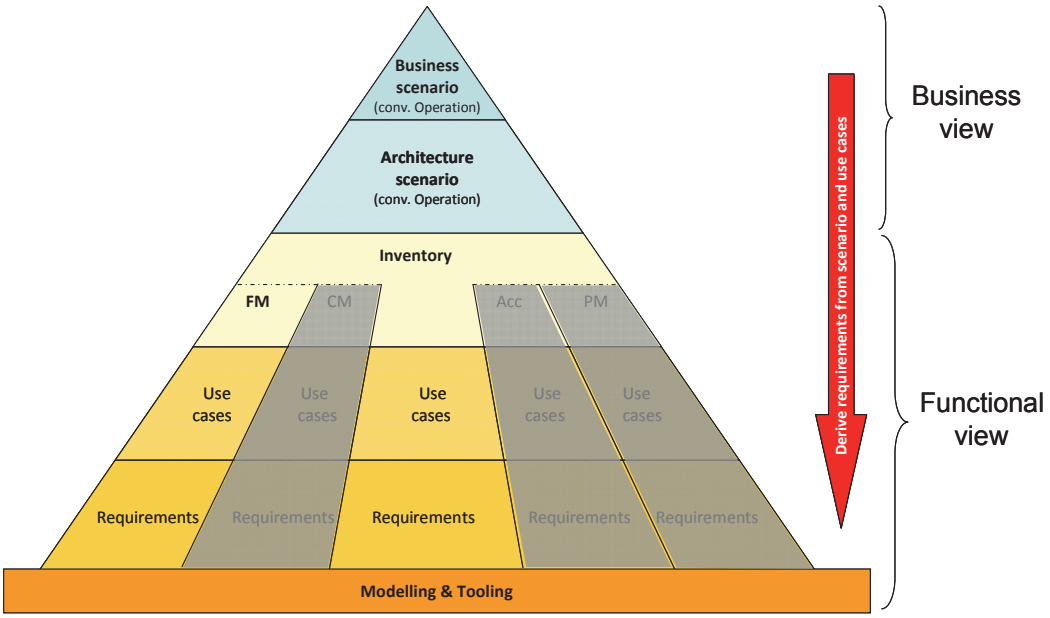

Figure 7: Business pyramid (specific view)

The requirements built up in the NGCOR project are derived from use cases that themselves are triggered by **Business Scenarios** and **Architecture Scenarios** which are described in Chapter 3 - High level requirements for Converged Operations (CON).

Base for the standardisation processes are the definitions which are described in the **Modelling and Tooling** chapter and that should give guidance to SDOs/organisations and industry bodies (e.g. 3GPP or TM Forum) in order to prioritize the work.

In general the operations tasks of service providers are well described and defined as a part of the ISO Telecommunication Management Network

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

together well known as FCAPS.

The project in its actual shape is focussing on the management domains **Fault Management** and **Inventory Management**.

1.6 The NGCOR document structure

The next chapters in this document are structured as follows

- Chapter 2 - Generic Next Generation Converged Operational Requirements (GEN)
- Chapter 3 - High level requirements for Converged Operations (CON)
- Chapter 4 - Requirements for NGCOR Modelling and Tooling (MT)
- Chapter 5 - Requirements for Fault Management Interface (FM)
- Chapter 6 - Requirements for Inventory Management (InvM)
- Chapter 7 - References
- Chapter 8 - Appendix with Glossary and Abbreviations and a summary of the NGCOR Requirements and their Addressees

2 Generic Next Generation Converged Operational Requirements (GEN)

2.1 Introduction

The GEN section contains the generic part of the Next Generation Converged Operational Requirements (NGCOR), which are valid for all other specific NGMN NGCOR sections. The intention of the GEN section is to avoid redundant requirement descriptions in different NGMN NGCOR sections.

2.2 Scope

Generic requirements for interfaces in the OSS domain.

2.3 Methodology

Explanation of Prioritization

Essential	→	The standard must fulfil this requirement. It is absolutely necessary and indispensable.
Major	→	The standard should fulfil this requirement. This is an important requirement. The value of the standard is reduced, if it cannot be fulfilled.
Minor:	→	The standard can fulfil this requirement (but must not). This is an optional requirement.

2.4 Non-Functional Interface Requirements

The following topics describe core business driven requirements for interfaces in the OSS domain. The following figure provides the overview.

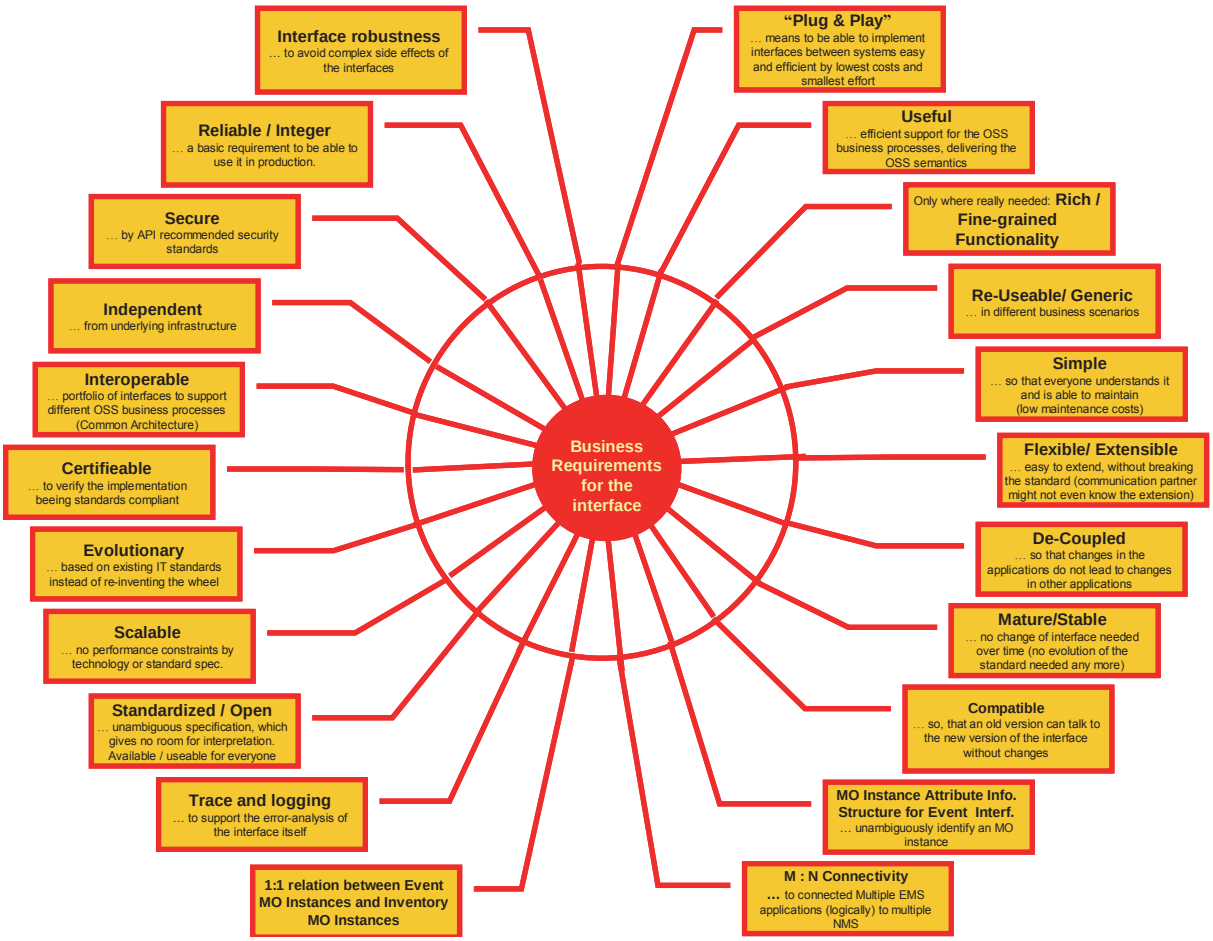

Figure 8: Business requirements for the interface

"MO Instance" Attribute Information Structure for EMS ←→ NMS Event Interfaces

REQ-GEN (1) "Plug & Play"

It must be possible to implement the interfaces between the OSS easy and efficient by lowest costs and smallest effort (ideally without any development and/or configuration). The standard specification must enable "Plug&Play" (e.g. by unambiguously defined interface capabilities)

- Comment: Backward compatibility (see related REQ-GEN (13)) is one major prerequisite to support this characteristics during the whole life-cycle of the standard interface (e.g. plug & play must be still possible, if the client of the interface uses version 1.0 and the server uses version 1.2 of the same interface specification)
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (2) Useful

It must deliver efficient support for the OSS business processes. The standard specification interface must deliver the needed OSS semantics to support the process.

- Implementable (not academic) support of business process frameworks (e.g. eTOM and ITIL, or other process frameworks) and common information models (e.g. SID semantic, or information models from other SDOs)
- Clear and unambiguous scope of the interface (e.g. to differentiate from Service Inventory), without mixing different business scenarios (e.g. an interface which supports Resource Configuration Management should not be mixed with a Resource Fault Management Interface, because this might lead to complex interface specifications and expensive implementations)

Priority: Major

REQ-GEN (3) Re-Useable/ Generic

The standard interface specification must be generic enough, to enable the re-use in different integration scenarios.

(e.g. NMS - FM offers a standard interface for communication with other NMS such as trouble ticketing)

- This is a prerequisite to support M : N integrations and to reduce cost and effort for integrations
- Extensions in future versions will not hinder to implement it in a generic way and will not hinder to re-use (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Essential

REQ-GEN (4) Simple

The standard interface specification must be simple (that means: the interface should offer only really necessary capabilities), so that people which have not been involved in the specification are able to understand it (or even do not need to understand the details), so that they are able to implement, maintain and use the interface.

- This will help to reduce cost and effort for the implementation and the operation/maintenance of the interface.

Priority: Essential

REQ-GEN (5) Flexible/ Extendible

The interface can be extended and refined, from basic setup to more complex implementations without impact on the other communication partners. It must be possible to extend the interface capabilities (methods and attributes), without breaking the standard. The standard interface specification must enable this capability to deliver standard compliant flexibility and extendibility.

- It must be possible to use a very simple, basic setup of the interface-implementation on one side of the communication partners, and a more complex interface-implementation on the other side of the communication partners (which contains the "simple" interface-implementation as the basic core) without disturbing the communication. That means, that there is a stable basic core, which can be extended and optionally used, but there is no dependency on all communication partners to use the extensions (as long as it is not part of the common standard itself).
- (The communication partner might not even know the extension, e.g. the server uses extended attributes, while only a small number of clients are aware about the extension → The interface still works as specified, without any impact on the clients which do not know the extension.) (Proposed solution: This will be supported by modular applications. A common module should be applied to all systems. Any specific requirements (customer or system specific requirements) should be expanded in separate modules without changing the generic/common module)
  (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

<u>Rationale</u>

- Avoid strict coupling of server and client. But, at the same time, enable complex interactions, to support complex Network behaviour.
- This capability can be used to implement new versions with extended capabilities without loosing backward compatibility.

Priority: Major

REQ-GEN (6) Fine grained (as far as needed)
Means: Focus on using valid Use case to motivate the interface design. In such case, the standard Interface specification will be of the correct grade of grain.

Fine grained functionality ONLY where really needed and absolutely necessary to support the common basic process. Adding more and more capabilities into the standard interface specification will lead to complex and expensive implementations (which often hinders the adoption of the interface) and might lead to a dilution of the scope of the interface and overlapping functionality with other interfaces.

- Fine grained/ rich functionality must be delivered in specific areas to address e.g. technology specific requirements (e.g. in case of Resource Configuration Management)
- BUT: consideration of the richness to support the business process in an appropriate way vs. business benefit for all standard interface implementers.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (7) Standardized/ Open

The requirement means, that we need an "unambiguously standardized specification" without room for interpretation (which usually hinders Plug & Play, s.o.). This standard can be an existing specification or a new one. NGMN-NGCOR will not specify any standard. The specification and everything needed to make use of the standard (e.g. appendixes to the specification-document which are not part of the document itself, etc.) must be freely available and useable for everyone.

- This is a prerequisite to enable compatibility between interface implementations of different vendors.

Priority: Essential

REQ-GEN (8) Mature/ Stable

The standard interface specification must be stable and mature, to avoid expensive changes on implemented interfaces.
(Ideally there is no requirement for change on the standard interface specification any more).

- Prerequisite: The standard interface specification has to be fault–free before it is released to the market.
- This helps also to avoid backward incompatibility by avoiding continuously changing interface specifications.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (9) De-Coupled

Changes in the application or in the interface implementation at one of the communication partners may not lead to the need for changes in the application or in the interface implementation of the other communication partners. (Please consider that this requirement does not assume any specific type of implementation technology.) The standard interface specification must enable this capability.

- This is a prerequisite to ensure that changes in one OSS will not impact other OSS, to avoid dependencies between OSS applications which might lead to high costs for the impacted communication partners and to enable M : N integrations.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Essential

REQ-GEN (10) Evolutionary

OSS standard interface specification shall re-use already existing, widely adopted and mature IT standards (e.g. transport protocols) to avoid "reinventing the wheel".

- This will reduce cost and effort to create and to implement new technologies.

Priority: Major

REQ-GEN (11) Independent

The interface standard specification must be independent from underlying infrastructure. The standard must be agnostic to the implementation-platform (e.g. the standard may not rely on capabilities of a specific Operating System).

- This will allow to re-use the same interface implementation in different environments, without dependencies on vendor specific capabilities, (e.g. the specification has to be independent from hardware, operating system bus environment, etc.) to avoid costs for the customization of interface implementations due to environmental dependencies of the specification.

Priority: Essential

REQ-GEN (12) Certifiable

The Interface must be specified in a way that makes it technically possible to validate an implementation compliancy. Beside of that, the standard should include a mechanism to certify the standard compliancy of the interface implementation

- This will allow the verification that the interface implementation is compliant with the standardized interface specification to avoid compatibility problems between interface implementations of different communication partners.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (13) Compatible

It must be possible to implement a new version of an interface specification at one of the communication partners while the other communication partners still use an old version of the interface specification. This "mixed versions" of interface implementations can be used without any impact on the communication partners or the interface implementations of the communication partners. The standard interface specification must enable this capability.

- The implementation of the new interface version at one of the communication partners must ensure the compatibility with the former version of the interface specification.
- This will allow to implement new interface versions in a productive environment without the cost and effort to upgrade all other communication partners (a real business need might lead to the upgrade sooner or later, but this can be decided by the owner of the "old" communication partner itself. Immediate upgrades are often difficult or simply impossible).
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Essential

REQ-GEN (14) Interoperable

The interface implementation shall be based on an interoperable portfolio of standard interfaces/ interface specifications to support different dynamic and configurable OSS business workflow and processes using a common architecture and a common information model. The standard must enable this by delivering the standard portfolio of interfaces and interface specifications

- This will allow the implementation of complex business scenarios, spanning different integrated OSS applications, using a common, well known interface environment without complex mapping of information models.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (15) Scalable

The standard interface specification must be able to be enlarged to accommodate a growth of traffic.

- The interface specification must enable the accommodation of traffic growth
- The specification or the selected implementation technology may not result in performance issues.

Priority: Essential

REQ-GEN (16) Secure

The standard interface specification has to be able to ensure confidentiality, integrity and availability of the data, which is transferred by the interface.

Priority: Depends on the type of the interface

REQ-GEN (17) Reliable

The interface implementation has to ensure the reliability of the data, which is transferred by the interface. The standard interface specification must enable this capability.

- This is a basic requirement to be able to use an interface in a productive environment.

Priority: Essential

REQ-GEN (18) Interface Robustness

No interface dependencies on availability between NMS and EMS if one of the EMSs (Server) communication partners is not available. The standard interface specification must enable this capability.

Description

- An outage of one or more EMSs (source) may not lead to any impact on the connectivity between NMS and other EMSs.

Rationale:

- Avoid complex behaviour of the interfaces. The interface to the remaining EMSs must still be available during the time then one or more EMSs are down.

Priority: Essential

REQ-GEN (19) Simple Trace and Logging

The standard interface specification must deliver a simple "trace and logging" functionality (in readable text format).

Description

- The standard interface specification must allow logging of all commands (send, receive, query, etc.), including the content in simple, human readable text format (no hex or binary, etc.) to support the error-analysis of the interface itself.
- The logging/tracing functionality is configurable.
- The level of details can be configured
- All attributes of the content can be used as to configure trace– masks
  - Masking of attributes
  - Masking of attribute- content
  - Logging of interface problems/ errors

The standard should define a technology neutral log (perhaps much simpler than standard COTS products) and then map this simple log to various technologies (to be implementation neutral)

Rationale:

- The goal is to enable the operator/administrator to restore a connection problem on the interface very quickly.

Priority: Essential

REQ-GEN (20) 1:1 Relation between Event MO Instances and Inventory MO Instances

Description

- If MO identifiers used/provided by the inventory component of an Element Manager need to be mapped to meet naming requirements of the inventory database, the same mapping must be applied to the MO identifiers in the event. The corresponding is true if mapping is driven by event naming requirements.
- If MO identifiers of events and inventory within an Element Manager are different, the difference must be eliminated before the above mapping can be applied.

Rationale

- MO identifiers used in Event Management Interface and used in Inventory Management Interface must be identical if they are used to identify the same MO instance. The intention of this requirement is just to avoid, that the EMS uses a different NE name for the interface to NMS-Inventory/Config as for the FM interface. This will help to ensure that there is no misalignment of NE-name between NMS-Inventory/Config and the NE-Name used in the EMS –Alarm.

Priority: Major

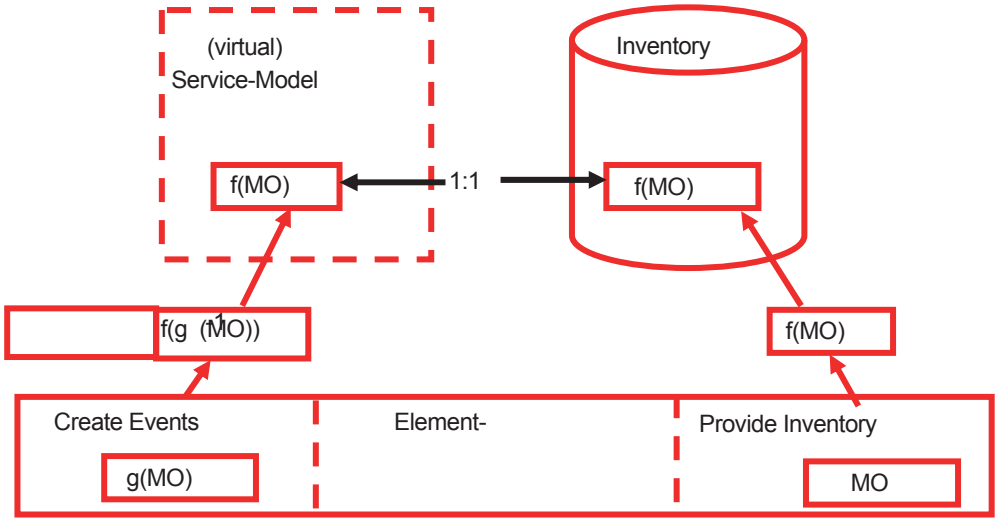

Figure 9: Managed Objects in the Context of Service Model and Inventory

REQ-GEN (21) "MO Instance" Attribute Information Structure for EMS ←→ NMS Event Interfaces

Description

MO Identifiers carried or used across the Interface (e.g. used in protocols or used in models) must unambiguously identify an MO instance (that is a representation of HW, SW or any other entities as the case may be). The main goal of this requirement is to ensure a clear identification of the entity, by avoiding complex object structures, which usually drive complexity and costs/effort to implement the interface without real additional benefit.

- The managed object, as an attribute of the event – object, shall not contain any detailed topology information. The assumption is that the NMS will use an inventory database (internal or external) to map between Managed Object Instance and inventory topology tree if needed.
- The basic assumption for this is that there is a one-to-one mapping between Managed Object Instance and the inventory information, so that the instance can be unambiguously identified. If this is not the case, the instance must contain a very simple and standardized methodology to describe the relationship between the first unambiguously identifiable object and the related not-unambiguously identifiable object, which is the originator of the event. One illustrative example to "If there is no one-to-one mapping". Let's assume we get a port – alarm. The port identifier might not be unambiguous (just "Port_1". Different NE's [e.g. Router] might also have Port 1). Therefore, there must be additional information in the identifier, which shows the relationship between this port and the unambiguous NE identification where the port is located. Example: Router_XYZ<->Port_1 (assuming that "Router_XYZ" is an unambiguous identification)
- NMS requirement (specific for the NMS layer): As soon as the event information leaves the area of Service Provider 1 (e.g. Network Provider 2 needs that information as well) and (assumption) the Managed Object attribute value does not deliver unambiguously any more, The Network Manager will add additional information, the "NameSpace" - string to the Managed_Object_Identifier attribute (Proposal: Company_Name + Technology-Domain → "Access"), so that it is unambiguous in the larger context again. (Remark: The name of the EMS should be part of the "additional information" attribute, and not part of the MO_ID)
- So the structure must be as simple as possible. Here the **illustrative proposal** for a general proposed structure of the "Managed Object Instance" attribute:
  Managed Object Instance::= <NameSpace.>*<MO_Name> <;MO_Detail>*
  NameSpace::=<Global IdentifierString> (see NMS Requirement above)
  MO_Name ::= <Ressource_Name>|<Inventory_Name>
  The Ressource_Name is delivered by the Ressource or the EMS itself.

Example:

- Inventory_Name::=<Hostname>|<Service>|<Serviceelement>|<ResourceGroup>|<UseCase>|<UseCaseSubtype>| ...
- MO_Detail ::=<Blocknn>|<Racknn>|<Slotnn>|<Portnn>|<IP_address>|…
  (The MO_Detail information is delivered by the resource or the EMS itself. It adds information about the detailed origin of the alarm as far as this is known by the resource or the EMS. There is no limit on the number of topological elements, but it should be limited to an absolute minimum, just to the number which is really necessary to unambiguously identify the defective component.

Priority: Major

REQ-GEN (22) M : N Connectivity

Multiple EMS applications might be connected (logically) to multiple NMS applications (M : N)

Description

- The standard interface specification allows connecting multiple EMS to multiple NMS. (This might have an impact on addressing – mechanisms in the interface-implementation).

Rationale

- This capability allows reducing the effort for the maintenance of several different server- side interfaces.

Priority: Major

2.5 Use Cases

The related Use Cases are covered in the REQUIREMENTS FOR FAULT MANAGEMENT INTERFACE (FM) Please consider that not all requirements are related to a specific Use Case in this document, because some of them are business requirements without a concrete technical implementation (e.g. generic requirements, like “Standardized”, “Mature”, “Useful”, etc…).

3.1 Introduction

This section aims at capturing high level requirements for converged operations. The chosen methodology is:

1. Identify Business Scenarios of high interest to operators (as real use cases) from converged operations perspective;
2. Describe basic architecture scenarios as illustrations of where convergence is of high interest for operators. Hence this description is based on any formal / recognized template. It is a free description;
3. Derive, from aforementioned basic scenarios, combined architecture scenarios, i.e. combinations of two or three basic ones. Hence this description is based on any formal / recognized template as well;
4. Describe the Business Converged Operations Scenarios according to ITU-T use case template and map them on either basic or combined architecture scenarios in order to demonstrate the benefit from the converged operations perspective;
5. Extract high-level requirements relative to convergence at three possible levels: Element Management System, Northbound interface, Network Management System;
6. Identify the expected benefits in terms of CAPEX / OPEX reduction.

Target Business Scenarios:

In this release, we are focusing on three Business Scenarios we are considering of high interest to operators and with high priority as well. This list of Business Scenarios will be extended in a new release.

Business Scenarios	
Business Scenarios within a Single Operator Environment	Business Scenario 1: Element Management System (EMS) Shared between Operators' Affiliates
	Business Scenario 2: Network Management System (NMS) Shared between Operators' Affiliates
Business Scenarios within Multi-Operator Environment	Business Scenario 4: RAN Sharing

Target audience:

This section focuses on three main cost elements on which substantial savings can be achieved. Consequently, depending on where potential savings are achievable, the requirements are addressed to three types of players:

Where convergence is expected	Whom requirements are addressed to
Element Management System	Telecom Equipment Manufacturers
EMS northbound interface	SDOs
Network Management System	OSS vendors, IT integrators

The ultimate objective of operators is to lower their CAPEX and OPEX in network operations. Main levers to achieve this are:

- Convergence at system level and/or interface level, on which this section focuses;
- Automated operations. This can be achieved e.g. by introducing self-management concepts in operators' OA&M / OSS solutions (cf. SON with 3GPP and ETSI Industry Specification Group (ISG) for Autonomic Future Internet (AFI)).

Main focus in RAN (Mobile Network) management in the Business Scenarios

From architecture point of view, RAN NEs have wireline connections and, as such, shall be managed as fixed NEs too. However, if we take the example of LTE NEs (eNodeBs), our main focus is on the management aspects of RAN features only. For the wireline connections b/w eNodeBs and the EPC NEs, we focus on the higher layers (S1-MME, S1-U, etc.) rather than on IP level aspects.

3.2 Scope

Referring to the **eTOM Business Process Framework**, requirements identified in this section focus on the process area named "Operations", which covers the core of operational service and resource management. Within the operations process area, the recommendations made in the current section focus on the following functional process groupings:

- Horizontal:
  - Resource Management & Operations
  - Service Management & Operations
- Vertical:
  - Operations Support & Readiness
  - Fulfilment
  - Assurance

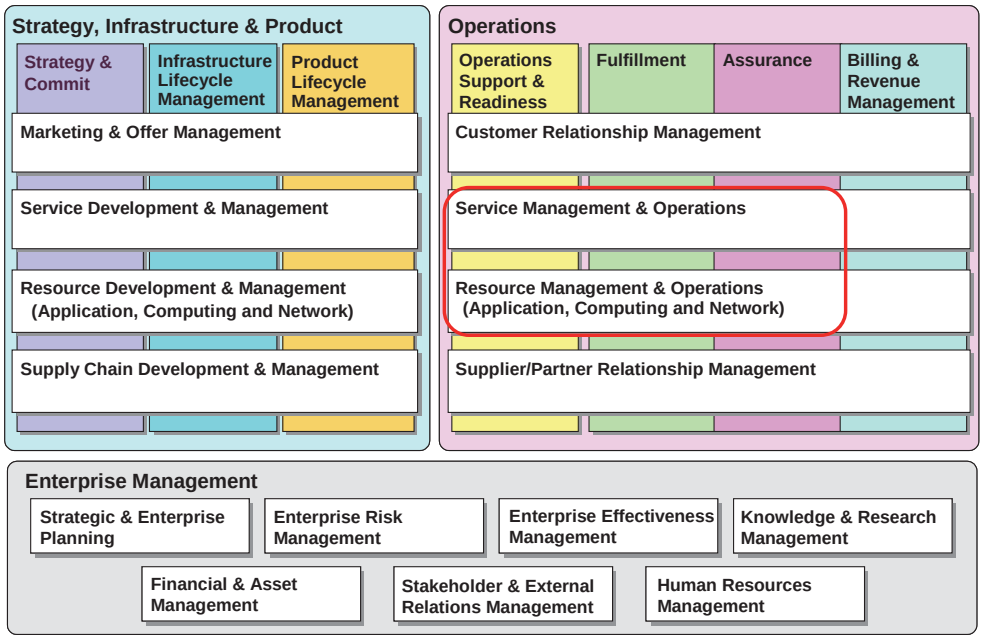

Figure 10: Scope of NGCOR within the eTOM framework

Regarding the Mobile network part (RAN) we are considering in the scope, indeed, RAN NEs also have wireline connections and, as such, shall be managed as fixed NEs too. However, our main focus in this Section, is on the management aspects of RAN features (eNodesBs in LTE for instance). For the wireline connections between eNodeBs and the EPC NEs, we focus on the higher layers (S1-MME, S1-U, etc.) rather than on IP level aspects. The whole management aspect of RAN, so called Mobile Backhaul (Mobile nodes as well as their wireline connections) is in the extended scope of this section.

3.3 Architecture Scenarios for Converged Operations

3.3.1 Basic Architecture Scenarios

This section describes "basic converged operations architecture scenarios" which constitute building blocks for elaborating combined architecture scenarios (cf. Section 3.3.2).
This Basic Architecture Scenarios family is broken down into 3 types of scenarios from methodology point of view:

- ***Current Architecture Scenario*** as starting point towards the Target Scenario within a migration path
- ***Intermediate Architecture Scenarios*** paving the way to the Target Architecture Scenario
- ***Target Architecture Scenario*** as ultimate goal of the migration process

3.3.1.1 No Convergence Architecture Scenario (Current Scenario)

Description

In the “no convergence” architecture scenario, convergence does not exist at all, either at the Element Management Layer, or at the EMS Northbound interface (NBI) or at the Network Management Layer, as illustrated in Figure 11. This architecture scenario is characterized by:

1. Element Management Systems are dedicated to specific network technologies/ domains/ regions, e.g. the operator’s LTE EMS is different from its 3G EMS, the operator’s EPC core network EMS is different from its IP backhaul EMS;
2. EMS northbound interfaces are specific to network technologies/ domains. Typically, they can be based e.g. on 3GPP IRPs for mobile network domain EMSs and on TMF interface programs for wireline domain EMSs;
3. Operator’s OSS applications are dedicated to network technologies/ domains/ regions and OA&M functional areas. For example, for legacy reasons, it may happen that the network operator has got one OSS application for fault management of its 2G network, another OSS application for fault management of its 3G network and yet another OSS application for fault management of its IP backhaul network.

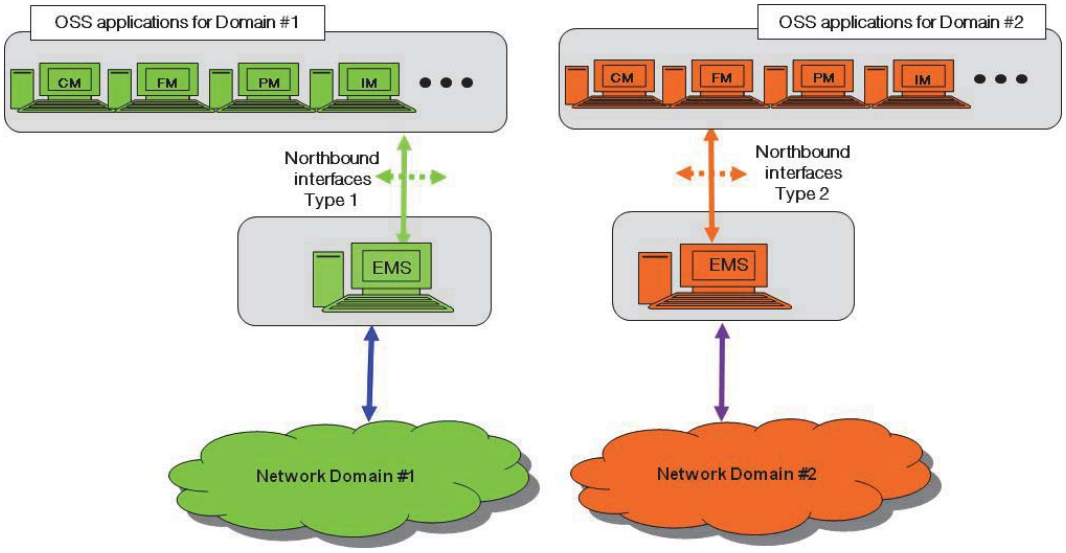

Figure 11: Basic Converged Scenario: "No convergence Architecture Scenario" (Current Scenario)

3.3.1.2 Converged Network Management Layer (Intermediate Scenario)

Description

In this scenario:

1. Element Management Systems are dedicated to network technologies/ domains/ regions, e.g. the operator LTE EMS is different from its 3G EMS, or the operator Radio Access Network is different from its IP transport network layer EMS;
2. EMS northbound Interfaces are specific to a given network technology. Typically, they are based on 3GPP IRPs for mobile network domain EMSs or on TMF interface programs for wireline domain EMSs;
3. Convergence has been achieved at the Network Management Layer: the operator has common OSS applications for multiple network technologies/ domains/ regions, for specific OA&M functional areas, e.g.:
    a. One single OSS application for fault management, covering all network domains/ technologies;
    b. One single OSS application for performance management covering all network domains/ technologies;
    c. Etc.

Important:
If the Northbound interface convergence is one aspect of high interest for operators, we need to point out through this scenario that, it is not the only one. CAPEX and OPEX savings are expected from NMS convergence and this is a requirement to OSS vendors and IT integrators.
In order to make it happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the two parties: operators and OSS vendors and IT integrators.

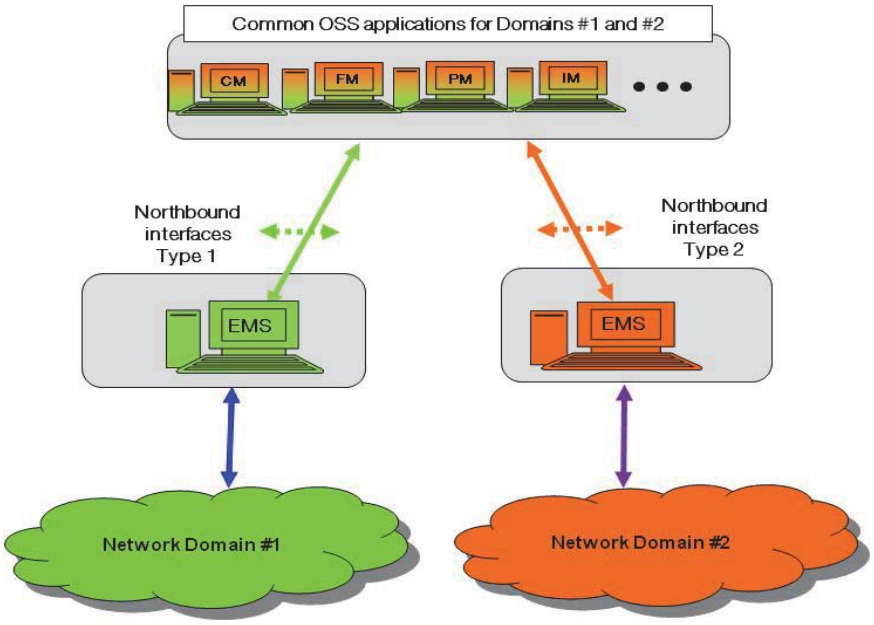

Figure 12: Basic architecture scenario "Converged Network Management Layer" (Intermediate Scenario)

3.3.1.3 Converged Element Management Layer (Intermediate Scenario)

Description

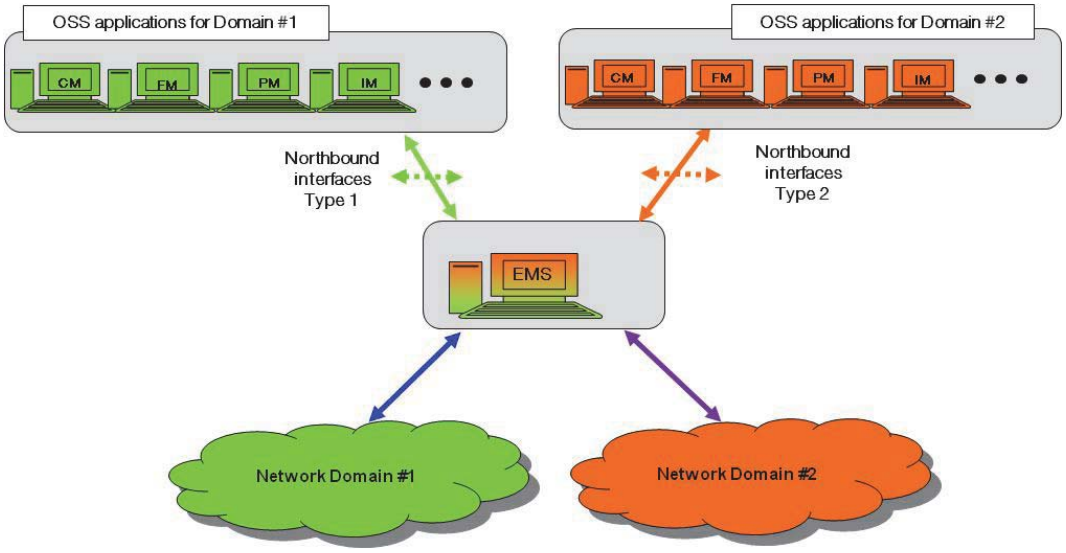

Figure 13: Basic architecture scenario "converged element management layer"(Intermediate Scenario)

This scenario is characterized by:

1. Operators get from a given network equipment provider a single Element Management System common to multiple network domains/ technologies/ regions, e.g. vendor X EMS is the same for 2G/ 3G/ LTE Circuit-Switched Core Network/ Packet-Switched Core network/ IMS/ Application Servers, etc.;

2. Vendors' EMSs support various kinds of northbound interfaces, e.g. one set for mobile networks (based on 3GPP IRPs), another set for wireline networks (based on TMF interface programs), meaning that no convergence is achieved at the EMS northbound interface;
3. Operators' OSS network management applications are dedicated to specific network domains/ technologies/ regions and OA&M functional areas, i.e. no convergence at the network management layer.

Important: It shall be noted that using the term "Converged Element Management Layer" in the present document does not necessarily mean having a single EMS platform instance for managing the whole operator network (e.g. for fixed and mobile). Though this might be the case in some environments where the number of managed network elements is limited, reliability/ availability of the EMS is not critical, etc. The architecture scenario depicted above also addresses the case where a network operator manages various network technologies/ domains/ regions using a single EMS product line (not a single EMS instance) for managing network elements of the same vendor.

We do not require having one single EMS instance for the whole network. We require having one single EMS product line for e.g. a given domain (2G/3G/LTE Radio Access Network) or, better, multiple domains (mobile + fixed). Besides, our requirement is for NEs coming all from a given vendor. The multi-vendor aspect is left to the NMSs.

If the Northbound interface convergence is one aspect of high interest for operators, we need to point out through this scenario, that it is not the only one. CAPEX and OPEX savings are expected from EMS convergence and this is a requirement to Network Equipment vendors.

This scenario will involve vendors' product line; therefore, in order to make it happen, a negotiation in a pragmatic way, must be undertaken as early as possible between the two parties: operators and vendors.

3.3.1.4 Converged EMS northbound interface (Intermediate Scenario)

This scenario requiring standardized interfaces shall be studied prior to those requiring EMS / NMS convergence. The operators are asking for standards in this section 3.3.1.

Description

In this scenario,

1. Vendors offer multiple Element Management Systems on a per network domain/ technology basis;

2. Vendors' EMS(s) support one single converged northbound interface:
   a. Based on a federated network information model, for both wireless and wireline network domains,
   b. Based on an harmonized functional interface per functional area, e.g. one single harmonized functional interface for fault management, for both wireless and wireline network domains, one other single harmonized functional interface for configuration management, etc.;

3. Operator has multiple OSS applications for specific network domains/ technologies and OA&M functional area, e.g.:
   a. Fault management
   b. Performance management, etc.

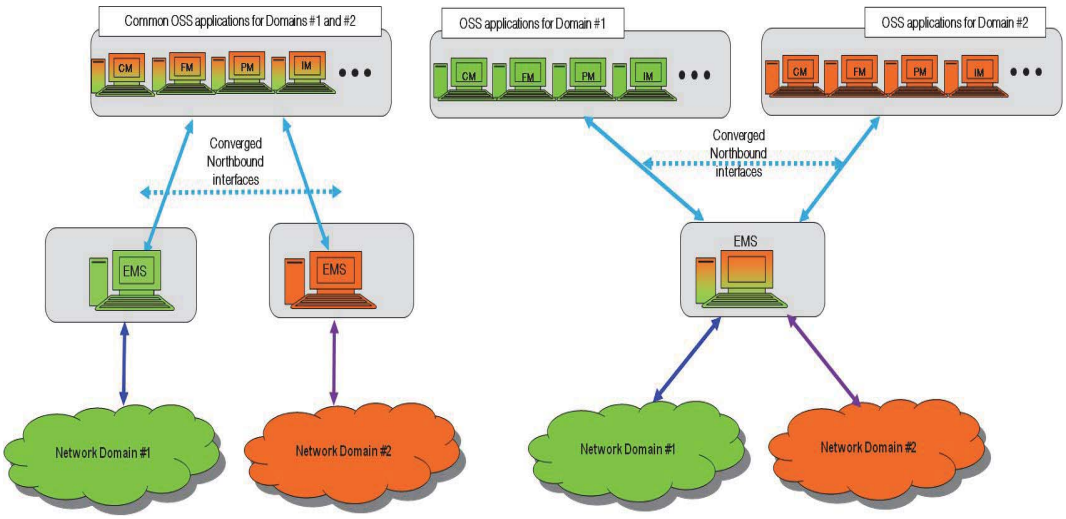

Figure 14: Basic Scenario: "Converged EMS northbound interface(s)" (Intermediate Scenario)

It shall be noted that the scenario “converged EMS northbound interface” may apply to the previously described architecture scenarios, as depicted by Figure 14.

Important: It shall be noted that one single EMS northbound interface for the management of any kinds of network domains/ technologies and for all functional areas is not envisaged here. The converged northbound interface shall be based on federated information and operations models. Please see section REQUIREMENTS FOR NGCOR MODELLING AND TOOLING (MT) for detailed information about the federated models.

3.3.2 Combined Architecture Scenarios

This Combined Architecture Scenarios family is broken down into 2 types of scenarios from methodology point of view:

- ***Intermediate Architecture Scenarios*** paving the way to the Target Architecture Scenario
- ***Target Architecture Scenario*** as ultimate goal of the migration process

In this section, we defined these "Intermediate" and "Target" Scenarios as possible combinations of basic converged operations architecture scenarios described in Section 3.3.1 within an operator’s environment:

C1: Converged Element Management Layer together with converged EMS northbound interface (Intermediate Scenario)

C2: Converged Network Management Layer together with converged EMS northbound interface (Intermediate Scenario)

C3: Converged Element Management Layer together with converged EMS northbound interface and converged Network Management Layer (Target Scenario)

In this family, the Current Scenario or starting point is implicit in the sense we assume that the operators have obtained from the SDOs the specification of the "Converged Northbound Interface" as depicted at Figure 14. Hence, the three "Combined Architecture Scenarios" C1, C2 and C3 are all "Converged Northbound Interface"-capable.

3.3.2.1 C1 - Converged Element Management Layer Together with Converged EMS Northbound Interface (Intermediate Scenario)

This combined architecture scenario combines the basic architecture scenarios described in Section 3.3.1.3 and Section 3.3.1.4.

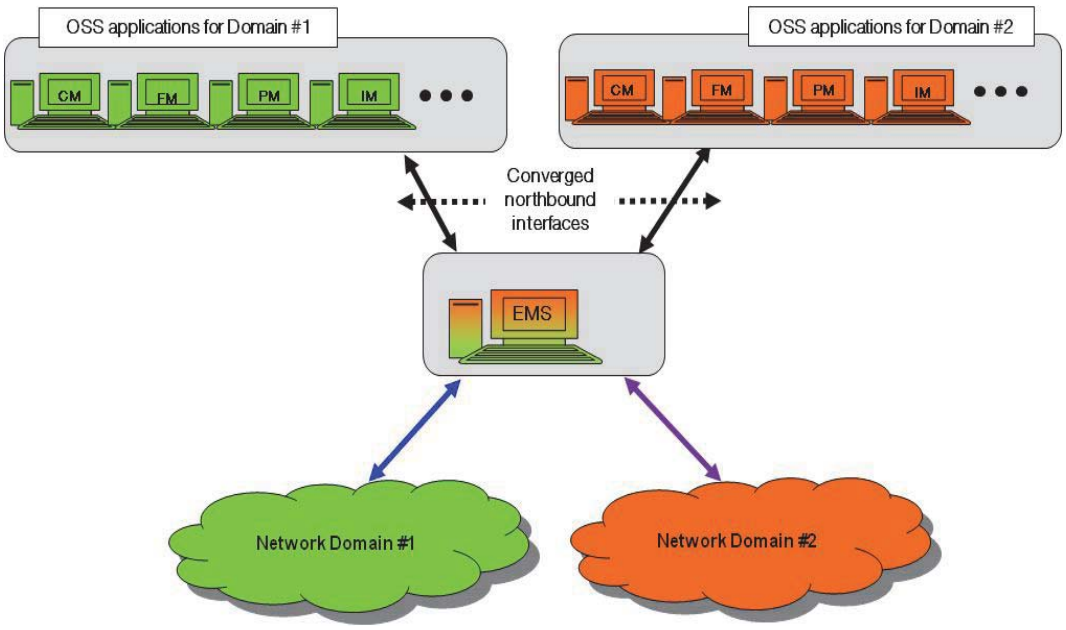

Figure 15: Combined architecture scenario "converged EMS and converged NBI" (Intermediate Scenario)

We do not require having one single EMS instance for the whole network. We require having one single EMS product line for e.g. a given domain (2G/3G/LTE Radio Access Network) or, better, multiple domains (mobile + fixed). Besides, our requirement is for NEs coming all from a given vendor. The multi-vendor aspect is left to the NMSs.

This scenario is considered as an "Intermediate Scenario" within the migration path hence paving the way to the target scenario depicted by Figure 17. The motivation behind is linked to the need of saving CAPEX and OPEX as highlighted in sub-section 3.3.1.4 beyond the benefit expected by the convergence of the Northbound interface. This scenario will involve vendors' product line assuming that converged Northbound Interface is already implemented by vendors. In order to make it happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the two parties: operators and vendors.

3.3.2.2 C2 - Converged Network Management Layer Together with Converged EMS Northbound Interface (Intermediate Scenario)

This combined architecture scenario combines the basic architecture scenarios described in Section 3.3.1.2 and Section 3.3.1.4. This scenario is considered as an "Intermediate Scenario" within the migration path hence paving the way to the target scenario depicted by Figure 17.

The motivation behind is linked to the need of saving CAPEX and OPEX as highlighted in sub-section 3.3.1.3 beyond the benefit expected by the convergence of the Northbound interface.

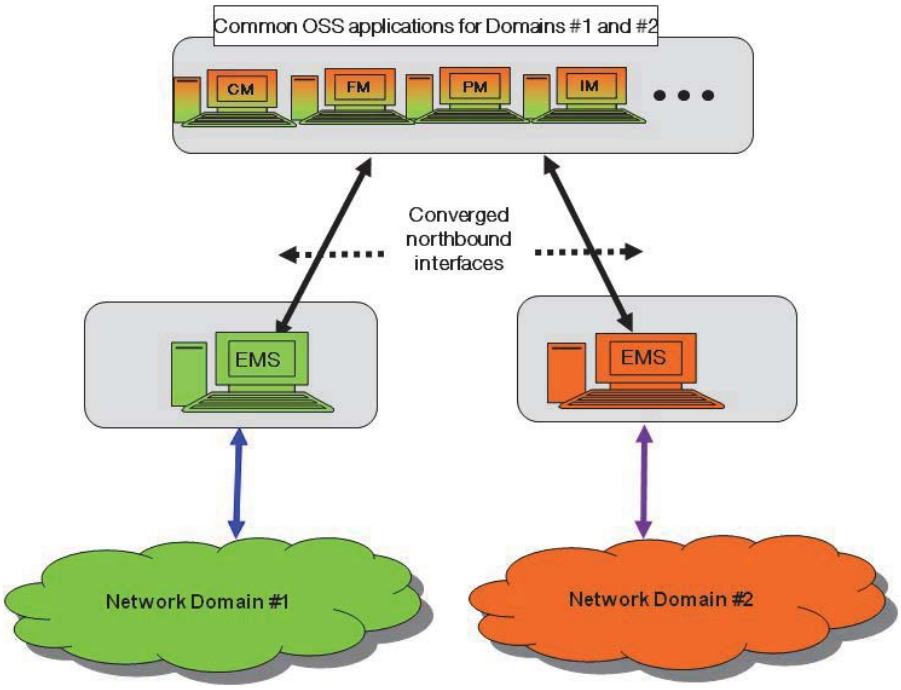

Figure 16: Combined architecture scenario "converged network management layer and EMS NBI" (Intermediate Scenario)

In order to make this scenario happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the two parties: operators and OSS vendors and IT integrators.

3.3.2.3 C3 - Converged Element Management Layer Together with Converged EMS Northbound Interface and Converged Network Management Layer (Target Scenario)

The combined converged operations architecture scenario shown in Figure 17: Combined architecture scenario "converged northbound interface, EMS & NMS" (Target Scenario) combines the basic converged operations architecture scenarios described in Sections 3.3.1.2., 3.3.1.3 and 3.3.1.4.

We do not require having one single EMS instance for the whole network. We require having one single EMS product line for e.g. a given domain (2G/3G/LTE Radio Access Network) or, better, multiple domains (mobile + fixed). Besides, our requirement is for NEs coming all from a given vendor. The multi-vendor aspect is left to the NMSs.

This scenario will involve vendors' product line assuming that converged Northbound Interface is already implemented by vendors. In order to make it happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the operators and vendors, in one hand, and between operators and OSS vendors and IT integrators, in the other hand.

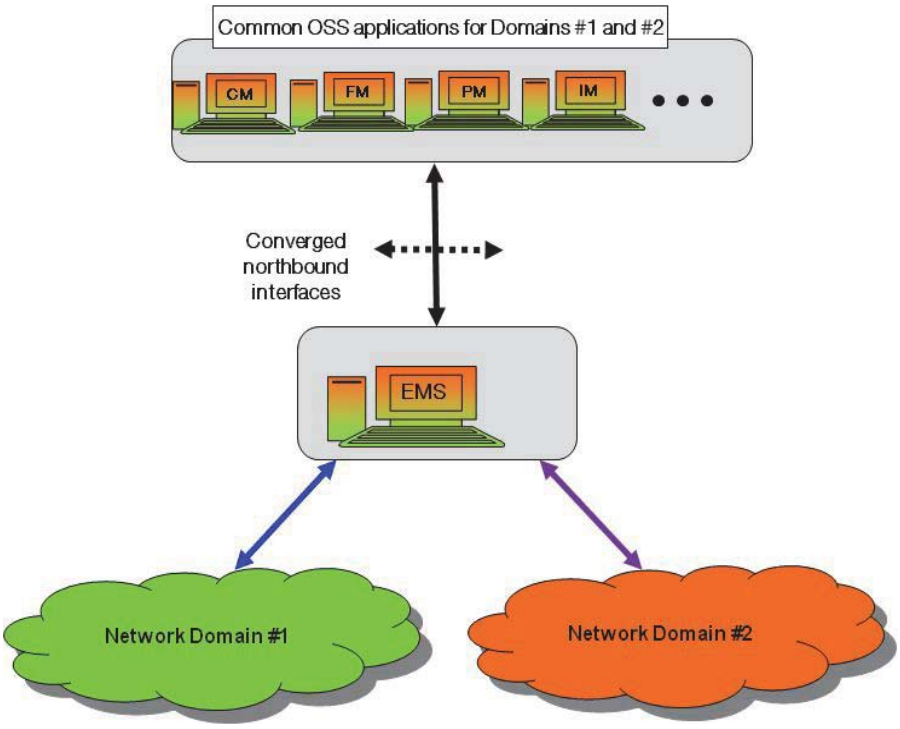

Figure 17: Combined architecture scenario "converged northbound interface, EMS & NMS" (Target Scenario)

3.4 Business Scenarios and Requirements regarding Converged Operations

In this section, we have identified a family of Business Scenarios (as real use cases) of high interest to operators. The list could be extended within the NGCOR scope. In order to demonstrate the benefit from the converged operations perspective, we map them on either Basic or Combined Operations Architecture Scenarios we described in Sections 3.3.1 and 3.3.2.

The whole methodology we adopted in this section is the following:

- Related Use Case description based on ITU-T framework (Goal, Actors & Roles, Assumption, Pr-conditions, Post-conditions…);
- Instantiation and relevance to Basic and / or Combined Operations Architectures Scenarios;
- High-level requirements description;
- Expected benefits (at very high level view, no figures)

3.4.1 Converged Operations Business Scenarios within a Single Operator Environment

3.4.1.1 Business Scenario 1: EMS Shared between Operators' Affiliates

Several affiliates of a network operator share an EMS (mono-vendor environment)

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal (*)	The objective is to lower CAPEX and OPEX by having one single EMS platform for managing networks belonging to several affiliates of a large service provider deployed over multiple neighbour countries.	
Actors and roles (*)	Several affiliates of a large service provider A near-shore network operation centre, in charge of operating several network domains from affiliates of a single large service provider.	
Telecom resources	Network resources in various countries, all from the same vendor, all from the same network domain, e.g. IMS. A single EMS in a near-shore network operation centre.	
Assumptions	Large service providers have footprints in many countries. Though, in some of these countries, they are incumbent, it also happens that, in some other countries, they are challengers, have limited footprints and have to lower their CAPEX and OPEX to be competitive. In some cases, they deploy a relatively limited number of network elements in each country and put in place a unique organization responsible for operating these domestic networks. The resulting 24/7 shared **Network Operation Centre** (NOC) uses a single EMS for all the nation-wide networks it is in charge of. NOC staff is responsible of daily operation of the various networks.	
Pre-conditions	Each affiliate has deployed its network elements in the country it is responsible for. These network elements are connected to the near-shore shared EMS. All managed network elements and the shared EMS are from a unique vendor.	
Begins when	In some countries, local staff, thanks to their local network operations capabilities, keeps limited capabilities for managing their network.	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)		
Exceptions		
Post-conditions		
Traceability (*)		
NOTE – Fields marked with "*" are mandatory for all use case specifications. Other fields are only mandatory when relevant for the specific use case.		

Figure 18 depicts this real use case.

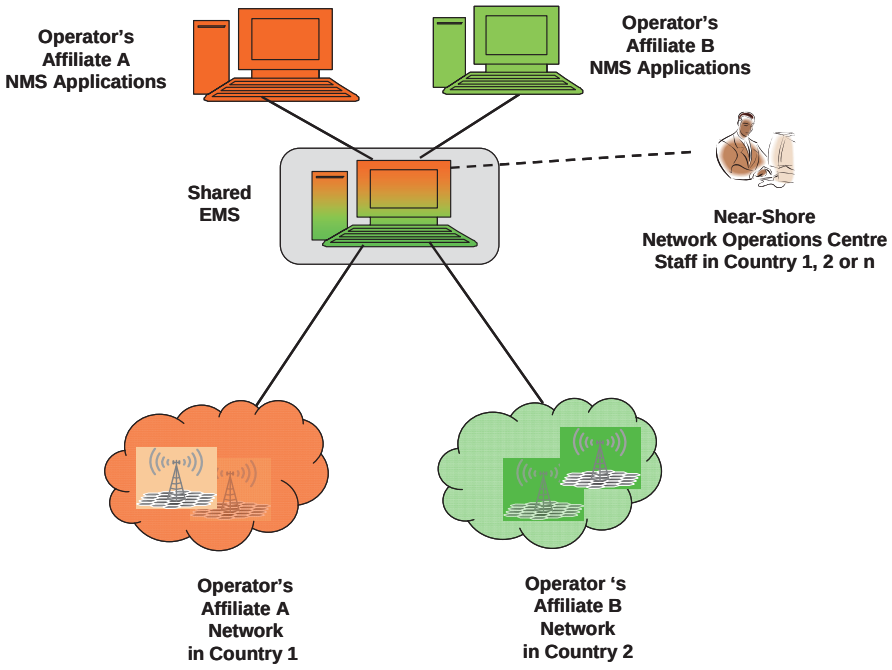

Figure 18: Business scenario 1: Single EMS platform managing multiple affiliates' networks in various countries

Instantiation and relevance

This use case makes use of the basic architecture scenario described in Section 3.3.1.3 (Converged Element Management Layer (Intermediate Scenario)).

We do not require having one single EMS instance for the whole network. We require having one single EMS product line for e.g. a given domain (2G/3G/LTE Radio Access Network) or, better, multiple domains (mobile + fixed). Besides, our requirement is for NEs coming all from a given vendor. The multi-vendor aspect is left to the NMSs.
This scenario will involve vendors' product line assuming that converged Northbound Interface is already implemented by vendors. In order to make it happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the operators and vendors,

High-level requirements

REQ-CON (1) Vendors' EMS shall be able to manage network elements belonging to several network operator affiliates. In a minimal configuration, it shall be able to manage multiple network domains / technologies, e.g. it shall be able to cover not only multiple radio access technologies but shall also enable network operators to manage their wireless and wire line network domains in a unified way.

REQ-CON (2) Alarms coming from operator affiliates' domestic network elements up to the shared EMS are handled by shared NOC staff. The shared EMS shall be able to filter such alarms and forward them to the relevant operator affiliate OSS FM application, either for information only or for action (acknowledge, clear, etc.). All alarm-related information exchanges between the shared EMS and the affiliates' OSS FM applications shall comply with standardized specifications.

REQ-CON (3) Operator affiliates shall be able to configure their own network elements from their own OSS CM application(s). The shared EMS shall ensure isolation of configuration action requests coming from the affiliates' OSS CM applications. All configuration management related information exchanges between the shared EMS and the affiliates OSS CM applications shall comply with standardized specifications.

REQ-CON (4) Operator affiliates shall be able to collect performance management counters/ KPIs related to their own network elements. They shall be able to trigger, from their own OSS PM application, performance measurement jobs for their own purpose, and collect related PM measurements within their OSS PM application. All performance management related information exchanges between the shared EMS and the affiliates' OSS PM Applications shall comply with standardized specifications.

REQ-CON (5) Operator affiliates shall be able to inventory resources related to their own network elements. They shall be able to retrieve, from their own OSS InvM application, all available inventory data. All inventory management related information exchanges between the shared EMS and the affiliates' OSS InvM applications shall comply with standardized specifications.

Expected benefits:

CAPEX savings:

- One EMS hardware platform instead of N (N being the number of affiliates);
- In case of highly available (HA) EMS platform, only one is needed instead of N

OPEX savings:

- One team for network operations instead of N
- EMS validation test phase (unitary + end-to-end) to be performed once instead of N times
- Common processes for N affiliates instead of 1 per affiliate, for e.g. backup and restore, software and hardware upgrade management, license management, etc.

3.4.1.2 Business scenario 2: Network Management Level Applications Shared Between Operators' Affiliates

Several affiliates of a network operator share NMS applications (multi-vendor environment)

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal (*)	The objective is to lower CAPEX and OPEX by having one single set of NMS applications for managing networks belonging to several affiliates of a large service provider deployed over multiple neighbour countries. Large network operators have their networks deployed in several countries. Instead of developing a dedicated OSS application in each country for e.g. fault management, it is common that they develop a single OSS application for multiple countries and/ or multiple domains and/ or multiple technologies. Such operator-wide OSS applications are based on a kernel and possible adaptations due to local and/ or domain-specific and/ or technology-specific requirements.	
Actors and roles (*)	Several affiliates of a large service provider A near-shore Network Operation Centre, in charge of operating several network domains from affiliates of a single large service provider	

Several affiliates of a network operator share NMS applications (multi-vendor environment)

Use case stage	Evolution/Specification	<<Uses>> Related use
Telecom resources	Network resources in various countries, from various vendors, all from the same domain, e.g. IMS. One EMS per country. A single set of NMS applications in a near-shore Network Operation Centre.	
Assumptions	Large service providers have footprints in many countries. Though, in some of these countries, they are incumbent, it also happens that, in some other countries, they are challengers, have limited footprints and have to lower their CAPEX and OPEX to be competitive. In some cases, they deploy a relatively limited number of network elements in each country and put in place a unique organization responsible for operating these domestic networks. The resulting 24/ 7 shared Network Operation Centre (NOC) uses a single set of NMS applications for all the nation-wide networks it is in charge of. NOC staff is responsible of daily operation of the various networks.	
Pre-conditions	Each affiliate has deployed its network elements in the country it is responsible for. These network elements are connected to their local EMS. All EMSs are connected to near-shore NMS applications. Each affiliate may have its own policy with regard to the vendor of their managed network elements and corresponding EMS.	
Begins when	In some countries, local staff, thanks to their local network operations capabilities, keeps some capabilities for managing their network.	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)		
Exceptions		
Post-conditions		
Traceability (*)		

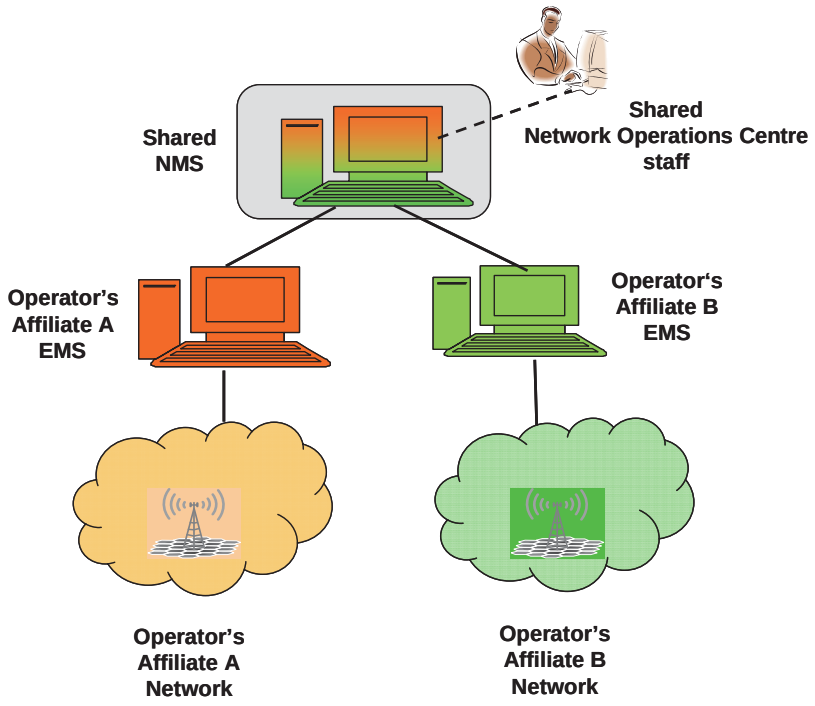

Figure 19: Business scenario 2: Common NMS applications for multiple affiliates

Instantiation and relevance

This use case makes use of the basic architecture scenario described in Section 3.3.1.2 (Converged Network Management Layer).

In order to make this scenario happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the two parties: operators and OSS vendors and IT integrators.

High-level requirements

REQ-CON (6) Network management applications shall be, up to the maximum, common to multiple network domains / technologies. They shall be based on a kernel, common to multiple network domains / technologies, and possibly technology-specific management capabilities.

REQ-CON (7) In order to lower the costs of integration of the various EMSs to the single set of NMS applications, it is required that all EMSs offer the same set of northbound interface(s), based on a standardized federated model (cf. Sub-Task Modelling & Tooling)

Expected benefits

- CAPEX savings:
  - One set of NMS hardware platforms per application instead of N (N being the number of affiliates);
  - In case of highly available (HA) NMS platform, only one is needed instead of N

- OPEX savings:
  - NMS applications release management is done centrally instead of locally

3.4.1.3 Business scenario 3: Converged Service Management Applications

Instantiation and relevance

End-to-end service configuration and activation from a unique OSS application is key for service providers. In the future, when a new fixed and mobile IMS VoIP subscriber is to be provisioned, the following list of NEs will have to be provisioned:

- Home Gateway
- IMS HSS
- HLR
- EPC HSS
- SPR/PCRF
- Possibly FemtoCell.

In order to enable end-to-end provisioning in a timely manner and error-freely, having a single service configuration and activation application capable of orchestrating provisioning requests to various underlying domain specific provisioning applications will help in reducing OPEX and improve customer satisfaction.

High-level requirement

REQ-CON (8) Operators expect common service management applications for the following functional processes, belonging to service operation and management:
- Service configuration and activation
- Service problem management
- Service quality management

Expected benefits

OPEX savings:
- Due to simpler way to manage subscribers from a single point (provisioning, monitoring, tracing, etc.)

3.4.2 Converged Operations Business Scenarios within Multi-Operator Environment

3.4.2.1 Business Scenario 4: RAN Sharing with EMS shared amongst Operators

RAN Sharing

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal (*)	The objective is to lower CAPEX and OPEX by sharing Radio Access Network elements between multiple operators in a given country.	
Actors and roles (*)	Several network operators sharing their RAN. Regulator A “Master Operator”, in charge of operating the shared network elements.	
Telecom resources	Radio Access Network resources shared between several operators in a single country, all from the same vendor. One single EMS under the responsibility of the Master Operator. Sharing Operators, having their own set of NMS applications.	

RAN Sharing

Use case stage	Evolution/Specification	<<Uses>> Related use
Assumptions	Shared Network Elements have an OA&M connection to the common EMS. Sharing Operators have no direct OA&M connection to the shared network elements. The EMS is under the full responsibility of the Master Operator. The EMS has interfaces to Sharing Operators' NMS applications.	
Pre-conditions		
Begins when		
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)		
Exceptions		
Post-conditions		
Traceability (*)		

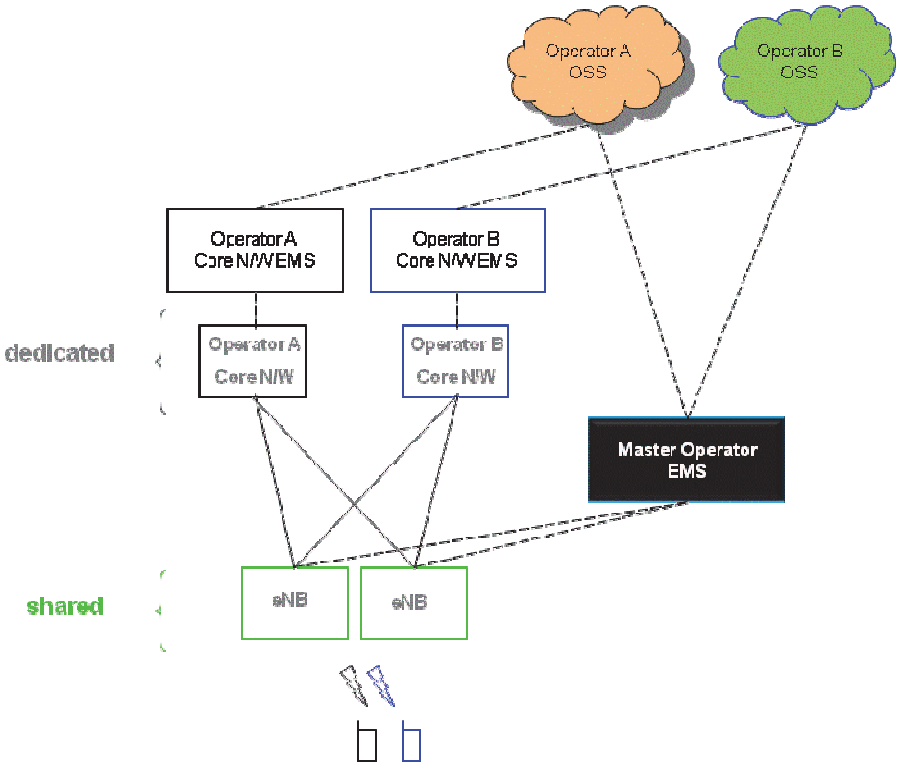

Figure 20: Business Scenario 4: RAN Sharing

Instantiation and relevance

This use case is an instantiation or an implementable scenario of generic operations use case depicted in Figure 15 which requires a converged EMS and Converged Northbound interface.

High-level requirements

REQ-CON (9) It shall be possible that the"Master Operator" EMS and "Sharing Operators" NMS applications communicate with each other through a standardized northbound interface. This interface shall be "online", i.e. not only based on offline file exchange. These exchanges shall be secured to ensure privacy of information. The Master Operator EMS shall be able to filter information exchanged with Sharing Operators' NMSs based on unique identifiers (PLMN Id, etc.). Standardized northbound interfaces shall enable such a use case.

Expected benefits

- CAPEX savings:
  - One single EMS platform to be deployed (HW + SW), instead of N (N being the number of Sharing Operators)
- OPEX savings:
  - Daily operations of the shared network are common. Sharing Operators can rely on the Master Operator for resource management and operations (only selected types of alarms, KPIs, etc. can be forwarded to each Sharing Operator, based on contract agreements).

3.4.3 General Requirements

3.4.3.1 Harmonized EMS Northbound Interfaces

High-level requirements

REQ-CON (10) Vendors' EMS shall offer a unique set of management capabilities at its northbound interfaces. It is expected that EMS northbound interfaces are implemented according to the following rules:

- Network resource models for various network domains are built on a standardized federated network resource model, i.e. network resource model for wire line network domains shall not be 100% different from network resource models for wireless network domains.
- Functional interfaces for wire line and wireless networks shall be similar for at least configuration management, fault management, performance management, inventory management, software management. EMS northbound Interface shall offer common management capabilities to the operator, regardless of the network domain.
- It is of primary importance that EMS northbound interface fully implements:
  - standardized northbound interfaces firstly and
  - clearly identifiable, vendor-specific extensions to capture vendors' own set of parameters and/or value added management capabilities. Vendor's specific capabilities shall be implemented as extensions
- EMS northbound interface shall be based on Web Services.

Expected benefits:

CAPEX savings:

- Integration of a new EMS in the Operator's environment is simpler, faster and thus cheaper

OPEX savings:

- Evolutions of already deployed EMSs northbound interfaces in the Operator's environment are handled more simply, fast, cheaply

3.4.4 To Which Players the Requirements are addressed

As indicated earlier, the requirements formulated in Section 3.1 are addressed to three types of players in order to be translated into standards **and** implementations, so as to meet operators' needs in terms of CAPEX and OPEX reduction:

- SDOs and Organisations
- OSS vendors / integrators
- Telecom equipment manufacturers.

Table 1: Converged Operations Requirements - Whom these requirements are addressed to summarizes this classification.

CON	Addressee / Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CON (1)	X	X	
REQ-CON (2)	X	X	
REQ-CON (3)	X	X	
REQ-CON (4)	X	X	
REQ-CON (5)	X	X	
REQ-CON (6)			X
REQ-CON (7)	X		
REQ-CON (8)			X
REQ-CON (9)	X		
REC-CON (10)	X		

Table 1: Converged Operations Requirements - Whom these requirements are addressed to

Comments

From the discussion with the partners, a clarification wrt requirements vs deployment scenarios, implementation was requested. Indeed, the high level requirements listed in this table are implementation neutral. The reason is that each operator can implement, and map them with regard to his own needs and organisation.
Here after, we try to make illustrations for Business Scenario 2.

Illustration 1
We can imagine a centralized structure that could perform the management of the Affiliates' EMSs and the shared NMS. In this case, the SW of EMSs and NMS can be located in this centralized structure.
The staff in charge of the networks management in the affiliates can remotely access to the EMSs and NMS to retrieve their own data.

Illustration 2

The network management can be provided as a service “SaS”. In this case, a third party can provide SW and HW for the management purpose as well as hosting facilities. The operator staff in their OMCs can access remotely and selectively (through filtering process) to these SW functions as well as to results processed. The third party can also collect and retrieve data from the operator’s equipment. This “Full” SaaS mode looks like to outsourcing Business Scenario the NGCOR as identified.

4 Requirements for NGCOR Modelling and Tooling (MT)

4.1 Introduction

4.1.1 Background for Modelling and Tooling

The main important future O&M requirements are specified and defined in the NGMN Top OPE Recommendations. Those requirements will need further enhancement with more details for guiding towards well standardized interfaces and interworking solutions throughout O&M/OSS. Resolving misalignments and open questions in the standardization of the area needs immediate actions already in the short term.

There is the need to give guidance to SDOs/organisations and industry bodies (e.g. 3GPP or TM Forum) in order to prioritize the work. Develop the solutions for most important requirements first and specify the recommendations for the best solutions.

The project should address and achieve a higher level of standardization in the converged (wireline and wireless networks) operations area which will lead to reduced OPEX and CAPEX. In addition a faster time to market is expected through these requirements.

The NGMN Top OPE Recommendations are dealing only with wireless requirements. Wireline and wireless networks will be merged in the near future within many operators. There is a need for the definition of Converged O&M requirements to ensure that the operational activities within the converged networks perform optimally.
The specification of common usable network data and operations for these networks allow reducing CAPEX (harmonised networks) and OPEX (seamless operation processes).

It reduces the integration cost by harmonising the Information Model and reduces the maintenance cost by unifying the Operations Model.

“An increasing number of Service Providers (SP) has to operate a variety of network and service production infrastructures, from mobile and fixed network environments up to converged networks and services across many countries. The increasing demand to maintain and improve customer experience requires full end-to-end service management and hence, multi-technology and multi-vendor network management capabilities. On the other hand, financial downturn has put even more pressure on operational efficiency improvement.”

4.1.2 Definitions

The MT section defines or specializes the following terms:

- Federated Model
- Interface

4.1.2.1 Federated Model

The Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. It enables the implementation of convergent network management functions and processes (for example alarm correlation) which need to operate on objects belonging to different network domains (for example wireless and wireline). The Federated Model is composed of the **Federated Information Model** (FIM) containing the data part of the model; i.e., the object classes with their attributes, and the **Federated Operations Model** (FOM)

containing the dynamic part of the model; i.e., operations (and their parameters) grouped in service interfaces which allow the transport of the data defined in the FIM through the management interfaces.
The model covers resource and service management layers (according to Figure 21) and all their management functions like **Configuration Management** (CM), **Fault Management** (FM), **Performance Management** (PM), and **Inventory Management** (InvM) or **provisioning and assurance**.

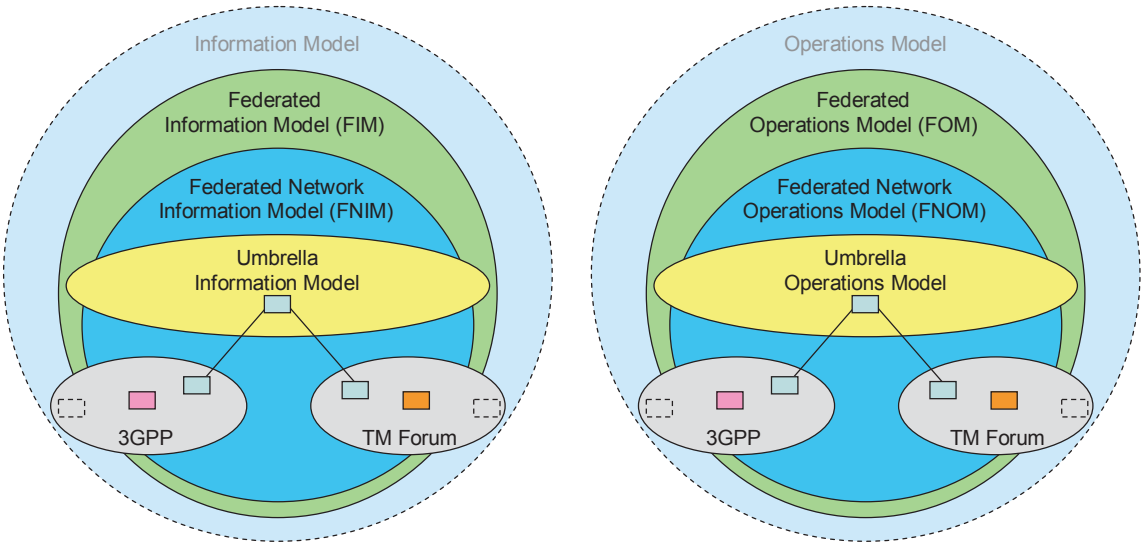

Figure 21: Federated Model

Note:
The FIM is similar to the NRM IRPs (Network Resource Model Integration Reference Points) in 3GPP and the Shared Information & Data Model (SID) in TM Forum.
The FOM is similar to the Interface IRPs (Integration Reference Points) in 3GPP and the Business Services in TM Forum.

4.1.2.2 Interface

The term “interface” used in the MT section is a network level management interface between various kinds of operation systems. Consequently, interfaces between Element Management System (EMS) and the Network Elements (NE) are out of scope.

Note:
In 3GPP terms: The term "interface" used in the MT chapter corresponds to 3GPP the northbound interface (Itf-N) between the EMS and the NMS (or operator's OSS for Operations Support System). The southbound interface, between EMS and the network elements is out of scope.
In TM Forum terms: The interface in scope is the MTNM/ MTOSI interface between EMS – NMS and more generally between all kinds of OSSs.

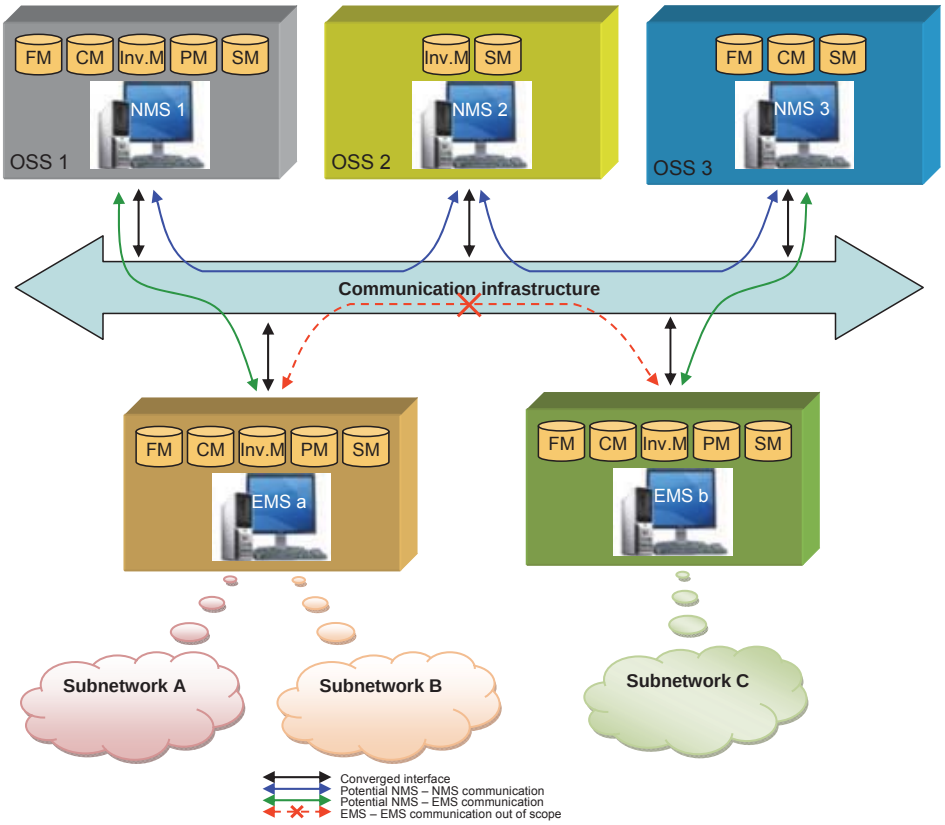

Figure 22: Converged Interface peers

4.2 Scope

Main scope of this sub task:

- Define requirements for the modelling environment
- Define requirements for the Federated Information Model
- Define requirements for the Federated Operations Model
- Define requirements for the tooling infrastructure
- Define requirements for general operations used at the interface.

Out of scope for this sub task:

- Define requirements for specific operations used at the interface. This shall be specified in the JWGs between the individual SDOs/ organisations.

4.3 Objective

The objective of the project is to produce detailed requirements from operator's point of view for an infrastructure that allows an efficient specification of management interfaces for converged networks. These requirements are based on the operator's expectations on a converged modelling and tooling infrastructure which need to be taken into account by the Standards Developing Organisations (SDOs) and organisations.
Already existing modelling and tooling specifications in 3GPP and TM Forum are taken into account and will be used as input to produce the requirements for the converged interface specification infrastructure.

4.4 Methodology

Methodology of this sub task:

- Definition of the level of details

Examination of the Information Models, design principles and guidelines from 3GPP SA5, TM Forum and their JWGs (See

- Figure 23: Model of 3GPP and Figure 24: Model of TM Forum)
- Definition of design principals and patterns
- Definition of interface modelling requirements.

Deliverables of this sub task:

- Modelling environment requirements (e.g., specification structure, general design principals and modelling patterns)
- Tooling infrastructure requirements (e.g., interchange file formats)
- Recommendations regarding implementation.

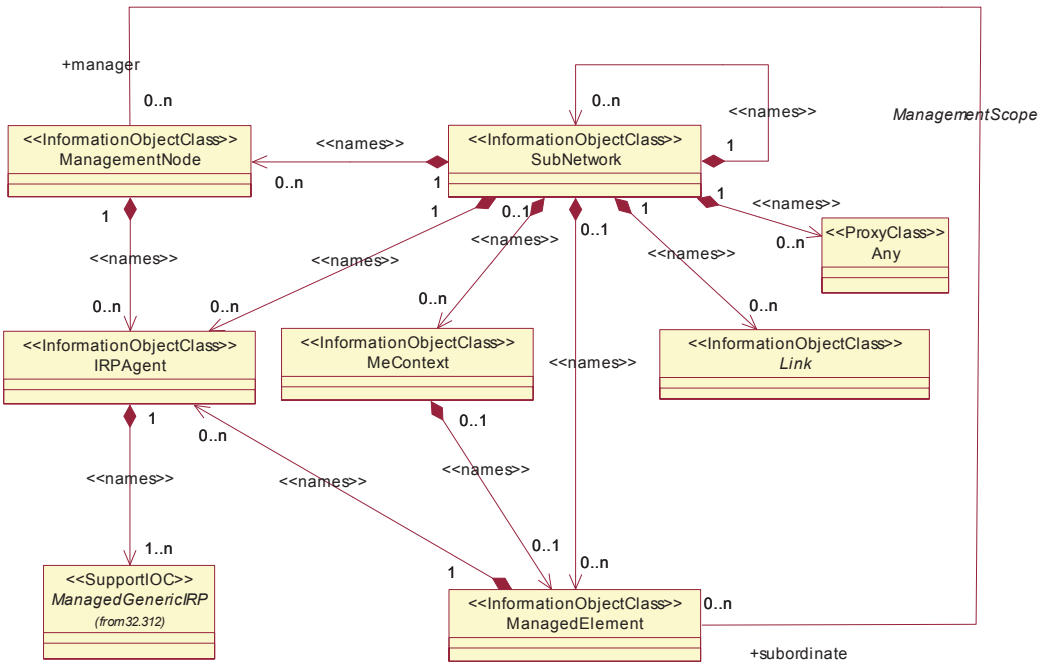

Figure 23: Model of 3GPP

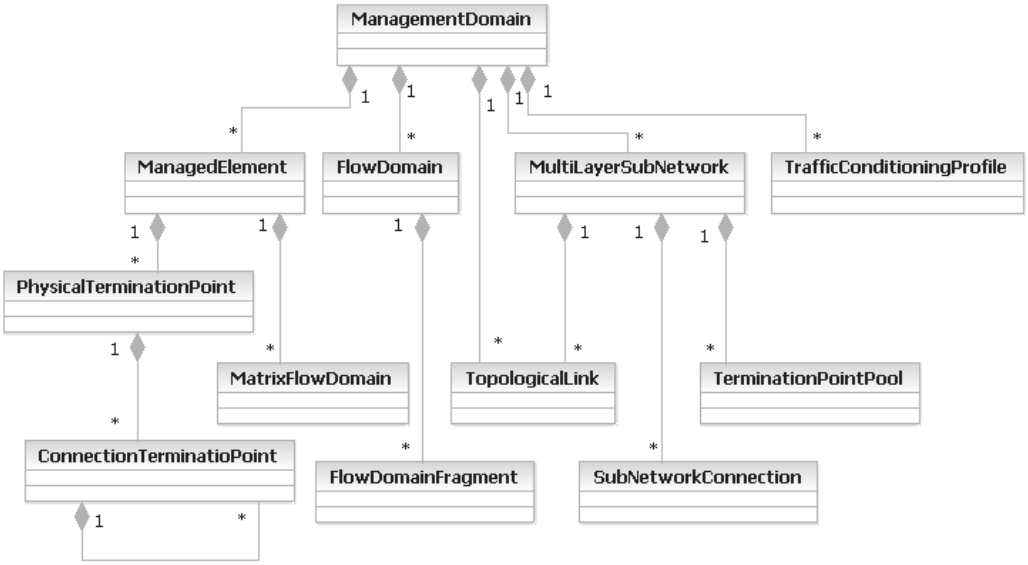

Figure 24: Model of TM Forum

The figures
Figure 23: Model of 3GPP and Figure 24: Model of TM Forum show the containment / naming hierarchy and the associations of the classes defined in the Joint 3GPP/ TMF model alignment project. (Top figure extracted from Figure 6.1: Generic NRM Containment/Naming and Association diagram (3GPP TS 32.622 [12])
Bottom figure extracted from Figure LR.35 - MTOSI/MTNM Containment (TM Forum SID Rel. 9.5 [41])

4.5 Requirements

Abstract:

3GPP WG SA5 has specified detailed **Network Resource Models** (NRMs) [16] for the management of mobile networks, plus a Generic Network Resource Model [12].

TM Forum has done the same for the management of various kinds of fixed networks, as well as a **Shared Information & Data** (SID) Model [28] providing a "common reference model for enterprise information that service providers, software providers, and integrators use to describe the network data", i.e., also generic definitions for network and service management aspects.

It shall be noted that the 3GPP Generic Network Resource Model (Generic NRM) [12] and TM Forum SID [28] have different scopes and have been developed independently from each other. As a consequence the resulting models are different.

Though there will always be a part in the Generic NRM [12] and the SID [28] which is different due to the different network technologies modelled, there are numerous model elements which do not have to be different between the two models because of the different network technologies.

Examples of these common elements are modelling of resource inventory information, modelling of security aspects, modelling techniques and how vendor specific Information Model extensions are managed using NRMs and SID.

Parallel to 3GPP und TM Forum are even more other Standards Development Organisations (SDOs) and organisations such as the Internet Engineering Task Force (IETF), International Telecommunications Union – Telecommunication Standardization Sector (ITU-T), Broadband Forum (BBF), Metro Ethernet Forum (MEF), etc., which have defined different management standards/ recommendations for mobile and fixed networks. In addition to the SDOs/ organisations many vendors deliver Element Management Systems (EMS) with their own proprietary solutions for specific technologies/ networks. It needs to be emphasised that the EMS is another OPEX cost centre that can be reduced thanks to the multi-technology-multi-domain capabilities of the EMSs.

Because all sets of specifications have been specified independently, the management of the mobile part and the fixed part is currently structured along silos with different management interfaces, information models, management architectures, and management workflows.
An additional problem is that even within mobile or fixed networks, we can find different specifications (modelling/ tooling) which are developed by different SDOs/ organisations or vendors.

All these different Standards (from SDOs/ organisations) and proprietary solutions (from vendors) use different modelling/tooling, therefore the CAPEX and OPEX for network operators and integrators to integrate all these interfaces have increased dramatically. A considerable obstacle is the complex mapping mechanism between all the different OSS tools when they need an interface to exchange information.

This heterogeneous modelling/tooling (1/ different models for different network domains/ technologies and 2/ different modelling frameworks (e.g. Stage 1-3 for 3GPP, BA, IA, IIS for TM Forum; UML for TM Forum with an inter-exchangeable format versus picture in 3GPP) also has a massive influence to scalability, time to market, complexity and applicability of these standards in OSS.

In the future the mobile and fixed networks will no longer be managed as separate networks. The convergence of mobile and fixed networks requires the convergence of the mobile and fixed OSSs.

The network operators and the telecommunication industry would greatly benefit from aligned management interfaces, management models, management architectures, and management workflows.

4.5.1 Modelling Requirements

Fixed and mobile networks are growing together → FMC. The specification of common usable network data and converged operations for these networks allow reducing CAPEX and OPEX.
We will be able to reduce integration cost by harmonising the Information Model and reduce the maintenance cost by unifying the Operations Model.

4.5.1.1 General Requirements

REQ-MT (1) The following SDOs/ organisations (at least 3GPP, TM Forum, ITU-T, BBF, MEF, and others) shall strengthen their joint activities regarding the Management topic

REQ-MT (2) It shall be possible to add other SDOs/ organisations in the future

REQ-MT (3) The resulting Umbrella Information Model shall be publicly available

REQ-MT (4) The Umbrella Information Model shall allow SDO/ organisation-specific enhancements based on common modelling patterns

REQ-MT (5) SDO/ organisation-specific enhancements should be realised in a way that enables a drill down process. The drill down process means the ability to identify a more generic class (super class) from the Umbrella Information Model which is enhanced in the SDO/ organisation-specific model. This assures that SDO/ organisation-specific extensions can be clearly identified as a detailed version of the commonly agreed classes and concepts

REQ-MT (6) The interfaces which use the SDO/ organisation-specific Information Model should be compliant with the interfaces defined in the Umbrella Information Model. Compliant means that object classes defined in an SDO/ organisation-specific Information Model need to subclass from the appropriate (abstract) classes defined in the UIM

REQ-MT (7) The proposed mechanism of SDO/ organisation-specific extension is via inheritance and the composition (decomposition) of object modelling design patterns. Direct usage of the Umbrella Information Model objects is desired. (Multi-) Inheritance shall be used for extensions

REQ-MT (8) The other SDOs/ organisations shall be informed of SDO/ organisations-specific enhancements if they believe that these enhancements are generic and should be added to the UIM

REQ-MT (9) The number of SDO/ organisation-specific enhancements shall be reduced to the absolute necessary minimum

REQ-MT (10) The common management operations for fixed and mobile networks shall be harmonised

REQ-MT (11) SDOs/ organisations shall agree on a common terminology

REQ-MT (12) The functional coverage of the converged specifications shall continuously grow; i.e., shall replace the functions in the SDO/ organisation-specific specifications

REQ-MT (13) The harmonisation shall begin with high level business use cases, requirements, and usage scenarios. Followed by the model harmonisation and finished by the protocol harmonisation. (See Figure 25)

REQ-MT (14) The modelling shall be able to comprehensively describe the functions in a protocol-neutral way. "Comprehensively" means that the modelling shall be detailed enough to be used as the basis for another protocol-specific specification.
Reason for this is that operators are mainly interested in functions which stay over the time even when the protocol changes.

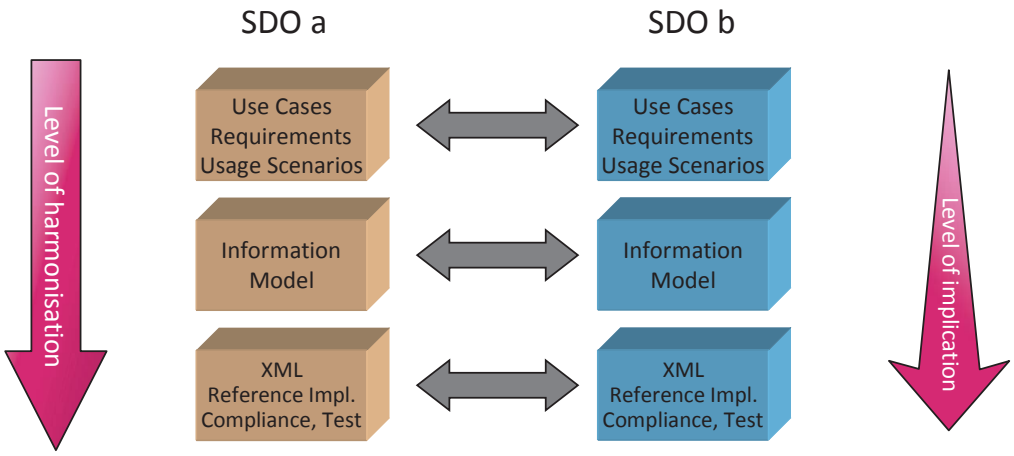

Figure 25: Interface Harmonisation Levels

The uses cases are the basis for the requirements and the requirements are the basis for the usage scenarios. Usage scenarios are defined for each required operation.

Note:
The "usage scenarios" are called "use cases*" in TM Forum.*

The level of impact is increasing because of the backward compatibility constraints appearing on the XML level.

REQ-MT (15) Harmonisation should include all network layers at vertical and horizontal view, in order to achieve a multi-domain, multi-technology perspective, see example in Figure 3

REQ-MT (16) The interfaces shall be based on high level business requirements

REQ-MT (17) Requirements shall be created for the static and dynamic parts of the interface

REQ-MT (18) The dynamic high level business requirements shall be converted into specific use cases

4.5.1.2 Requirement and Usage Scenario Templates

4.5.1.2.1 Requirement Template

Based on [45].

REQ-MT (19) Requirements shall be defined in text format

REQ-MT (20) Requirements shall be structured in six categories:
- Business Requirement
- Category I: Static and structural requirements
- Category II: Normal sequences, dynamic requirements
- Category III: Abnormal or exception conditions, dynamic requirements
- Category IV: Expectations and non-functional requirements
- Category V: System administration requirements

REQ-MT (21) Requirement identifiers must be unique within each category

REQ-MT (22) Requirements shall be defined using the following tabular template:

R_<SDO>_DDD_C_N	Description of the requirement
Source	Source of the requirement

where:

- <SDO> denotes the SDO / organisation
- DDD denotes the specification
- “C” designates the category of the requirement and is one of “BR”, I, II, III, IV, V
- “N” is a 4 digits integer (e.g. 0012).

REQ-MT (23) A requirement is referred to by its identifier “R_<SDO>_DDD_C_N"

REQ-MT (24) It must be possible to display the definition of a requirement by a simple mouse click from any of its references

4.5.1.2.2 Usage Scenario Template

Based on [45].

REQ-MT (25) Usage scenarios shall be defined in text format

REQ-MT (26) A usage scenario identifier must be unique

REQ-MT (27) Usage scenarios are defined using the following tabular template:

Usage Scenario Id	<US_<SDO>_DDD_N>
Usage Scenario Name	
Summary	
Actor(s)	
Pre-Conditions	
Begins When	
Description	<Step 1> <Step 2> … <Step n>
Ends When	
Post-Conditions	
Exceptions	Put a reference here to a document or a separate table which lists all the exceptions. Specific exceptions will be explicitly listed in the Description clause.
Traceability	Hyperlinks to the associated requirements

where:

- <SDO> denotes the SDO/ organisation
- DDD denotes the specification
- "N" is a 4 digits integer (e.g. 0012).

REQ-MT (28) A usage scenario is referred to by its identifier "US_<SDO>_DDD_N"

REQ-MT (29) It must be possible to display the definition of a use case by a simple mouse click from any of its references

REQ-MT (30) It must be easy to "navigate" from a requirement to the usage scenarios where this requirement applies and vice versa

REQ-MT (31) When a new specification is generated, the "N" part of the usage scenario identifier must be generated in sequence (no "hole"), until the document is released for official approval. From this stage the identifier of a given usage scenario will never change

4.5.1.3 Federated Model Requirements

REQ-MT (32) The SDOs/ organisations shall define a common model for mobile and fixed networks as a shared Umbrella Information Model

REQ-MT (33) The FIM shall enable the modelling of all resources of the mobile and fixed networks

REQ-MT (34) The Umbrella Model containing the network data and operations that are necessary for managing mobile and fixed networks shall be increased (over time). All generic (i.e., not fixed or mobile specific) network data and operations specified outside the Umbrella Model increase the operators OPEX and CAPEX significantly

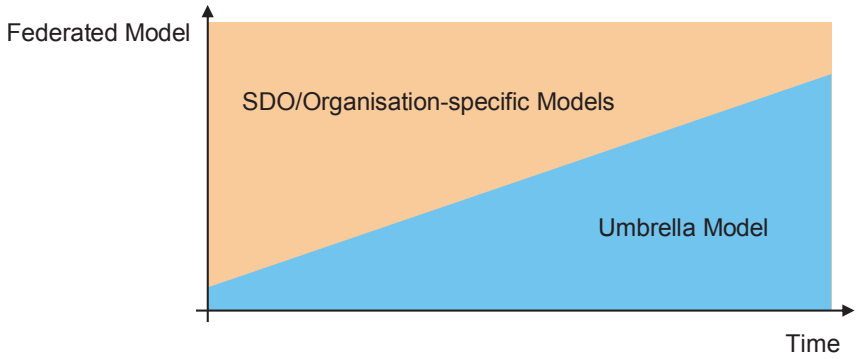

Figure 26: Relation between Federated Model – Umbrella Model

REQ-MT (35) The FIM shall enable the modelling of both the connection oriented technologies and connectionless technologies; e.g., model the connection oriented sub network connection and the connectionless flow domain fragment in one single object class. This also includes e.g. mobile access technologies and broadcast technologies

REQ-MT (36) All functionalities in the areas of Fault Management, Performance Management, Configuration Management (incl. Resource Provisioning and Service Configuration & Activation) and Inventory Management which are common to wireline and wireless management interfaces have to be consolidated in the harmonised Federated Model

REQ-MT (37) The static Information Models from wireline (e.g. MTOSI) and wireless (e.g. 3GPP) technologies have to be harmonised.
It is acceptable to have wireline and wireless specific parts but these parts shall as much as possible be based on the common Umbrella Information Model

REQ-MT (38) The Federated Model shall offer the necessary network data and operations for all domains such as Operations Support & Readiness (OS&R; which includes Inventory Management), Fulfilment and Assurance [46].

REQ-MT (39) The Umbrella Information Model shall initially contain specifications for networks, network elements, topological links, termination points and sub network connections (eg. id, userLabel)

REQ-MT (40) Network resources (managed objects) shall be named using a harmonised naming convention. The naming convention must uniquely identify the network resources

REQ-MT (41) It is required to have a 1:1 relation between Event Managed Object Instances and Inventory Managed Object Instances. If Managed Object (MO) identifiers used/ provided by the inventory equipment of an element manager need to be mapped to meet naming requirements of the inventory database, the same mapping must be applied to the MO identifiers in the event. The corresponding is true if mapping is driven by event naming requirements.
If MO identifiers of events and inventory within an element manager are different, the difference must be eliminated before the above mapping can be applied.
Rationale:
An event must be unambiguously related to a known Object Instance (in the inventory).

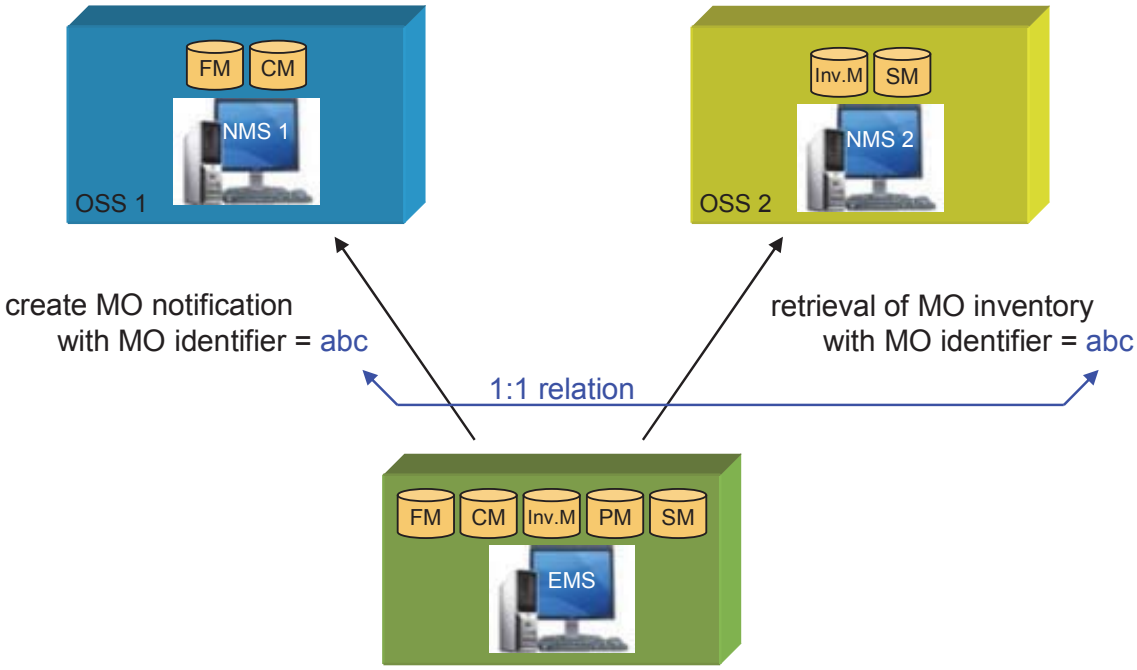

Figure 27: Event / Inventory relation

REQ-MT (42) The information in the "Managed Object" attribute of the interface must allow a clear and unambiguous identification of the resource (HW or SW), which is the originator of the event.

- The Managed Object, as an attribute of the basic generic event object, shall not contain any detailed topology information. The assumption is that the NMS will use an inventory database (internal or external) to map between Managed Object Instance and inventory topology tree if needed.
- The basic assumption for this is that there is a one-to-one mapping between Managed Object Instance and the inventory information, so that the instance can be unambiguously identified. If this is not the case, the instance must contain a very simple and standardized methodology to describe the relationship between the first unambiguously identifiable object and the related not-unambiguously identifiable object, which is the originator of the event

REQ-MT (43) The Federated Model shall provide the static (read only attributes) and dynamic (create/ delete/ modify objects; modify attributes)

REQ-MT (44) The Federated Model shall provide a common identification mechanism (format) of entities

REQ-MT (45) The Federated Model shall enable the correlation of the network data:

- between different layers and technologies in fixed networks (eg, WDM, SDH/S ONET, ATM, IP/MPLS)
- in fixed and mobile networks (eg, IP/ MPLS <-> RAN, WDM <-> core network)
- from different resources in mobile networks (RAN, core network, etc.)
- from different mobile network technologies (eg, WiMAX, WLAN, LTE, UMTS, etc.)

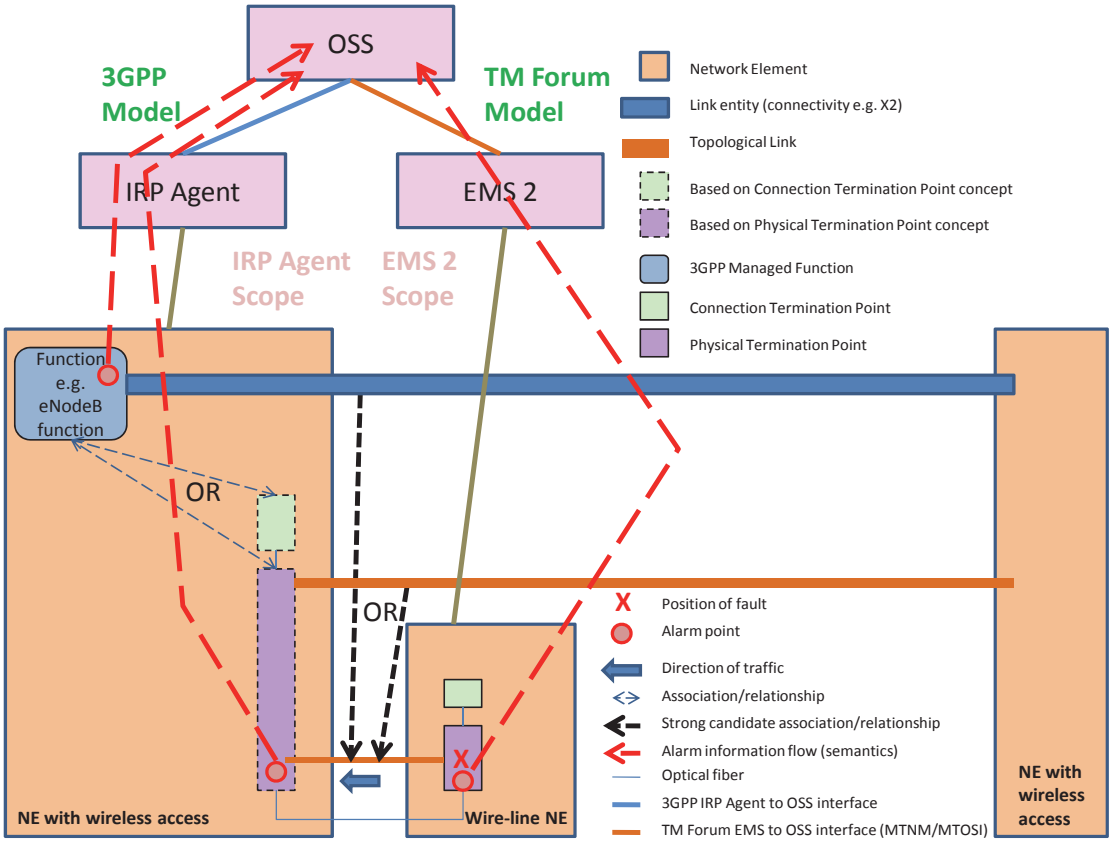

Figure 28: Example OSS receives the alarms from different EMS and different models

(Mobile Network model from 3GPP model and Fix Network model from TMF model) (Figure extracted from [37])

REQ-MT (46) The SDOs/ organisations shall specify the Federated Model in a protocol neutral way using UML

REQ-MT (47) The Umbrella Model shall be governed by all participating SDOs/ organisations via a dedicated cross-SDOs/ organisations structure

REQ-MT (48) The Federated Model shall be machine readable

REQ-MT (49) The Federated Model shall also be delivered in the portable document format (PDF)

REQ-MT (50) The modelling of the SDO/ organisation-specific enhancements shall be based on the Umbrella Model

REQ-MT (51) Traceability between model and requirements/ use cases shall be provided in two ways:

1. Where appropriate, a UML artefact should reference the corresponding requirement and/ or use case identifier in the documentation field
2. Traceability matrices shall be provided for:
   - mapping from object classes to requirements
   - mapping from object class attributes to requirements
   - mapping from object class operations to requirements
   - mapping from object class operations to use cases
   - mapping from use cases to requirements

REQ-MT (52) Multiple NMS applications might be connected (logically) to several EMS applications (M : N). The interface specification must allow to connect one NMS to multiple EMS. (This might have an impact on addressing – mechanisms in the interface).
Furthermore the interface specification must allow splitting the incoming event/ alarm traffic between different instances of the same interface implementations to avoid overload situations in one interface instance
Rationale:
This capability allows reducing the effort for the maintenance of several different client-side interfaces

REQ-MT (53) The Federated Model shall cover network resources with dimensions of “physical resources" and "logical resources"

REQ-MT (54) The Federated Model shall provide the relationship of network resources from different networks (e.g., wireless network, core network, transmission network, IP network, switching network, etc.), such as correlation of wireless network resource and transmission network resource can be easily learned

REQ-MT (55) The Federated Model shall support to provide the uniform view of resources from different networks, such as end-to-end topology of network resources

REQ-MT (56) The Federated Model shall be used as an equipment information template, since it is useful to implement large quantities of network equipment instances. An equipment information template can provide information rules of verification and constraints for card/ bay/ slot/ rack, thereby it shall improve the data accuracy and quality of the stock of equipment resources to support network resource lifecycle management

4.5.1.4 Model Artefact Property Requirements

This chapter defines the requirements for the properties of the model artefacts:

- managed object classes
- attributes
- service interfaces (grouping of operations in the FOM)
- operations
- parameters
- notifications
- data types
- relationships between managed object classes
- UML diagrams

Editor's notes: Requirements for extension mechanisms may need to be added. The definition of the multiplicity in the meta model may be too restrictive.

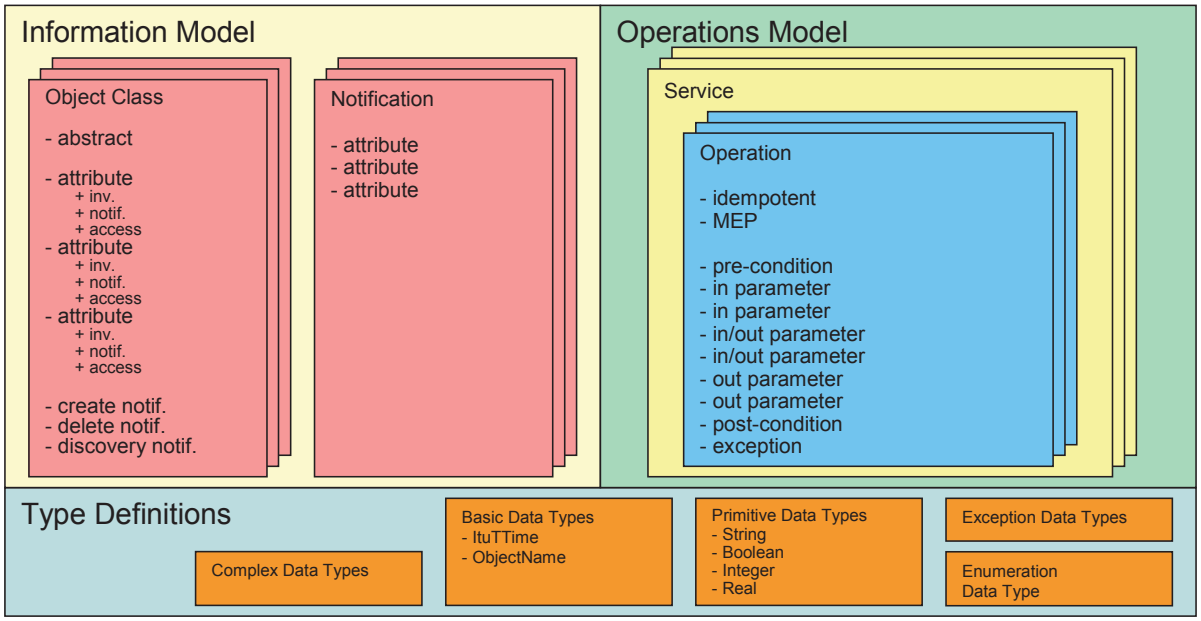

Figure 29: Model Artefacts

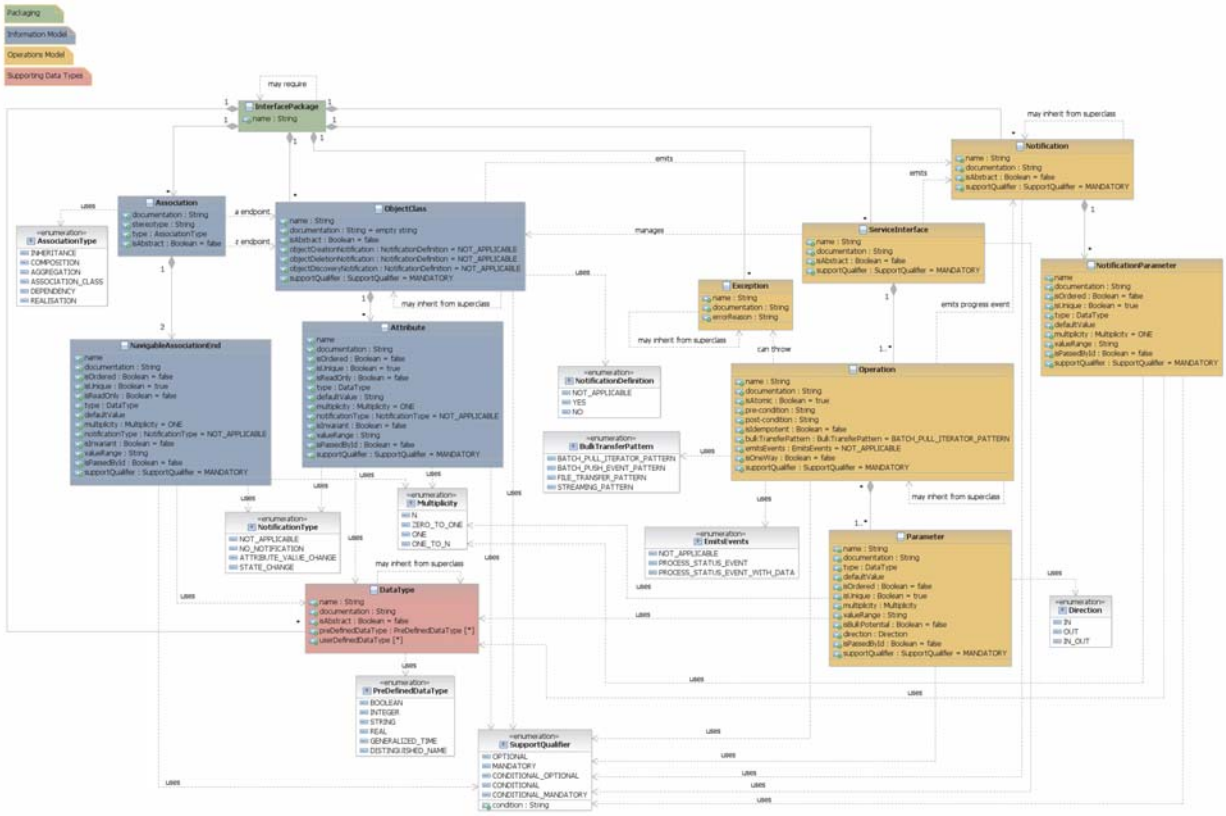

Figure 30: Meta-Model

4.5.1.4.1 Object Class Requirements

Object classes are used to model data entities in the Information Model and shall be derived from the static requirements.

REQ-MT (57) An object class shall have the following properties:

- Object Class name
  Shall follow Upper CamelCase (UCC)
  The complete Distinguished Name (DN) having this name as a equipment must be unique across an interface instance
- Object Class description
  Shall contain a textual description of the object class
  Shall refer (to enable traceability) to the appropriate requirement
- Superclass(es)
  Inheritance and multiple inheritance may be used
- Abstract Object Class
  Indicates if the object class can be instantiated or is just used for inheritance
- Required Object Notifications
  Shall identify if creation/ deletion notifications are to be send
  "objectCreationNotification" <NO | YES | NOT_APPLICABLE>
  "objectDeletionNotification" <NO | YES | NOT_APPLICABLE>
  "objectDiscoveryNotification" <NO | YES | NOT_APPLICABLE>
- Support Qualifier
  Identifies the required support of the object class: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

REQ-MT (58) An attribute within an object class shall have the following properties:

- Attribute name
  Shall follow Lower CamelCase (LCC)
  - Boolean typed attribute names shall always start with a verb like ‘is’, 'must', etc. (e.g., ‘isAbstract’) and the whole attribute name must be composed in a way that it is possible to answer it by "true" or "false"
  - Enumeration typed attributes always end with “Kind” (e.g., ‘aggregationKind’)
  - List typed attributes shall end with the word "List"
  - Attributes referencing an instance identifier shall contain the word "Ref"
- Attribute description
  Shall contain a textual description of the attribute
  Shall refer (to enable traceability) to the specific requirement
- Qualifiers
  - Ordered
    For a multi-valued multiplicity; this specifies whether the values in an instantiation of this attribute are sequentially ordered; default value is false
  - Unique
    For a multi-valued multiplicity, this specifies whether the values in an instantiation of this attribute are unique (i.e., no duplicate attribute values are allowed); default value is true

  Excerpt from UML superstructure specification, [44]: *When isUnique is true (the default) the collection of values may not contain duplicates. When isOrdered is true (false being the default) the collection of values is ordered. In combination these two allow the type of a property to represent a collection in the following way:*

isOrdered	isUnique	Collection type
false	True	Set
true	True	OrderedSet
false	False	Bag
true	False	Sequence

Table 2: Collection types for properties

(Table extracted from UML Superstructure Specification [44])

- Read Only
  If true, the attribute may only be read, and not written by the client OS. The default value is false
- Type
  Refers to a pre-defined or user-defined data type; see also chapter 4.5.1.4.7
- Default Value
  Provides the value that the attribute has to start with in case the value is not provided during creation or already defined because of a system state
- Multiplicity
  Defines the number of values the attribute can simultaneously have
- Attribute Notifications
  Identifies if a notification has to be sent in case of a value change
- Invariant
  Identifies if the value of the attribute can be changed after it has been created; default value is "False"
- Value Range
  Identifies the allowed values the attribute can have
- Passed by Id
  Identifies if the attribute contains just a pointer to the information (passed by id = true) or contains the whole information itself (passed by id = false); default value = "false"
- Support Qualifier
  Identifies the required support of the attribute: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

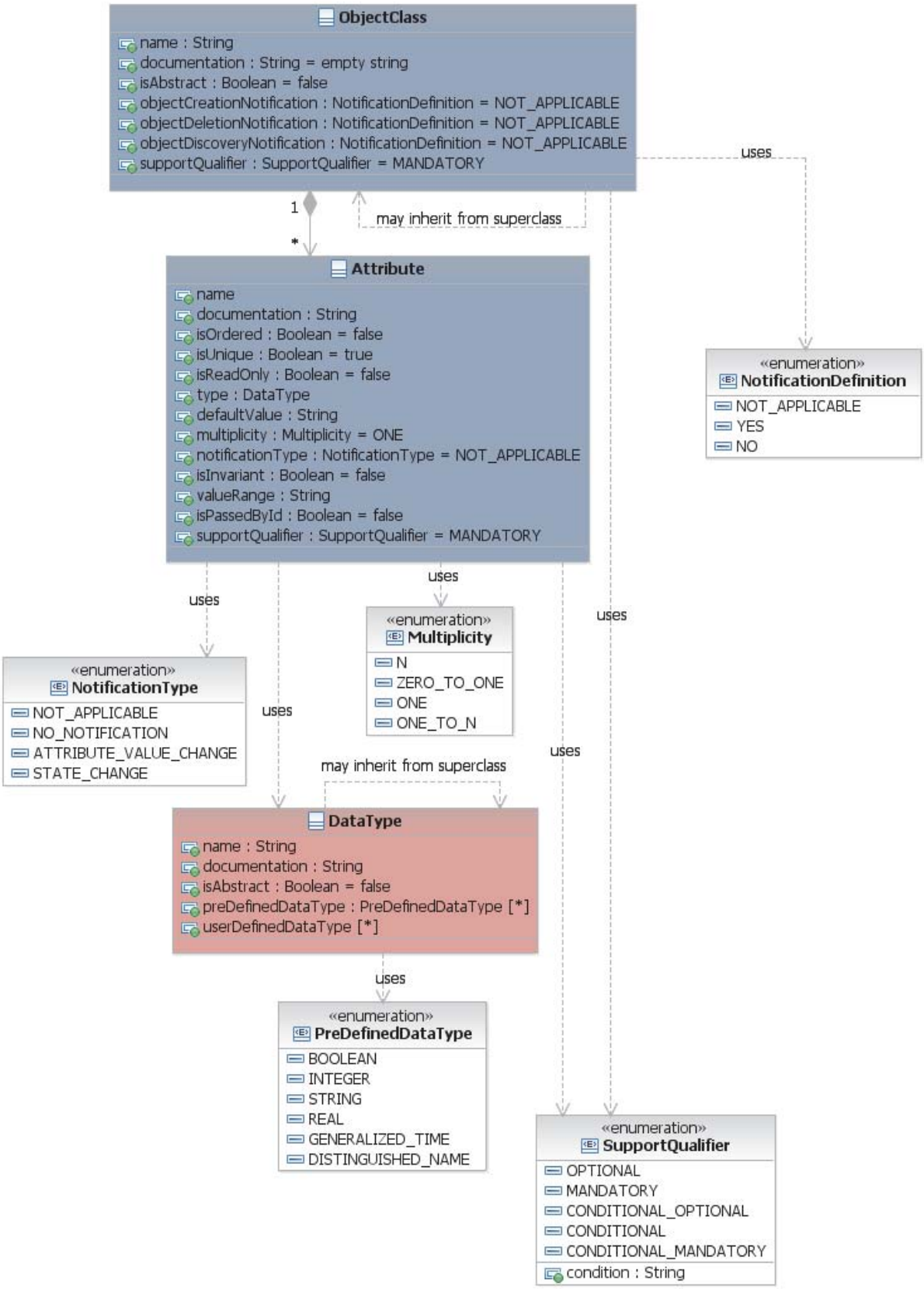

Figure 31: Meta Model: Object Class

4.5.1.4.2 Service Interface Requirements

REQ-MT (59) Interface object classes shall be used to model the interfaces in the operations model and shall be derived from the dynamic requirements

REQ-MT (60) A service interface shall have the following properties:

- Service interface name
  Shall follow Upper CamelCase (LCC)
  Shall be expanded by the word "Service"
- Service interface description
  Shall contain a textual description of the service interface
  Shall refer (to enable traceability) to the specific requirement
- Support Qualifier
  Identifies the required support of the service interface: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

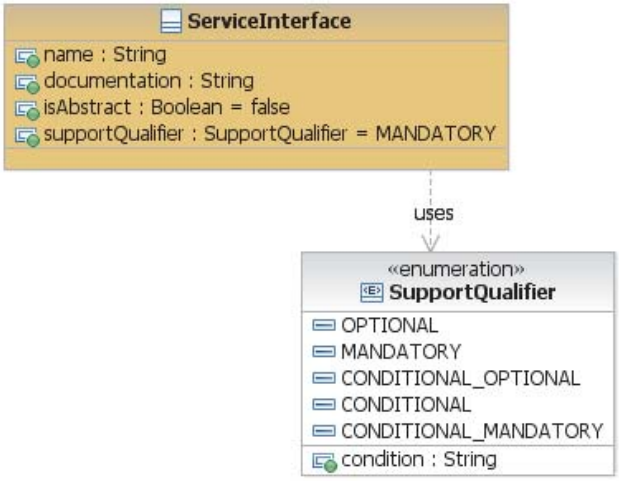

Figure 32: Meta-Model: Service Interface

4.5.1.4.3 Operation Requirements

REQ-MT (61) Operations shall be grouped in interface object classes and shall be derived from the dynamic requirements and usage scenarios

REQ-MT (62) An operation shall have the following properties:

- Operation name
  Shall follow Lower CamelCase (LCC)
- Operation description
  Shall contain a textual description of the operation
  Shall refer (to enable traceability) to the specific requirement
- Atomic
  Identifies if the operation is best effort or is successful/ not successful as a whole
- Return Type
  Shall be fixed to "void"

- Pre-condition(s)
  Shall list the conditions that have to be true before the operation can be started (i.e., if not true, the operation will not start at all)
  Note: It is recommended to define the pre-condition in OCL
- Parameter(s)
  Refer to specific requirement below
- Post-condition(s)
  Shall describe the state of the system after the operation has been successfully executed
  Note: It is recommended to define the post-condition in OCL
- Idempotency
  Defines if the operation is idempotent or not
- Bulk Transfer Pattern
  The Bulk Transfer Pattern fully identify the messages and the choreography (sequencing and cardinality) of the messages independently from a business activity; default value is "batch pull iterator pattern"
  The following distinct communication patterns are required:
  - Batch pull iterator pattern
  - Batch push event pattern
  - File transfer pattern
  - Streaming pattern
- Emits events
  Identifies the operation as a process status event with/ or without associated data; default value = "not applicable"
- One way
  The operation is one way, when it has only input parameter or only output parameter; default value = "false"
- Operation Exceptions
  The allowed exceptions together with a failure reason shall be defined for each operation
- Support Qualifier
  Identifies the required support of the operation: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

REQ-MT (63) The following list of common exceptions shall be supported by the operations:

- AlreadyInPostCondition
  This exception can be used by operations which are not defined as idempotent. It is used to indicate that the target OS is already in the post-condition
- AtomicTransactionFailure
  This exception shall be raised when an atomic operation is not successful due to a failure of one of its sub-parts. The failure reason shall indicate which object/ part failed
- CapacityExceeded
  This exception shall be raised when the request will result in resources being created or activated beyond the capacity supported by the NE or target OS
- Duplicate
  This exception shall be raised if an object instance cannot be created because an object with the same identifier/name already exists
- EntityNotFound
  This exception shall be raised when the specified object does not exist
- FilterNotSupported
  This exception shall be raised when a filter definition is not supported by the implemented filter. The failure reason shall indicate the more precise reason

- InventoryOutOfSync
  This exception shall be raised when the operation fails because the inventory data bases from the target and requesting OS are out of sync
- NotInValidState
  This exception shall be raised when the state of the specified object is such that the target OS cannot perform the operation
- ObjectInUse
  This exception shall be raised when the object identified in the request is currently in use
- UnableToNotify
  This exception shall be raised when the target OS is unable to connect to the Notification Service
- CommunicationLoss
  This exception shall be raised when the target OS is unable to communicate with the subordinate OS
- InternalError
  This exception shall be raised when the request has resulted in an OS internal error
- NotImplemented
  This exception shall be raised when the target OS does not support this operation
- UnableToComply
  This exception shall be raised when the target OS cannot respond to the request
- AccessDenied
  This exception shall be raised when the requesting OS is not permitted to perform the operation
- InvalidInput
  This exception shall be raised when the operation contains an input parameter that is syntactically incorrect or identifies an object of the wrong type or is out of range

REQ-MT (64) The following common exceptions shall be supported by all operations:

- AccessDenied
- CommunicationLoss
- InternalError
- InvalidInput
- NotImplemented
- UnableToComply

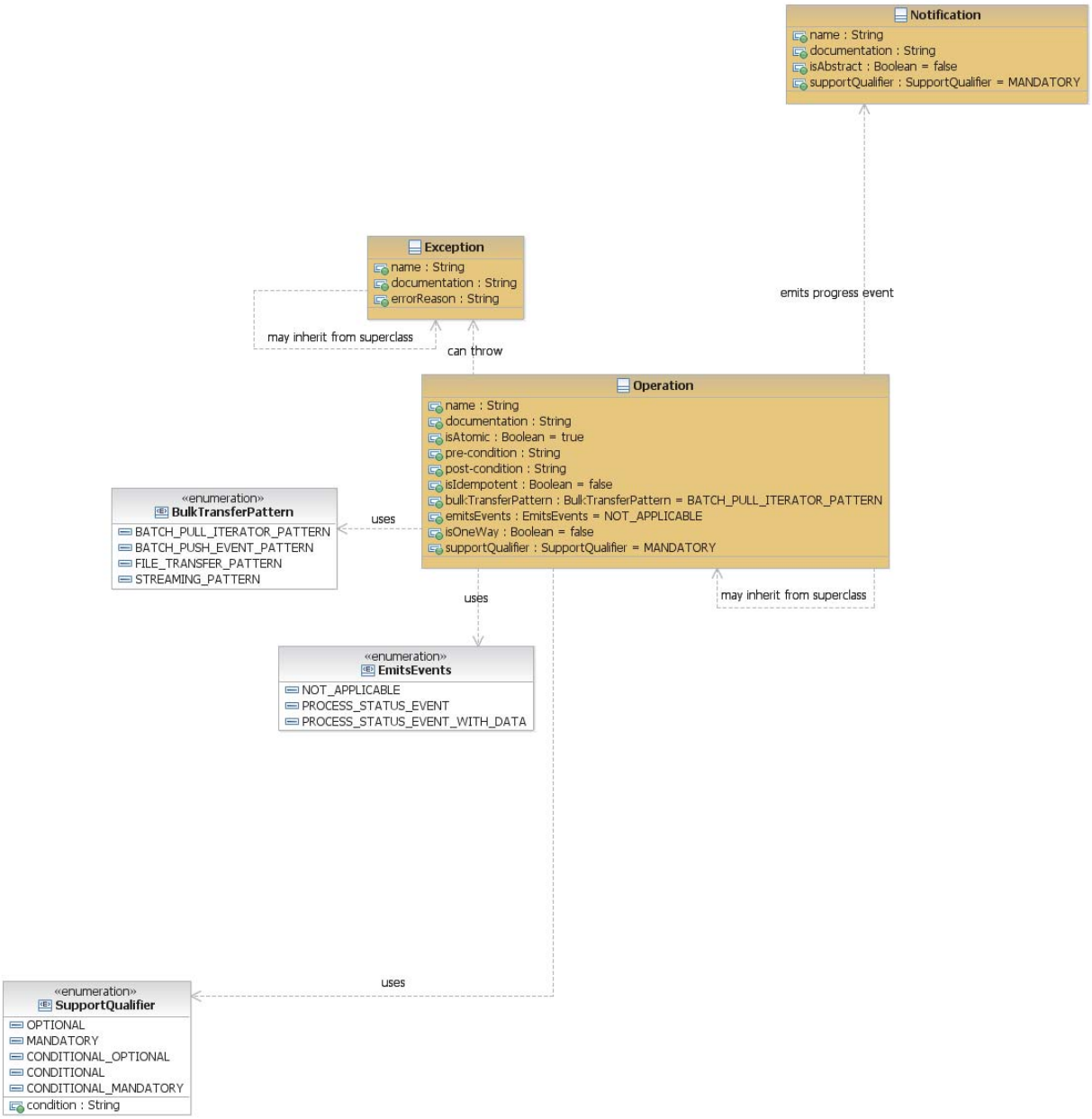

Figure 33: Meta-Model: Operation

4.5.1.4.4 Operation Parameter Requirements

REQ-MT (65) Each parameter within an operation shall have the following properties:

- Parameter name
  Shall follow Lower CamelCase (LCC)
- Parameter description
  Contains a textual description of the parameter.
  Shall refer (to enable traceability) to the specific requirement
- Type
  Shall refer to a basic or complex data type

Note: A list of input (in a few cases also output) parameters could also be combined in a data type

- Default Value
  Provides the value that the parameter has to start with in case the value is not provided
- Ordered
  For a multi-valued parameter; the order of the values is important
- Unique
  For a multi-valued parameter, no duplicate values are allowed
- Multiplicity
  Defines the number of values the parameter can simultaneously have
- Value Range
  Identifies the allowed values the attribute can have
- Bulk Potential
  Indicates that this parameter can potentially carry a very large amount of data which will require a bulk data transfer pattern
- Direction
  In | InOut | Out
- Passed by Id
  Identifies if the parameter contains just a pointer to the information (passed by id = true) or contains the whole information itself (passed by id = false); default value = "false"
- Support Qualifier
  Identifies the required support of the operation: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

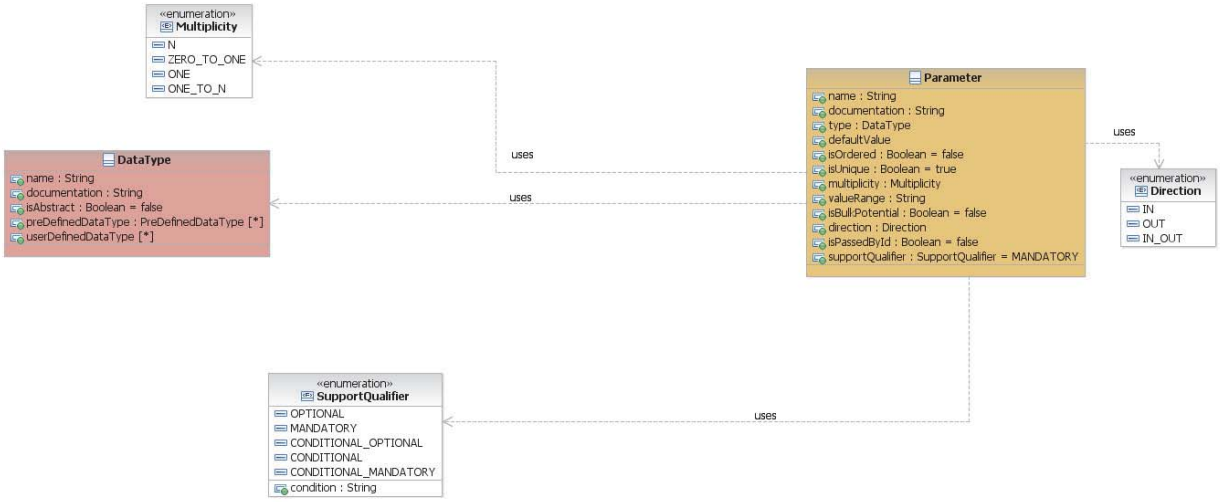

Figure 34: Meta-Model: Operation Parameter

4.5.1.4.5 Notification Requirements

REQ-MT (66) Object classes shall be used to model the notifications in the Information Model

REQ-MT (67) Notifications shall have the following properties:

- Notification name
  Shall follow Upper CamelCase (UCC)
  Shall end with the word "Notification" (e.g., EquipmentProtectionSwitchNotification)

- Notification description
  Contains a textual description of the parameter
  Shall refer (to enable traceability) to the appropriate requirement
- Superclass(es)
  Inheritance and multiple inheritance may be used
- Abstract Object Class
  Indicates if the notification can be instantiated or is just used for inheritance
- Support Qualifier
  Identifies the required support of the notification: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

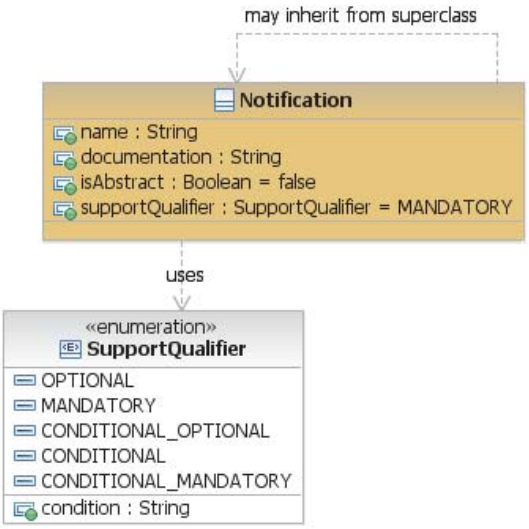

Figure 35: Meta-Model: Notification

4.5.1.4.6 Notification Parameter Requirements

The information which has to be provided by a notification is contained in the notification parameters which are modelled as attributes of Notification object classes.

REQ-MT (68) Notification Parameters shall have the following properties:

- Parameter name
  Shall follow Lower CamelCase (LCC)
  Shall follow the naming conventions defined for the object class attribute names defined in chapter 4.5.1.4.1
- Parameter description
  Contains a short textual description of the parameter
  Shall refer (to enable traceability) to the specific requirement
- Type
  Refers to a basic or complex data type
- Passed by Id
  Identifies if the parameter contains just a pointer to the information (passed by id = true) or contains the whole information itself (passed by id = false); default value = "false"

- Support Qualifier
  Identifies the required support of the notification parameter: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

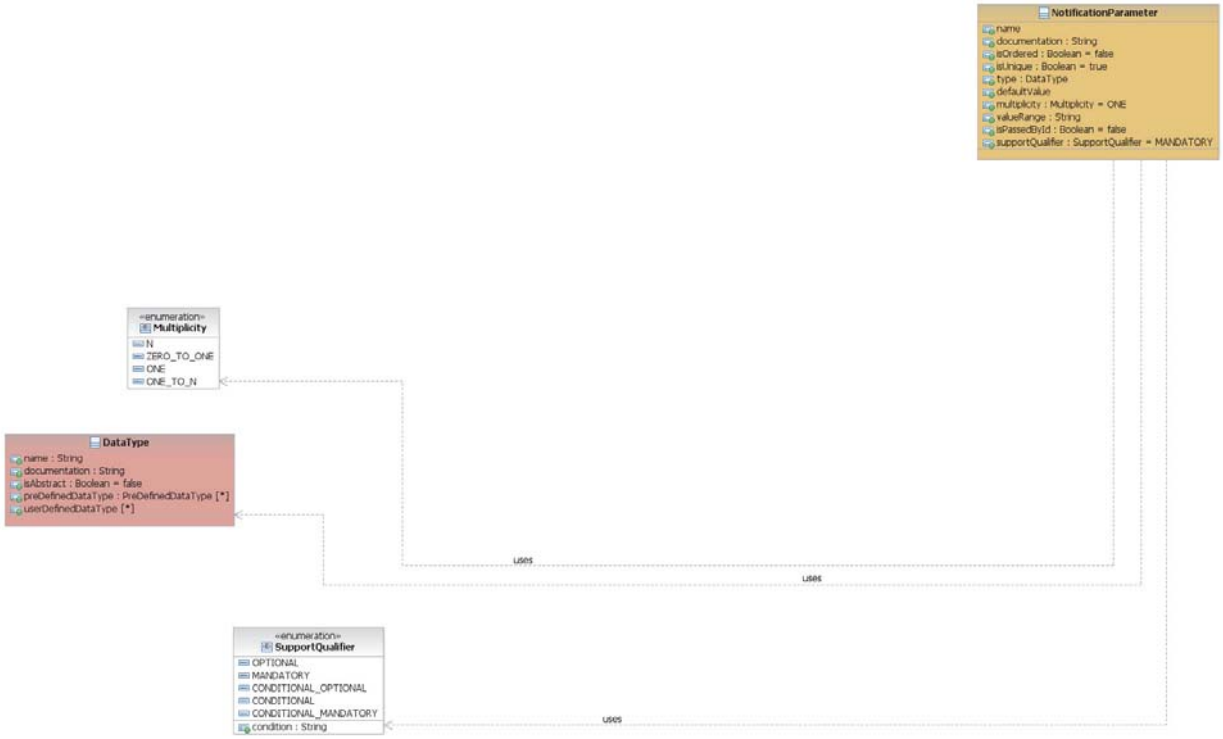

Figure 36: Meta-Model: Notification Parameter

4.5.1.4.7 Data Type Requirements

Data Types are distinguished between "pre-defined" and "user-defined" data types.

REQ-MT (69) The following pre-defined data types shall be used:

- Boolean
- Integer
- Real
- String
- DistinguishedName
  The DistinguishedName has to be used for the unique, read-only name of an object. The exact type is protocol specific
- GeneralizedTime
  "yyyyMMddhhmmss.s[Z|{+|-}HHMm]" where:

yyyy	"0000".."9999"	year
MM	"01".."12"	month
dd	"01".."31"	day
hh	"00".."23"	hour
mm	"00".."59"	minute
ss	"00".."59"	second
s	".0".."9" tenth of second (set to ".0" if EMS or ME cannot support this granularity)	

Z	"Z"	indicates UTC (rather than local time)	
{+|-}		"+" or "-" delta from UTC	
HH		"00".."23"	time zone difference in hours
Mm		"00".."59"	time zone difference in minutes

REQ-MT (70) User-defined data types shall have the following properties:

- Data type name
  Shall follow Upper CamelCase (UCC)
- Data type description
  Shall contain a textual description of the data type
  Shall refer (to enable traceability) to the appropriate requirement
- Attributes within data types
  Data type attributes have the same properties as the object class attributes; see chapter 4.5.1.4.1

REQ-MT (71) The literals of Enumeration data types shall have only upper case characters; words are separated by "_"

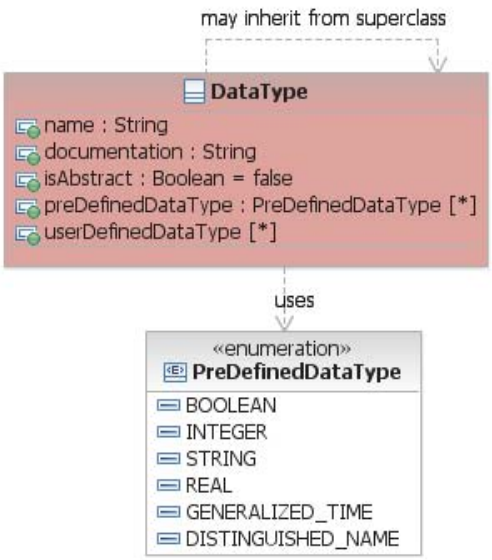

Figure 37: Meta-Model: Data Type

4.5.1.4.8 Association Requirements

REQ-MT (72) Associations shall have the following properties:

- Association description
  Shall contain a textual description of the association
  Shall refer (to enable traceability) to the appropriate requirement
- Stereotype
  E.g., <<naming>> shall be used if the association defines the object naming tree
- Association Type
  E.g., inheritance, association (composition, aggregation, and association class), dependency, and realisation
  An association may represent a composite aggregation (i.e., a whole/part relationship).

Only binary associations can be aggregations. Composite aggregation is a strong form of aggregation that requires a part instance be included in at most one composite at a time. If a composite is deleted, all of its parts are normally deleted with it. Note that a part can (where allowed) be removed from a composite before the composite is deleted, and thus not be deleted as part of the composite. Compositions may be linked in a directed acyclic graph with transitive deletion characteristics; that is, deleting an element in one part of the graph will also result in the deletion of all elements of the sub graph below that element. Composition is represented by the isComposite attribute on the part end of the association being set to true

- Role names

  Identifies the role that the object plays at the navigable end of the relationship
  Shall follow Lower CamelCase (LCC)
  Navigable association ends will lead to an attribute in the remote object class. Therefore, the name shall follow the naming conventions defined for the object class attribute names defined in chapter 4.5.1.4.1
  Note: Only navigable relationships have role names
- Constraint(s)

  List the constraint(s) under which the association can exist
- Abstract

  It is recommended to create associations which are just for explanation to the reader of the model. These associations should be defined as "abstract", they are not navigable and have no role names. They shall not be taken into account in the protocol specific specification. This can for example be used to show the association to the object which is retrieved by a get-operation.

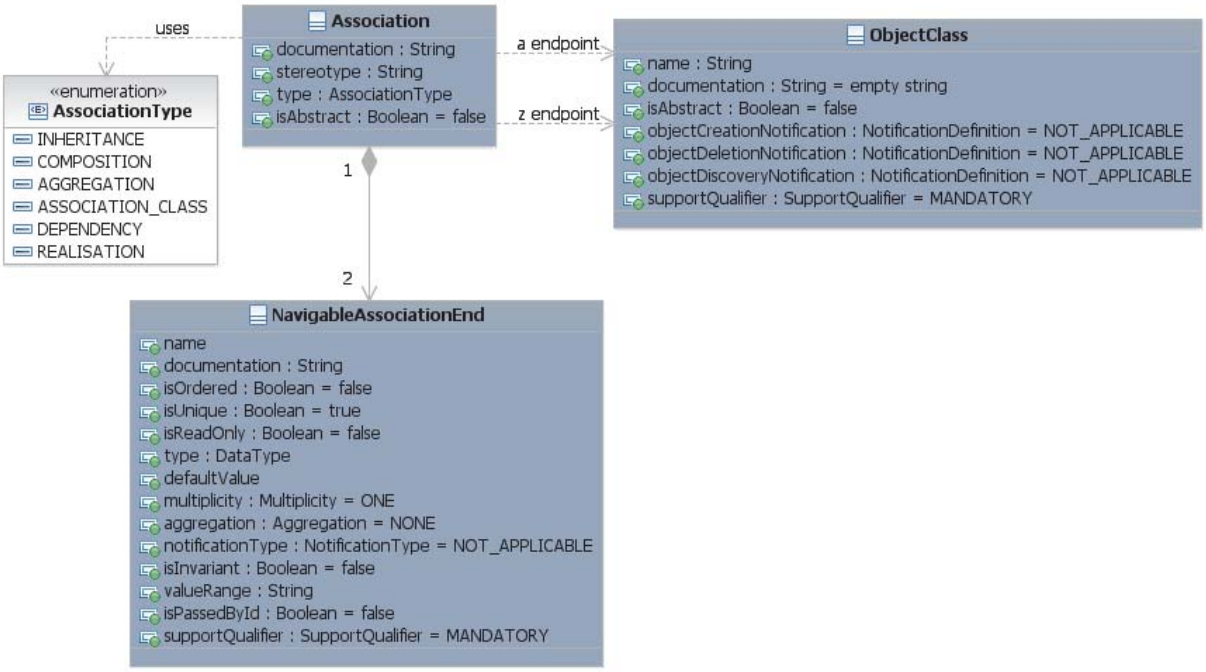

Figure 38: Meta-Model: Association

REQ-MT (73) A navigable association end shall have the following properties:

- Name
  Shall follow Lower CamelCase (LCC)
  - Boolean typed association end names shall always start with a verb like ‘is’, 'must', etc. (e.g., ‘isAbstract’) and the whole association end name must be composed in a way that it is possible to answer it by "true" or "false"
  - Enumeration typed association end always end with “Kind” (e.g., ‘aggregationKind’)
  - List typed association ends shall end with the word "List"
  - Association ends referencing an instance identifier shall contain the word "Ref"
- Description
  Shall contain a textual description of the association end
  Shall refer (to enable traceability) to the specific requirement
- Qualifiers
  - Ordered
    For a multi-valued multiplicity; this specifies whether the values in an instantiation of this association end are sequentially ordered; default value is false
  - Unique
    For a multi-valued multiplicity, this specifies whether the values in an instantiation of this association end are unique (i.e., no duplicate association end values are allowed); default value is true

Excerpt from UML Superstructure Specification, [44]: *When isUnique is true (the default) the collection of values may not contain duplicates. When isOrdered is true (false being the default) the collection of values is ordered. In combination these two allow the type of a property to represent a collection in the following way:*

isOrdered	isUnique	Collection type
False	True	Set
True	True	OrderedSet
False	False	Bag
True	False	Sequence

Table 3: Collection types for properties
(Table extracted from UML Superstructure Specification [44])

  - Read Only
    If true, the association end may only be read, and not written by the Requesting OS. The default value is false
- Type
  Refers to a pre-defined or user-defined data type; see also chapter 4.5.1.4.7
- Default Value
  Provides the value that the association end has to start with in case the value is not provided during creation or already defined because of a system state
- Multiplicity
  Defines the number of values the association end can simultaneously have
- Notifications
  Identifies if a notification has to be sent in case of a value change
- Invariant
  Identifies if the value of the association end can be changed after it has been created; default value is "False"
- Value Range
  Identifies the allowed values the association end can have

- Passed by Id
  Identifies if the association end that points to an object contains just a pointer to the object (passed by id = true) or contains the whole object information itself (passed by id = false); default value = "false"
- Support Qualifier
  Identifies the required support of the association end: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

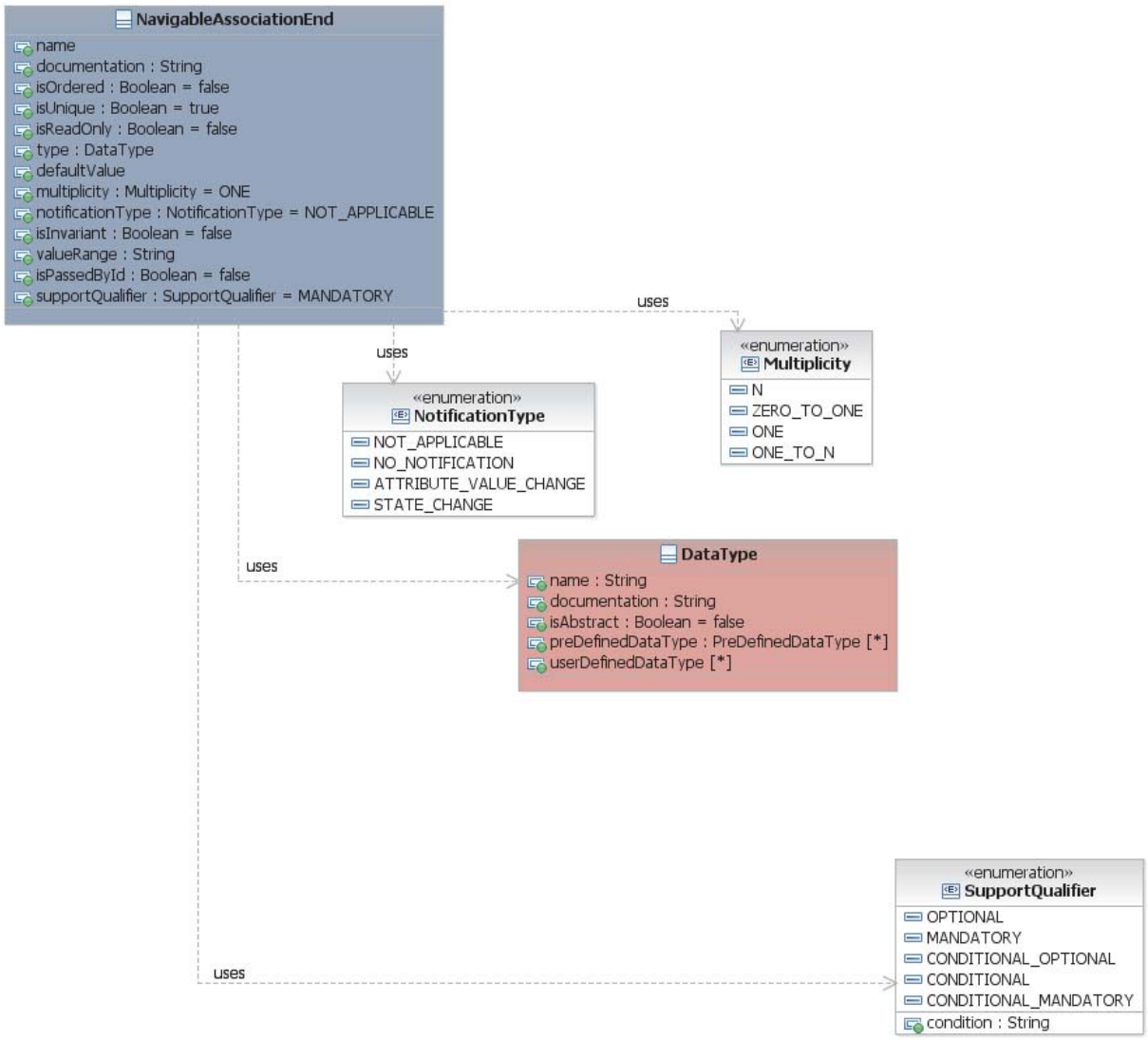

Figure 39: Meta-Model: Association End

4.5.1.4.9 UML Diagram Requirements

REQ-MT (74) Objects and their relationships shall be presented in class diagrams

REQ-MT (75) It is recommended to create

- An overview class diagram containing all object classes related to a specific management area (Class Diagram)
- An overview interface diagram containing all interfaces related to a specific management area (Interface Diagram)
- A separate inheritance class diagram in case the overview diagram would be overloaded when showing the inheritance structure (Inheritance Class Diagram)
- A class diagram containing the defined notifications (Notifications Diagram)
- A class diagram containing the defined data types (Type Definitions Diagram)
- Additional class diagrams shall be established to show specific parts of the specification in detail
- State diagrams shall be created for complex state attributes
- Activity diagrams\Sequence Diagrams shall be created for complex operations
- The class name compartment shall contain the "Qualified Name"
- The class attributes and operation shall show the "Signature"

4.5.1.5 Infrastructural Requirements

REQ-MT (76) The SDOs/ organisations shall agree on a list of common modelling patterns defined in a kind of meta-model

REQ-MT (77) The SDOs/ organisations shall integrate the existing models into the Federated Model through "translators" and/ or "adapters". For new technologies, the modelling shall be based on the Federated Model. They shall also define a migration path which allows bringing appropriate parts of the present individual models into the common Umbrella Model

REQ-MT (78) It shall be possible to use the Federated Model (and its SDO/ organisation-specific enhancements) as input to a tool based Interface development process

REQ-MT (79) The SDOs/ organisations shall agree on a common UML version (e.g., 2.3)

REQ-MT (80) The SDOs/ organisations shall use – if possible – open source modelling tools. XMI shall be used as common interchange format

4.5.2 Tooling Requirements

4.5.2.1 General Requirements

REQ-MT (81) The creation of the specification shall be tool supported.

REQ-MT (82) Open interchange formats shall be agreed to export/import data between the tools in the chain.

REQ-MT (83) A **single** tool shall be used to map/transform the protocol-neutral specification into the protocol-specific specification.

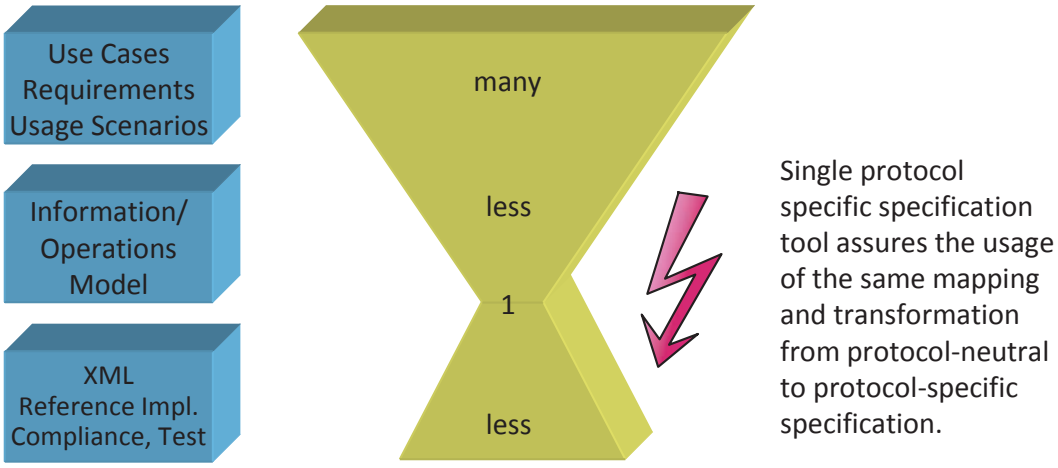

Figure 40: Number of Tools in the Tool Chain

REQ-MT (84) The dynamic Operations Models from wireline and wireless technologies have to be harmonised. The harmonisation shall concentrate on:

- Common operations (basic operations for create/ delete, modification and retrieval)
- Common exceptions
- Common notifications
- Common extendibility patterns
- Common message Exchange patterns
- Common scheduling mechanisms
- Common filter mechanisms

REQ-MT (85) The complete Information and Operations Models shall be part of standardized specifications and made available in a machine readable format

REQ-MT (86) The interface specification shall be tool supported to significantly reduce the time to market for those who are specifying and implementing the interfaces

REQ-MT (87) The interface protocol specification shall be created automatically supported by a single software tool to ensure the usage of common design guidelines.
Using a single tool increases also the interoperability of the specified interfaces

REQ-MT (88) The tool shall be able to provide:

- an XML based interface protocol specification (web services)
- interface documentation
- input for a reference implementation
- input for a compliance and test tool kits
- traceability mechanisms, e.g. between requirements and protocol neutral Information Model and between protocol neutral Information Model to protocol-specific parts

REQ-MT (89) The tool shall be developed outside of any specific standardisation body in an open source environment.
This allows the usage of the tool by other standardisation bodies

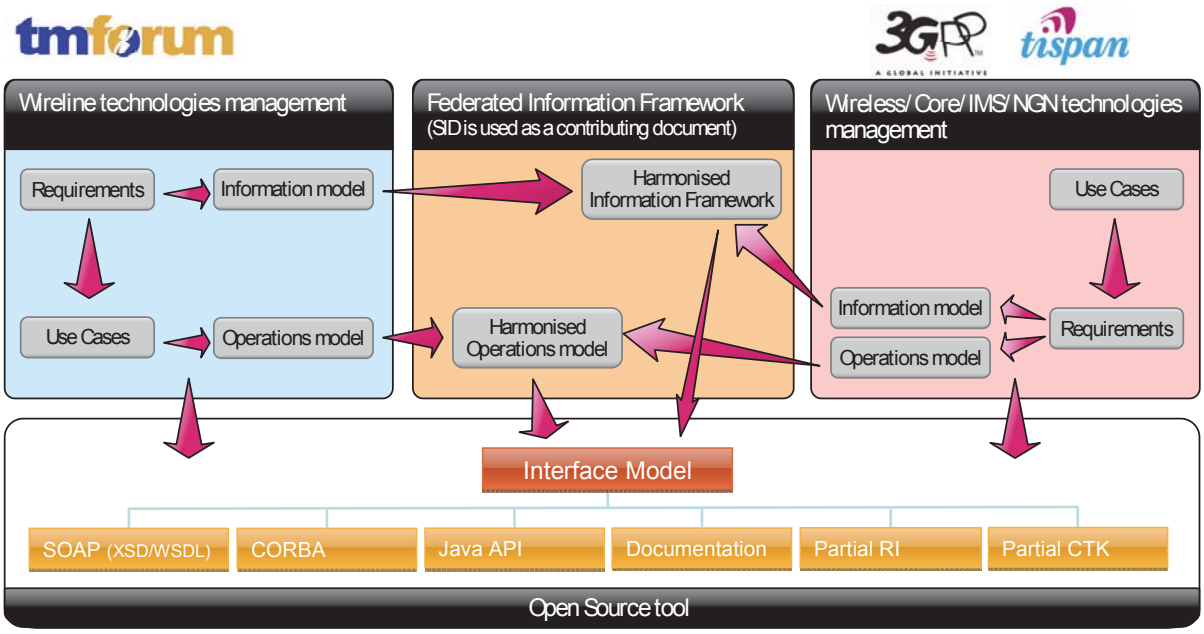

Figure 41: Modelling/Tooling Architecture

4.5.2.2 General Pattern Requirements

REQ-MT (90) The tool shall provide general patterns to ensure a common basis for all interfaces

4.5.2.2.1 Object Identifier Pattern

REQ-MT (91) The tool shall add a globally unique object identifier to every object to uniquely identify the object across an interface

REQ-MT (92) The object identifier shall contain a context, a distinguished name and a type

4.5.2.2.2 Common Exceptions Pattern

REQ-MT (93) The tool shall provide two types of common exceptions: predefined common exceptions and optional common exceptions.
The predefined common exceptions shall be automatically inserted into all operations by the tool
The optional common exceptions shall be inserted into the operations by the tool on request

REQ-MT (94) All exceptions shall be able to provide a reason and a details description

REQ-MT (95) The following list of predefined common exceptions shall be automatically inserted into all operations by the tool:

- InternalException (default exception)
- AccessDenied
- CommunicationLoss
- InternalError

- InvalidInput
- NotImplemented
- UnableToComply

For a description of the exceptions see chapter 4.5.1.4.3

REQ-MT (96) The following list of predefined common exceptions shall be automatically inserted into all operations by the tool:

- AlreadyInPostCondition
- AtomicTransactionFailure
- CapacityExceeded
- Duplicate
- EntityNotFound
- FilterNotSupported
- InventoryOutOfSync
- NotInValidState
- ObjectInUse
- UnableToNotify

For a description of the exceptions see chapter 4.5.1.4.3

4.5.2.2.3 Iterator Pattern

REQ-MT (97) The tool shall support a common iterator pattern for bulk data transfer

REQ-MT (98) The iterator pattern shall contain the following functionality:

- IteratorInfo
  This is the Info contained in the first response to a bulk based request
- GetNextResponse
  This is the response object to a getNextRequest
- GetNextRequest
  This is the Iterator getNextRequest to retrieve the next batch of replies
- ReleaseRequest
  This is the Iterator release request to release all the associated resources and invalidate the iterator
- HasNext
  Resturns a Boolean; True meaning that additional data is available; false meaning that this is the last information
- Remove
  Deletes the information contained in the iterator
- IsEmpty
  Returns a Boolean; True meaning that iterator has no information; false meaning that the iterator contains still information
- ReleaseResponse
- IteratorNotFound
- InvalidIteratorContext

4.5.2.2.4 Notification Pattern

REQ-MT (99) The tool shall support common notifications

REQ-MT (100) The following types of notifications shall be provided:
- AttributeValueChangeNotification
- ObjectCreationNotification
- ObjectDeletionNotification
- ObjectDiscoveryNotification

REQ-MT (101) All notifications shall at least provide:
- Object identifier
- Object type
- Source time

4.5.2.2.5 Common Operations Pattern

REQ-MT (102) The tool shall support common operations covering create, delete, set and get associated to a single interface class

REQ-MT (103) It shall be possible for the common create operation to define a reference object (existing instance of a Managed Object). The attribute values associated with the reference object instance shall become the default values for those not specified by the also provided create data attribute values

REQ-MT (104) The tool shall support the following types of get operations:
- Single object get
  Getting the values of a single instance
- Multiple entities get
  Get all entities matching a filter; returning the attributes and values of the entities
- Multiple entities get by ids
  Get all entities matching a filter; returning only the identifiers of the entities

REQ-MT (105) The created Object Instances shall be returned

REQ-MT (106) It shall be possible to have all three types of get operations associated to the same interface class

REQ-MT (107) It shall be possible for the common delete operation to provide a list of Object Instances (object identifiers) to be deleted

REQ-MT (108) The delete operation shall return the list of Object Instances that could not be deleted

REQ-MT (109) The tool shall support the following types of set operations:
- Single object set
  Setting a single object; all attributes should be set in an atomic way
- Multiple entities set, best effort
  Setting all entities matching a filter in a best effort way
- Multiple entities set, atomic
  Setting all entities matching a filter in an atomic way

4.5.2.2.6 Filter Pattern

REQ-MT (110) The tool shall support a common filter construct (based on attribute values) for operations requiring the selection of Object Instances

REQ-MT (111) The filter construct shall be a template or a combination of a template and a query filter

REQ-MT (112) A query filter shall be mapped to a string which is implementation technology specific. For example in XML it is filled by the implementation with an XPATH expression. In Java it is filled by a JPA query expression

REQ-MT (113) A template filter shall be mapped to a sequence of attribute matching filters

4.6 Use cases

No use cases are defined in the Modelling and Tooling sub task.

5 Requirements for Fault Management Interface (FM)

5.1 Introduction

Today's Fault Management interfaces between Element Management Systems (EMS) and Network Management Systems (NMS) are based on a large variety of different technologies and standards. Each EMS which has been delivered to Service Providers (SP) in the past uses his own specific interface type and implements element-specific extensions and behaviour, which evolve over time, leading to a continuous need for upgrades on EMS side and to related adaptations/ upgrades on NMS side. SPs estimate of one major upgrade project per EMS per two to three years. The cost and effort for the EMS upgrades are often covered by the budgets for the related network element upgrades. But there are additional costs and effort for the related upgrade adapters/access-modules in the NMS-FM system, although the main requirements on such an interface are almost the same for the last ~ 15 years.

So SPs are driven by vendors to start interface upgrade projects, perform complex and time consuming type acceptance to ensure the needed quality, train administrators and project managers, etc. to get at least no additional value.

The authors of the FM section strongly believe, that there is potentially huge business benefit in using a common officially standardized technical approach, enabling the re-use of the same interface for different EMSs, enabling the planned exchange/ upgrade of the NMS-FM system and enabling us to stop vendor driven upgrades of interfaces which deliver no or small additional value.

So, the FM interface “plug & play” concept, described in the FM section, will be used as a goal for next generation service assurance.

In today's market, service providers aim to ever decrease the time-to-market of new and enhanced services in a cost-conscious manner. As a consequence, the need arises for existing OSS/ BSS infrastructure applications to adapt in an ever increasing pace. This affects OSS applications themselves and also increasingly their integration. Furthermore, there is a growing demand for automation of business processes at service providers, especially in the area of network/service operations to improve operational efficiency. This leads to the need for improved integration of OSS as a common demand from service providers. An integration strategy using SOA concepts, commonly adopted interface standards and NGOSS concepts like eTOM and SID might have the potential to deliver the needed technical basis for real life, standardized OSS integrations.

In the past, Service Providers often over-specified the tenders for FM interfaces and, on the other hand, opened to many degrees of freedom for the implementation of the interface. So they missed the opportunity to describe a simple, useable, maintainable interface, with a clear responsibility assignment between EMS and NMS.

Most of the existing integrations between Element Management systems and Network Management systems are based on proprietary point-to-point interfaces although vendors offer “standard” interfaces such as SNMP, CORBA, etc., which are adapted to their applications. In a real integration scenario these interfaces need a lot of customization to fulfil the business requirements and to allow the communication between different proprietary OSSs because each of these applications follow its own business process, internal logic and semantic. Usually application needs to know a part of the business logic of system B (and vice versa) to be able to implement the interface. This situation ends with the implementation of very specific interfaces with dependencies on the integrated OSS.

This means, re-use of interfaces or dedicated parts of the interfaces in other integration scenarios is not possible. So, there is a need for a standardized interface, which delivers the semantic connectivity and not only the underlying transport mechanisms, which helps to provide out-of-the-box interoperability and more flexible integration.

See also chapter 8.1 “Abstract” from NGMN Top OPE Requirements Version 1.0:

> “Although it is not the intention of the current document to specify implementation details, the operators expect the industry to jointly develop and use common standards, which deliver the semantic connectivity and not only the underlying transport mechanisms. The goal is to achieve out-of-the-box interoperability and more flexible integration, as well as the re-use of the same interfaces between OSS/BSS and the Network or EMS. Based on existing frameworks, provided by the standardization bodies, solutions should be implemented that support plug & play behaviour of network and OSS/BSS infrastructure. This will lead to more open interfaces to allow for 3rd party software integration. Amongst others this implies usage of common data models, e.g. based on SID, interface standards, such as SNMP and XML (if appropriate), and state-of-the-art technologies as SOA, web services, etc. As those standards are evolving over time, the operators resign from specifying exact software versions and implementation details. Our aim is to ensure upwards and downwards compatibility to ease integration of multi-vendor, multi-technology systems for all management areas.”

5.2 Scope

The main scope is the specification of the business requirements and related semantics, which describes the interaction of element management systems to network management (umbrella Fault Management) systems to exchange event/alarm information. The interface requirements support converged networks, that means that wireless and wireline networks are in scope.

In addition to this, there are specific requirements for the Element Management Systems and the Network Management Systems to use the capabilities of the specification in order to support the business requirements.
Please consider that different application topologies have to be supported by the interface:

- Several NMSs can be connected to the EMSs, e.g. operational NMS and test NMS
- An NMS can serve as an EMS (e.g. a technology domain specific NMS, which acts like an EMS to upper level NMS

5.3 Objective

The objective of the FM section is to deliver the specification of the major requirements for a unified, re-useable Fault Management Interface for the alarm interface between EMS → NMS. The FM section will serve as an input for standardization activities which address the FM interface standard.

The FM interface requirements are generic for FMC. They are completely independent from the network/service type which will be monitored by the EMS. So the FM interface requirements are valid for wireless and wireline networks, as well as for IT systems or service platforms.

Please consider that the FM section contains only mandatory requirements to deliver a basic, simple and cost efficient FM Interface. Additional requirements might be added later on as “optional”. (All requirements are “mandatory”, as long as they are not explicitly marked as “optional”). These requirements may not harm the business goals of the basic, mandatory requirements to achieve a simple, cost efficient and easy to integrate FM interface. It must be possible to implement an interface, which contains functionalities in line with the optional requirements, in a mixed mode with the simple/basic interfaces, which contain the mandatory requirements in this section, without any change for simple/basic interface (e.g. the EMS delivers just the mandatory interface

functionality and the NMS delivers also the optional part of the interface. In that case, the interface will use only the mandatory functionality, without any change on the EMS or NMS interface functionality).

Benefit and Drivers

The main benefit is achieved, as soon as the specification can be re-used to implement similar interfaces for different integration scenarios, to connect different EMS to NMS applications without creating a complete new implementation of the interface. The goal is to improve efficiency (in terms of cost and effort) for the integration of new EMS and to reduce cost and effort to maintain each single interface in a different way. Another benefit comes from the fact, that a real decoupled approach will reduce the effort to adapt both communication partners, in case there is a need to upgrade just one of the partners.

Saving potential:

- The support for a better level of standardization of the itf-N will reduce the integration effort between EMS and NMS (OSS) during the implementation and the life cycle of network technologies and related EMS.

Possible issues for guidance:

- "Plug & Play" integration of EMS into the OSS domain (no additional cost and effort during the implementation and the life cycle of network technologies and related EMS)
- De-coupling of EMS – OSS domains (changes on EMS or on NE may not lead to changes on OSS domain)
- Re-use of OSS clients of the interfaces

5.4 Methodology

It's the intention to describe the interface capabilities from business point of view, without technology specific requirements. That means, that these requirements reside on the semantically layer and not on protocol specifications. Nevertheless, there are some assumptions which might have an impact on the selected technology, e.g. the de-coupling of the interface specification (which is a basic requirement to support re-usability, exchange of SW versions, etc.) might have an impact on the technology. Furthermore the requirements have to be independent from the tool selection, so that they may not depend on specific tool capabilities.

Explanation of Prioritisation

Essential	→	The standard must fulfil this requirement. It is absolutely necessary and indispensable.
Major	→	The standard should fulfil this requirement. This is an important requirement. The value of the standard is reduced, if it cannot be fulfilled.
Minor:	→	The standard can fulfil this requirement (but must not). This is an optional requirement.

5.5 Requirements

5.5.1 Non-Functional Requirements for Fault Management Interface

The following topics describe some core business driven requirements for the EMS → *"alarm"* → NMS interface, independent from functional requirements. These requirements are not specific for the FM Use Cases and can be used as core "non-functional" requirements for other types of interfaces as well.

Note: The detailed descriptions of these "non-functional requirements" have been shifted into the Generic-Next-Generation-Converged-Operational-Requirements (GEN) section, because they are valid for most types of OSS interfaces.

The following list describes the prioritization of requirements from the GEN section especially for the FM Interface section:

REQ-GEN	Name	Priority
1	**Plug & Play**	**Major**
2	**Useful**	**Major**
3	**Re-Usable / Generic**	**Essential**
4	**Simple**	**Essential**
5	**Flexible / Extensible**	**Major**
6	**Fine grained (as far as needed)**	**Major**
7	**Standardized / Open**	**Essential**
8	**Mature / Stable**	**Major**
9	**De-coupled**	**Essential**
10	**Evolutionary**	**Major**
11	**Independent**	**Essential**
12	**Certifiable**	**Major**
13	**Compatible**	**Essential**
14	**Interoperable**	**Major**
15	**Scalable**	**Essential**
16	**Secure**	**Minor**
17	**Reliable**	**Essential**
18	**Interface robustness**	**Essential**
19	**Simple trace and logging**	**Essential**
20	**1:1 Relation between Event MO Instances and Inventory MO Instances**	**Major**
21	**"MO Instance" Attribute Information Structure for EMS ←→ NMS Event Interface**	**Major**
22	**M : N Connectivity**	**Major**

5.5.2 Functional Requirements for Fault Management Interface

The functional requirements for the FM interface describe the mandatory and some optional requirements for the Fault Management interface between EMS and NMS from an FM business point of view. The optional requirements are not intended to be complete, but mention some of the most likely needed optional features for **the** interface. It does not define the functional capabilities needed on EMS or the NMS itself, although there are some requirements in this areas mentioned to serve as a "basic" information to understand the needed capabilities on system level (they can be used for EMS/NMS vendor selection processes).

Please consider: Several functional requirements have been shifted into the Generic-Next-Generation-Converged-Operational-Requirements (GEN) section, because they are valid for most types of OSS interfaces.
Examples listed here are:

- Trace and Logging
- "Managed Object Instance" Attribute Information Structure
- M : N Connectivity
- 1:1 Relation between Event Managed Object Instances and Inventory Managed Object Instances

REQ-FM (1) X.733 Event/Alarm Attributes

The event/alarm must contain structured information according to the X.733 specification
Description:

- The attributes of the event/alarm object shall follow the X.733 standard definition (for details see X.733 specification – see References)

Short overview of attributes:

- The yellow marked attributes are mandatory for the interface. So they have to contain a useable value (this can be empty, if this is a useable value). The other attributes are optional in this specification. The interface and the connected systems must work in a proper way, if the optional attributes do not contain any value. Additional explanation: The meaning of "useable" used in this context is that the content should deliver a real information for operations, not just something like an unreadable system message without any meaning for the operator. Furthermore, attributes like Event Time may not be empty. They must contain a date.
- Please consider:
    - That the allowable values for the Managed Object Class should be based on classes defined in the Federated Model (see chapter 4.1.2.1 Federated Model)
    - That the value for the Managed Object Instance should enable to identify an object instance to which an alarm refers to via a configuration management interface.
    - That the standardization should eliminate (or minimize) the need of using vendor specific problem identification. The standardization should leverage the Federated Model (see chapter 4.1.2.1 Federated Model) to provide the library of problems per classes of object which may be defined for different network domains, but should not be vendor specific.

Parameter name	Req/Ind	Rsp/Conf
Invoke identifier	P	P
Mode	P	---
Managed object class	P	P
Managed object instance	P	P
Event type	M	C(--)
Event time	P	---
Event information		---
Probable cause	M	---
Specific problems	U	---
Perceived severity	C	---
Backed-up status	U	---
Backu-up object	C	---
Trend indication	U	---
Threshold information	C	---
Notification identifier	U	---
Correlated notifications	U	---
State change definition	U	---
Monitored attributes	U	---
Proposed repair actions	U	---
Additional text	U	---
Additional information	U	---
Current time	---	P
Event reply	---	---
Errors	---	P

→ The content of the Eventtype and the Probablecause should follow the recommendation in ITU-T M3703 Annex A Table A.1 and Annex B Table B.1 and B.2. to enhance the operational value of these attributes.

→ The Notification ID must be unambiguous to resolve the clear-problem and the synchronization problem (see specific requirements later on)

→ Additional information from Service Quality Management (SQM) oriented data sources (e.g. KPI, DATASOURCE, STIME, etc. …) will be part of the „Additional Text“ attribute.

Table 4: Event/Alarm Attributes

Special remarks:

* The event/alarm has to be encoded in ASCII

* DateAndTime Format: "yyyyMMddhhmmss.s[Z|{+|-}HHMm]"

where:

yyyy	"0000".."9999"	year
MM	"01".."12"	month
dd	"01".."31"	day
hh	"00".."23"	hour
mm	"00".."59"	minute
ss	"00".."59"	second
s	".0".."9"	tenth of second (set to ".0" if EMS or ME cannot support this granularity)
Z	"Z"	indicates UTC (rather than local time)
{+|-}	"+" or "-"	delta from UTC
HH	"00".."23"	time zone difference in hours
Mm	"00".."59"	time zone difference in minutes.

* Event type is very useful for operators to locate the alarms and decide which professional team to do trouble shooting. Thus more event type should be added according to network operation requirement. Refer to ITU-T M.3703, event subtype are defined as following table.

Event Types	Explanation
Communications Alarm	An alarm of this type is associated with the procedure and/or process required conveying information from one point to another (ITU-T Recommendation X.733).
Communications_Signalling and IP Alarm	An alarm of this type is associated with signalling and IP failure, e.g.SS7 protocol error. It is a subtype of Communications Alarm.
Communications_ Interface Alarm	An alarm of this type is associated with interface error, e.g.physical interface of communication error. It is a subtype of Communications Alarm.
Processing Error Alarm	An alarm of this type is associated with a software or processing fault (ITU-T Recommendation X.733).
Environmental Alarm	An alarm of this type is associated with a condition related to an enclosure in which the equipment resides (ITU-T Recommendation X.733).
Quality of Service Alarm	An alarm of this type is associated with degradation in the quality of a service (ITU-T Recommendation X.733).
Quality of Service_Equipment Performance Alarm	An alarm of this type is associated with degradation of equipment performance. e.g. system resources overload. It is a subtype of Quality of Service Alarm.
Quality of Service_ Traffic Performance Alarm	An alarm of this type is associated with degradation of traffic performance. e.g. excessive retransmission rate. It is a subtype of Quality of Service Alarm.
Equipment Alarm	An alarm of this type is associated with an equipment fault (ITU-T Recommendation X.733).
Equipment_Traffic Equipment Alarm	An alarm of this type is associated with traffic related equipment fault, e.g. antenna, receiver, transmitter, and switch fault etc. It is a subtype of Equipment Alarm.
Equipment_ Charging System Alarm	An alarm of this type is associated with charging system fault, e.g.billing file error etc. It is a subtype of Equipment Alarm.
Equipment_External I/O Equipment Alarm	An alarm of this type is associated with an external I/O equipment failure, e.g. disk problem. It is a subtype of Equipment Alarm.
Equipment_Relay and Transmission Alarm	An alarm of this type is associated with relay and transmission failure, e.g. printer un-reachable. It is a subtype of Equipment Alarm.
Equipment_Equipment Power Alarm	An alarm of this type is associated with equipment power problem, e.g. power supply failure. It is a subtype of Equipment Alarm.
Integrity Violation	An indication that information may have been illegally modified, inserted or deleted.
Integrity Violation_ Data Configuration	An alarm of this type is associated with data configuration failure. e.g. switch data configuration error. It is a subtype of Integrity Violation.
Integrity Violation_ Database System	An alarm of this type is associated with database system failure. e.g. database out of service. It is a subtype of Integrity Violation.
Operational Violation	An indication that the provision of the requested service was not possible due to the unavailability, malfunction or incorrect invocation of the service.
Physical Violation	An indication that a physical resource has been violated in a way that suggests a security attack.
Security Service or Mechanism Violation	An indication that a security attack has been detected by a security service or mechanism.
Time Domain Violation	An indication that an event has occurred at an unexpected or prohibited time.
Unknown	Event type that cannot be supported by the above definitions.

Table 5: Event Types

Rationale:

- X.733 is widely used as a standard for the specification of a generic event/alarm. The attributes, as well as the state model and the behaviour of the model are quite stable since more than 15 years now. So that this seems to be a commonly accepted definition for the FM interface, which can be adopted to create an “implementation-ready” standardized interface..

The abbreviations and conventions used here are part of the CCITT Rec. X.733 specification. See document: T-REC-X[1].733-199202-I!!PDF-E.pdf , quoted here:

Chapter 4 Abbreviations

Conf	Confirm
Ind	Indication
Req	Request
Rsp	Response

…

Chapter 5 Conventions

This Recommendation | International Standard defines services following the descriptive conventions defined in CCITT Rec. X.210 | ISO/TR 8509. In clause 9, the definition of each service includes a table that lists the parameters of its primitives. For a given primitive, the presence of each parameter is described by one of the following values

M	the parameter is mandatory
(=)	the value of the parameter is equal to the value of the parameter in the column to the left
U	the use of the parameter is a service-user option.
–	the parameter is not present in the interaction described by the primitive concerned.
C	the parameter is conditional. The condition(s) are defined by the text which describes the parameter.
P	subject to the constraints imposed on the parameter by CCITT Rec. X.710 | ISO/IEC 9595.

…

Priority: Essential

REQ-FM (2) Event/Alarm Transport

It must be possible to send (Server) [and receive/listen to (Client) event/alarms]
(see also REQ-FM (9))

Description:

- EMSs (FM servers) can distribute (send) event/alarms according to X.733 event/alarm structure specification to NMS (OSS)
- [NMSs (FM clients) can receive/listen to event/alarms according to X.733 event/alarm structure specification. ("NMS send" is not required. Please consider that these requirements focus on the EMS→ NMS interface only!)]

Rationale:

- This is a basic and generic requirement for an FM interface.

(Remark: the NMS can also query for alarms, beside "Send" and "Receive". This requirement is covered under REQ-FM (5))

Priority: Essential

REQ-FM (3) Clear – Event/Alarm Transport

It must be possible to send [and receive/listen to] "clear" - event/alarm events

Description:

- The interface specification has to support "clear" events, according to the X.733 specification. Element Management Systems (servers) should be able to deliver "clear-event/alarm" events, which can be

unambiguously mapped on related event/alarm events. (See “clear correlation” requirement later on [part of requirement “Unambiguous Notification ID”]). The Network Management System (client) must be able to handle the clear-event/alarms. The interface specification has to support this capability. The EMS must support “clear” - event/alarm handling. (But the NMS must be able to handle situations, if there are missing clear-events/alarms.)

Rationale:

- Support for “clear” – event/alarms improve the ability of network operators to understand the actual status of NEs -> do they deliver the NE service, or are there still open faults in the NE which might impact the NE service and eventually other subsequent end user services. “Clear” - event/alarms reduce the costs for operational processes, because they reduce the effort to identify the status of NEs. Without “clear” - event/alarms, the operator has to perform additional tests to verify the actual NE status.

Priority: Essential

REQ-FM (4) Unambiguous ID

It must be possible to correlate between clear–event/alarm and the original event/alarm, by using an unambiguous ID.

Description:

- A unique and unambiguous ID is a prerequisite to enable the NMS to correlate between “clear” – event/alarms and original event/alarms. It is not allowed to use a combination of different attributes to create unambiguousness.
- The EMS will send a “clear” – event/alarm, as soon as the incident, which caused the original event/alarm, does not exist any more. The NMS needs to be able to correlate between the “clear” - event/alarm and the original event/alarm. So the Element Management System must be able to deliver “clear” - event/alarm events, which can be unambiguously mapped on related event/alarm events. The interface specification has to support this capability. Although this is a general requirement for Element Management Systems and out of scope for this requirement specification for the interface itself, there must be an interface specification which describes the usage of the event/alarm attributes, so that the relation between event/alarm and “clear” - event/alarm can be uniquely identified.
- Remark: the requirement is different to the correlation mechanism described in the document “ITU-T X.733 Correction”.

Rationale:

- The actual X.733 mechanisms used to correlate between “clear” - event/alarms and the original event/alarms are inefficient and complex. They lead to complex and expensive implementations of FM interfaces, especially to be able to deliver NMS support for **Event/Alarm Correlation (Clearing) and Re-Synchronization**.

Priority: Essential

REQ-FM (5) Event/Alarm Query

It must be possible for the client (NMS) to query all active event/alarms.

Description:

- The interface has to support the "Synchronization" functionality of the Network Management System. That means, the Network Management System can use a "query" functionality of the interface to get all event/alarms, which are known by the Element Management System (during the time of the "query" command) and which do not have the perceived severity = "cleared".

Remark: this capability requires the "unambiguous Notification ID" (see related requirement "REQ-FM(4) Unambiguous Notification ID"

Rationale:

- This functionality allows the implementation of a synchronization mechanism in the Network Management – System. In case of an undefined state of the event/alarm data in the NMS (e.g. caused by a restore of the NMS database), the Network Management System can send a query to the EMS to synchronize between EMS event/alarm data and NMS event/alarm data.

Priority: Essential

REQ-FM (6) Heartbeat

The interface has to support a heartbeat capability which allows EMS to send heartbeats (configurable) and NMS to receive/listen to heartbeats.

Description:

- The interface has to support EMS heartbeat signals to the NMS. This functionality allows to indicate that the EMS and also the connection between EMS and NMS is up and running.

Rationale:

- The heartbeat functionality ensures that the NMS is able to inform the operator about a connection loss between EMS and NMS (alarming of connection-loss and clearing if connection is back).

Priority: Essential

REQ-FM (7) Supplementary Information contained within alarm

The interface has to provide all information required for correlation

Description:

- All information required for the correct analysis of the fault context must be provided. All supplementary information from the EMS or NE explaining the alarm context shall be embedded / encoded into one alarm parameter in a regular expression. This should include ID's, topological information. The field must be structure in a regular manner, so that automatical processing by a post processing function is possible.

Rationale:

- It shall not be required to consult the Element Manager or other tools to analyse the fault context.

Priority: Essential

REQ-FM (8) Co-operative alarm acknowledgement (OPTIONAL)

The interface shall support a co-operative alarm-acknowledgement function as described in 3GPP TS 32.111-1 (Optional feature)

Description:

- Acknowledgement performed at EM layer is notified at NM layer and vice versa, thus the acknowledgement-related status of this alarm is the same across the whole management hierarchy. The alarm acknowledgement function requires that:
  a) All involved OSSs have the same information about the alarms to be managed (including the current responsibility for alarm handling).
  b) All involved OSSs have the capability to send and to receive acknowledgement messages associated to previous alarm reports.

Rationale:

- The alarm acknowledgement function assures that activities concerning the resolving of the specific problem are indicated.

Priority: Minor

5.5.3 EMS Specific Functional Requirements for Interface Support

REQ-FM (9) Reliable Event/Alarm Communication (supported by EMS)

- EMS buffers event/alarms if they cannot be sent to the NMS
- EMS sends event/alarms immediately as soon as the connectivity to the NMS is up again

Description:

- The main intention of this requirement is to ensure that no event/alarm is lost when NMS goes down (caused by NMS problems or by maintenance work). (For example: X.733 (relates to X.710 for events) requests a logging mechanism for events on the originator site. This enables the NMS to synchronize with its data sources as soon as the NMS is back again) → this is a requirement for the EMS.
  Another problem might occur, when the transport mechanism between EMS and NMS is not available. To ensure that the operator is aware about the malfunction of the interface, which will stop the ability to retrieve and to monitor event/alarms. This situation cannot be handled by the interface itself, but it can be handled either on EMS site (For example: X.733 specifies a confirmation event which has to be delivered by the NMS, as soon as the NMS receives the event/alarm) and/or by the NMS (e.g. via regular queries to the EMS [heartbeat]). → These requirements have to be supported by EMS and NMS. The interface itself has to support the confirmation of “sent – events” and it has to support “queries”.

Rationale:

- Ensure that no event/alarm gets lost if the NMS or the interface to the NMS goes down.

Priority: Essential

REQ-FM (10) Configurable EMS Heartbeat Message

EMS will send heartbeats in regular (configurable) intervals to NMS.

Description:

- The EMS will send heartbeat signals to the NMS in regular intervals (configurable intervals) to indicate that the EMS and the connection between EMS and NMS are up and running.

Rationale:

- The heartbeat functionality ensures that the NMS is able to inform the operator about a connection loss between EMS and NMS (event/alarming of connection loss and clearing if connection is back).

Priority: Essential

REQ-FM (11) Alarm Suppression

The EMS - NMS - Fault Management interface should enable the alarm suppression.

Description:

- The EMS interface offers the possibility to suppress the alarm of physical and logical objects when the NMS should not receive any alarms from EMS. After alarm suppression all alarms will be cleared on the NMS and a warning will be generated on the NMS which indicates the alarm suppression. After re-enabling of the alarms all active alarms will be sent from EMS to NMS. This capability has to be configurable (manual / automatically).

Rationale:

- This functionality is very important for maintenance of equipment, hardware / software upgrade, testing etc.

Priority: Major

REQ-FM (12) Summary Alarms

EMS interface summary should provide summary alarm functionality.

Description:

- For minor alarm is sometimes not practicable to send every alarm from EMS to NMS. EMS generates a summary alarm and sends it to NMS when an alarm occurs several times within a certain window-time. This capability should be configurable. E.g. if a alarm occurs and clear more than 50 times per minute, then EMS will send a summary alarm to NMS. If this alarm occurs and clear less than 50 times per minute, then EMS will sent clear alarm to NMS.

Rationale:

- This feature protects the NMS from alarms flood.

Priority: Major

5.5.4 NMS Specific Functional Requirements for Interface Support

REQ-FM (13) Re-Synchronization

The NMS must be able to synchronize the own event/alarm list with the EMS event/alarm lists

Description:

- The NMs will use the query functionality of the FM interface to synchronize the own event/alarm list with all EMs event/alarms with a perceived severity ≠ "cleared". This functionality will be invoked automatically by re-connection of the NMs with the EMs after startup of the NMs or the interface

Rationale:

- This capability has to ensure, that the event/alarm lists of the EMs and the NMs are always synchronized.

Priority: Essential

5.6 Use Cases

Introduction

This document contains "Use Cases" to explain the meaning of the requirements REQUIREMENTS FOR FAULT MANAGEMENT INTERFACE (FM) and GENERIC NEXT GENERATION CONVERGED OPERATIONAL REQUIREMENTS (GEN). Please consider, that not all requirements are related to a specific Use Case in this document, because some of them are business requirements without a concrete technical implementation (e.g. generic requirements, like "Standardized", "Mature", "Useful", etc.)

Event/Alarm Transport

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**It must be possible to send (EMS) and to receive/listen to Event/Alarms (NMS) via the FM Interface** [See REQ-FM (2), REQ-FM (1)and REQ-GEN (21).	
Actor and Roles	1. Element Management – systems (FM Servers) can distribute (send) Event/Alarms according to the alarm structure specified in REQ-FM (1). 2. Network Management– systems (FM Clients) can receive/listen to Event/Alarms according to the alarm structure as specified in REQ-FM (1).	
Assumptions	EMS and NMS implemented and connected	
Pre conditions	EMS and NMS started and connected	
Begins when	EMS created an alarm	
Step n	EMS issues an alarm	
Step (n+1)	-	
Ends when	NMS receives the alarm	
Exceptions	-	

Post Conditions	- The Alarm information between EMS and NMS is consistent for this alarm. - The Alarm structure fulfils the requirements from REQ-FM (1). - The "Managed Object Instance" – Attribute for the EMS ← Alarm → NMS Interface fulfils the requirements from REQ-GEN (21). - Mapping of Event Attributes between Event and NMS are aligned - Inventory Source is CMDB	
Traceability	-	

Event/Alarm Update Transport

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**It must be possible to send (EMS) and to receive/listen to an Update of the Event/Alarms (NMS) via the FM Interface** [See Requirement REQ-FM (2) and REQ-FM (1).	
Actor and Roles	1. Element Management – systems (FM Servers) can distribute (send) an Event/Alarms – Update 2. Network Management – systems (FM Clients) can receive/listen to an Event/Alarms Update	See Use Case: "2.1 Event/Alarm Transport"
Assumptions	EMS and NMS implemented and connected	
Pre conditions	EMS and NMS started and connected. An EMS Alarm has been send to the NMS already.	
Begins when	EMS updated an alarm attribute	
Step n	EMS issues the updated alarm	
Step (n+1)	-	
Ends when	NMS receives the updated Alarm	
Exceptions	-	
Post Conditions	The Alarm information between EMS and NMS is consistent for this alarm, Existing Alarm will be overwritten , no additional Alarm in Alarm list	
Traceability	-	

Clear – Event/Alarm Transport

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	It must be possible to send [and receive/listen to] "Clear" Event/Alarm events [See Requirement REQ-FM (3) and REQ-FM (4)]	

Actor and Roles	Element Management systems (Servers) should be able to deliver "Clear-Event/Alarm" events, which can be unambiguously mapped on related Event/Alarm events (See "Clear Correlation" requirement later on). The Network Management system (client) must be able to handle the Clear Event/Alarms. The interface specification has to support this capability. The EMS must support Clear - Event/Alarm handling.(But the NMS must be able to handle situations, if there are missing Clear-Events/Alarms)	
Assumptions	EMS and NMS implemented and connected	
Pre conditions	EMS and NMS started and connected. An EMS Alarm has been send to the NMS already.	
Begins when	The Alarm is being cleared.	
Step n	EMS issues an Alarm-Clear notification	
Step (n+1)	-	
Ends when	NMS receives the Alarm-Clear - notification	
Exceptions	-	
Post Conditions	- The Alarm information between EMS and NMS is consistent for this alarm - The Notification ID´s of the original Alarm and the related Clear Alarm update are unambiguously correlated to each other by a combination of the numerical Notification ID and the "Managed Object" [See REQ-FM (4)and REQ-FM (3)]	
Traceability	-	

Event/Alarm Query

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**NMS queries all active Event/Alarms at EMS.** [See REQ-FM (5)]	
Actor and Roles	The interface has to support the "Synchronization" functionality of the Network Management system. That means, the Network Management system can use a "query" functionality of the interface to get all Event/Alarms, which are known by the Element Management system (during the time of the "query" – command) and which do not have the perceived-severity: "cleared" (Comment: This functionality allows the implementation of a synchronization mechanism in the Network Management – system. In case of an undefined state of the Event/Alarm – data in the Network Management system (e.g. caused by a restore of the NMS database), the Network Management system can send a query to the EMS to synchronize between EMS Event/Alarm – data and NMS Event/Alarm – data.)	
Assumptions	EMS and NMS are implemented and connected	
Pre conditions	- EMS and NMS are started and connected. - There are active (not cleared) alarms in the Alarm-List of the EMS and the NMS. Both lists are synchronized - EMS and NMS are disconnected - The Alarm-List of the NMS is deleted??	

	Alarms which are not in NMS will be created, don't change Alarm status of existing Alarms like Ack ,Operator Note ...	
Begins when	EMS and NMS are connected again	
Step n	The NMS queries for all active Alarms (automatically or manually)	
Step (n+1)	The EMS sends all active Alarms	
Ends when	NMS receives all Alarm events	
Exceptions	-	
Post Conditions	The list of Alarms between EMS and NMS is consistent	
Traceability	-	

Heartbeat

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**EMS sends heartbeat events (configurable) to NMS.** [See REQ-FM (6)]	
Actor and Roles	EMS sends heartbeat signals in regular (configurable) time intervals to the NMS. This functionality allows to indicate, that the EMS and the connection between EMS and NMS and is up and running.	
Assumptions	EMS and NMS are implemented and connected	
Pre conditions	EMS and NMS are started and connected. Heartbeat – Interval is configured in EMS and NMS	
Begins when	Time for first Heartbeat-Interval in EMS is arrived	
Step n	EMS issues Heartbeat-Event to NMS in regular Intervals	
Step (n+1)	NMS receives the Heartbeat-Event in regular Intervals	
Step (n+2)	Cut of Network Connectivity between EMS and NMS, or EMS shutdown	
Step (n+3)	NMS detects, that it does not received the Heartbeat – Event in the expected Heartbeat-Interval. NMS will show a "lost-connection" notification (e.g. Alarm), that the connectivity to the EMS does not work any more.	
Step (n+4)	Connect EMS with NMS again	
Step (n+5)	EMS sends all outstanding (buffered) Alarms to the NMS	See also Use Case "Reliable Alarm/Event Communication"
Step (n+6)	EMS sends Heartbeat Event again	
Step (n+7)	NMS clears the "lost-connection" notification.	
Ends when	NMS receives all outstanding Alarms	See also Use Case "Reliable Alarm/Event Communication"
Exceptions	-	
Post Conditions	The list of Alarms between EMS and NMS is consistent	
Traceability	-	

Reliable Event/Alarm Communication (supported by EMS)

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**No lost Alarm/Event, after connection breakdown between EMS and NMS.** [See REQ-FM (9)]	
Actor and Roles	- EMS buffers Event/Alarms if they cannot be send to the NMS - EMS sends Event/Alarms immediately as soon as the connectivity to the NMS is up again It has to be ensured that no Event/Alarm is lost, when NMS goes down (caused by NMS problems or by maintenance work). X.733 (relates to X.710 for Events) requests a logging mechanism for Events on the originator site. This enables the NMS to synchronize with its data sources as soon as the NMS is back again. → this is a requirement for the EMS Another problem might occur, when the transport mechanism between EMS and NMS is not available. To ensure, that the operator is aware about the malfunction of the interface, which will stop the ability to retrieve and to monitor Event/Alarms. This situation cannot be handled by the interface itself, but it can be handled either on EMS site (X.733 specifies a confirmation event which has to be delivered by the NMS, as soon as the NMS receives the Event/Alarm.) and/or by the Network Management system (e.g. via regular queries to the EMS [heartbeat]). → These requirements have to be supported by EMS and NMS. The Interface itself has to support the confirmation of "send – events" and it has to support "queries".	
Assumptions	EMS and NMS are implemented and connected	
Pre conditions	EMS and NMS are started and connected.	
Begins when	Disconnection of the physical connectivity between EMS and NMS	
Step n	EMS creates several new Alarms	
Step (n+1)	Connect EMS with NMS again	
Step (n+2)	EMS sends all outstanding (buffered) Alarms to the NMS	
Ends when	NMS receives all outstanding Alarms	
Exceptions		
Post Conditions	The list of Alarms between EMS and NMS is consistent Connection Lost is alarmed in Alarm list	
Traceability	-	

De-Coupled, Flexible/Extendible and Compatible

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Implementation of a new Version of an Interface on EMS OR NMS** [See REQ-GEN (5), REQ-GEN (9) and REQ-GEN (13)]	
Actor and Roles	One of the communication partners implements a new version of the interface, e.g. with additional attributes, while the other communication partners still use an old version of the interface specification. This "mixed versions" of interface implementations can be used without any impact on the communication partners or the interface implementations of the communication partners, so that changes in the application or in the interface implementation at one of the communication partners do not lead to the need for changes in the application or in the interface implementation of the other communication partners. It must be possible to extend the interface capabilities (methods and attributes), without breaking the standard	
Assumptions	EMS and NMS are implemented and connected	
Pre conditions	- EMS and NMS are started and connected. The interface works as expected and the EMS sends Alarms to NMS successfully.	See UseCase "Event/Alarm Transport"
Begins when	A new EMS Interface-Version is ready to implement. The new Interface Version uses one additional optional attribute (for example)	
Step n	Disconnect EMS from NMS.	
Step (n+1)	Activate new EMS Interface Version	
Step (n+2)	Connect EMS to NMS	
Step (n+3)	NMS performs a synchronization (started by a "query for active alarms") with the EMS	
Step (n+4)	The NMS receives Alarms from the EMS (just don't use/show the additional attribute).	
Ends when	NMS received all outstanding Alarms without any impact on NMS	
Exceptions	-	
Post Conditions	The list of Alarms between EMS and NMS is consistent	
Traceability		

Certifiable

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Certify the standard compliancy of the interface implementation** Remark: There is no description of the concrete steps for the certification in this Use Case description, because there is no description of the certification mechanism available today. [See REQ-GEN (12)]	
Actor and Roles	The interface implementation on EMS and NMS will be certified (e.g. via tool). This will allow the verification, that the interface implementation is compliant with the standardized interface specification to avoid compatibility problems between interface implementations of different communication partners.	
Assumptions	The FM Interface is implemented on EMS and NMS.	
Pre conditions	-?	
Begins when	-?	
Step n	-?	
Step (n+1)	-?	
Ends when	-?	
Exceptions	- ?	
Post Conditions	The Certification of the FM Interface on EMS and NMS has been passed successfully	
Traceability	-	

Interface Robustness

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Outage of the connection to one of the EMS does not harm the interfaces from other EMS to the NMS.** [See REQ-GEN (18)]	
Actor and Roles	An outage of one or more EMSs (source) may not lead to any impact on the connectivity between NMS and other EMSs	
Assumptions	Several EMS are connected to one NMS	
Pre conditions	All connections between the EMS and the EMS´s are up and running	
Begins when	Disconnect EMS 1	
Step n	The NMS receives Alarms from the other (still connected) EMS´s without any impact caused by the connection breakdown to EMS 1	
Step (n+1)	Connect EMS 1 again	See also 2.10 : “Reliable Event/Alarm Communication (supported by EMS) “
Ends when	NMS receives Alarms from all EMS´s	
Exceptions	-	
Post Conditions	The list of Alarms between all EMS´s and NMS is consistent	
Traceability	-	

Simple Trace and Logging

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Error analysis of the FM Interface by check of the Log on EMS and NMS in case of interface problems** [See REQ-GEN (19)]	
Actor and Roles	The Operator/Administrator of the NMS and the EMS check the logs on "their" systems in case of problems with interface. Examples: - Connection breakdown between EMS and NMS - EMS does not react on "Query"- Command - The EMS does not deliver a mandatory attribute The level of logging details will be configured on EMS and NMS: - Masking of attributes - Masking of attribute- content	
Assumptions	EMS and NMS are implemented and connected. The logging mechanism is working on EMS and NMS.	
Pre conditions	The logs do exist in a human readable format. EMS and NMS are up and running.	
Begins when 1.0	Breakdown of the connection between EMS and NMS	
Step 1.1	Check Log on EMS and NMS manually. (Verify, that the Log contains all the information needed to understand the problem and to restore the connectivity)	
Step 1.2	Restore the connectivity	
Ends when 1.3	The connectivity is up and running. The log on EMS and NMS shows, that the problem has been resolved.	
Begins when 2.0	Stop EMS database.	
Step 2.1	Start NMS query: "Query all active alarms" manually.	See Use Case "Event/Alarm Query"
Step 2.2	Check Log on EMS and NMS manually. (Verify, that the Log contains all the information needed to understand and to solve the problem)	
Step 2.3	Restart EMS database	
Step 2.4	Start NMS query: "Query all active alarms" manually.	See Use Case "Event/Alarm Query"
Ends when 2.5	The NMS Query is successfully. The NMS receives all active alarms from the EMS. The log on EMS and NMS shows, that the problem has been resolved.	
Begins when 3.0	EMS creates a new alarm. The content of the Managed Object attribute is deleted manually.	
Step 3.1	The EMS sends the alarm to the NMS. (The NMS will not be able to handle the alarm correctly in this case)	
Step 3.2	Check Log on EMS and NMS manually. (Verify, that the Log contains all the information needed to understand and to solve the problem)	
Step 3.3	The EMS sends further alarms to NMS (this time correctly, with the MO – attribute, as expected)	
Step 3.4	The NMS receives the alarms and can handle it correctly.	
Ends when 3.5	The log on EMS and NMS shows, that the problem has been resolved.	

Begins when 4.0	The Operator/Administrator on EMS and NMS mask attributes in the log.	
Step 4.1	The EMS sends alarms to the NMS.	
Step 4.2	Check Log on EMS and NMS manually. (Verify, that the Log contains all the needed information without the masked attributes)	
Step 4.3	The Operator/Administrator on EMS and NMS de-mask attributes in the log.	
Ends when 4.4	Check Log on EMS and NMS manually. (Verify, that the Log contains all the needed information including the de-masked attributes)	
Begins when 5.0	The Operator/Administrator on EMS and NMS mask attributes-content in the log (e.g. masking of Severity = "Warning")	
Step 4.1	The EMS sends alarms to the NMS. Some of them (not all) must contain Alarm with Severity="Warning"	
Step 4.2	Check Log on EMS and NMS manually. (Verify, that the Log contains all transactions, without "send/receive Alarm" with Severity="Warning")	
Step 4.3	The Operator/Administrator on EMS and NMS de-mask all attributes-content in the log	
Ends when 4.4	Check Log on EMS and NMS manually. (Verify, that the Log contains all transactions, including Alarms with Severity="Warning")	
Exceptions	-	
Post Conditions	The log on EMS and NMS shows, that the problems have been resolved.	
Traceability	-	

M : N Connectivity

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Connect several [min. 3] EMS to several [min. 2] NMS.** [See REQ-GEN (22)]	
Actor and Roles	Implementation of an N:M scenario	
Assumptions	Several EMS are connected to several NMS	
Pre conditions	All connections between the EMS and the NMS´s are up and running	
Begins when	All EMS´s send alarms to all NMS´s	See Use Case: "2.1 Event/Alarm Transport"
Step n	-	
Ends when	All NMS´s receive all Alarms from all EMS´s	
Exceptions	-	
Post Conditions	The list of Alarms between all EMS´s and all NMS´s are consistent	
Traceability	-	

6 Requirements for Inventory Management (InvM)

6.1 Introduction

The NGCOR Inventory Management work was initiated within NGMN member community (operators) during March - June 2011 with phase 1. The results were defined as high level Inventory Management requirements and were sent to NGMN partners to be reviewed, discussed and elaborated with clarifications and enhancements.

In phase 2 of the Inventory Management sub-task during autumn 2011 the selected prioritized areas of high level requirements were worked out as more detailed use cases and requirements, presented in chapter 6.6. Also during phase 2 it was complemented and clarified:

- Objectives and general business rationale for enhanced Inventory Management, presented in chapter 6.3
- A common OSS architecture reference model focusing on Inventory Management, presented in chapter 6.4.4 with summarizing Figure 46.

As an outlining summary of the problem space and concepts, NGCOR positions Inventory Management at the core of information management for resources, services and products within OSS/BSS environment of operators. NGCOR shares an aligned view of TM Forum TIP Inventory harmonization study, i.e.

- The general acceptance that the term “Inventory” designates a repository of information (Data Base), and more precisely a repository of instance entities. Depending on the focus, this repository may contain instances of Products, Services, Resources and Configurations.
- The term “Catalogue” would be more used to designate a repository of specifications (Service Specs, Resource Specs). The term “Specification” is used to define the invariant characteristics and behaviour (attributes, methods, constraints, and relationships) of a (Managed) Resource/ Service
- In the document we will consider Inventory Repository in the broad sense, meaning that it may contain instances and/or specifications. The instances that may be present in an Inventory repository are instances of object classes all specified in an information model.
- Complementary to the repository (data store) view point, an Inventory system can expose services either by sending notifications to external systems or by allowing external systems to invoke operations that it exposes. The operations may be used by external systems:
    - to modify the content of the repository (we talk about updating or synchronizing processes) or
    - to query the repository in order to collect specific information that it contains.
- The notifications generated by an Inventory system are used to inform other systems of any change in the repository.

With respect to Inventory Management specified by 3GPP, NGCOR has a broader scope by addressing functionalities of Inventory Management within OSS architecture of operators and interfacing inventory with other OSS applications. I.e. in 3GPP terms; NGCOR is dealing with functionalities of NMSs and also NMS - NMS interfacing. The common problem space of 3GPPP and NGCOR is interfacing towards the network, i.e. aiming to a standard northbound interface.

It is to be noted that when describing OSS architecture models, e.g. Figure 46: OSS reference architecture emphasizing Inventory Management, the presented architecture structures does not imply any implementation models. Which means that implementation models derived from the reference model can include variants for example; the descried functionalities can be implemented separately or jointly, the needed databases can be centralized of distributed.

6.2 Scope of Work of Inventory Management Sub Task and Limitations

The focus of NGCOR Inventory Management sub-task in the phase 1 was to get a common view on Inventory Management area in broad sense; the main Inventory Management concepts, the main roles and characteristics of inventories within OSS/BSS environment of operators. This was defined as high level Inventory Management requirements.

In phase 2 of the sub-task during autumn 2011 the work continued with

- Describing objectives and business rationale for enhanced Inventory Management
- Elaboration and refinement of the reference model
- Selected prioritized areas of high level requirements were worked out as use cases and more detailed requirements, the selected sub-areas addressed are focusing on resource Inventory Management
    - Resource Inventory Management support for Fault Management
    - Resource Inventory Management support for Resource Configuration
    - Resource Inventory Management support for planning and deployment

The sub-areas which were not addressed in detail analysis were be left as high level requirements as defined in phase 1, presented I chapter 6.5 and are potential objects for further work in later projects.

Editor's note:
As an overall summary and guidance to readers for right positioning of NGCOR Inventory Management requirements it is recognized and understood that needs for different levels of details and completeness of requirements vary among usage of this document. NGCOR wants to highlight that first it has been crucial to start from top-down view to build a common understanding for Inventory Management problem space and addressing in a holistic way inventory issues from traditional network resource layer up to customer service and product layer. Operators' needs for requirements are different as well; depending on the evolution status spanning e.g. from architecture specifications to existing solution migration paths and deployments. NGMN has been preparing a continued work for developing an extended set of Inventory Management use cases and respective detailed requirements focusing especially Service Inventory Management, in conjunction of the continued project may also selected parts of Resource Inventory requirements be complemented.

6.3 Objectives and Business Rationale for Enhanced Inventory Management

Information today pervades every aspect of an organization, including reporting, marketing, product development, and resource allocation. In the last years, business reports to management and investors as well as planning decisions of a service provider have become much more dependent on information derived from various sources than ever before.

The Inventory sub-task of NGCOR places the Inventory Management in the focal point of view as it is understood that inventories are the key and core parts of OSS architecture of operators. The main role of inventories is to provide comprehensive and reliable data supporting efficiently different operational, planning and deployment processes when managing the infrastructure and the services. Inventories are the key OSS applications/systems and central points of managed and structured way of information handling throughout different management layers. A direction to harmonized inventory interfaces and information models is a must when having a growing complexity of OSS support needs. Operators still do have a lot of old legacy inventory systems; the information of which is not flexible to use, where the information is split to many pieces and many data stores. When implementing next generation networks and services increasing amount of new network and service data has to be managed in conjunction with the older. At the same time customer focused information management accelerates integration

needs between BSS level and OSS level and requires inventory support, a federated view from different inventory systems is foreseen need. Generally inventory development projects are perceived as expensive and the answer to the question how to make migration paths cost effectively and secure way to new generation commercial-of-the shelf (COTS) inventories is of high importance for operators.

Within the information-driven business of a service provider the approach to the design and implementation of a future multi-vendor, multi technology resource and Service Inventory solution has to include the implementation of an **information governance process** - this is one of the key success factors.

A process driven approach to the design and implementation of a future multi-vendor, multi technology resource and Service Inventory solution is another key success factor. This implies to start with process analysis and use case definitions as well as with the analysis of information needs & consumption for the process groups.

- Operations (fulfilment and assurance processes and operations support and readiness from the eTOM
- Lifecycle management processes incl. planning and deployment

Having done this first step we are able to derive requirements towards the information model, the connectivity needs and architectural requirements from process and use case definitions.

Dominated by the process view, an Inventory Management system becomes a dynamically changing system presenting current, past and future states of the network and services. Inventory becomes a real heart of the OSS, loosely coupled with OSS applications in the eTOM-domains of product/service/resource life cycle management, fulfilment and assurance.

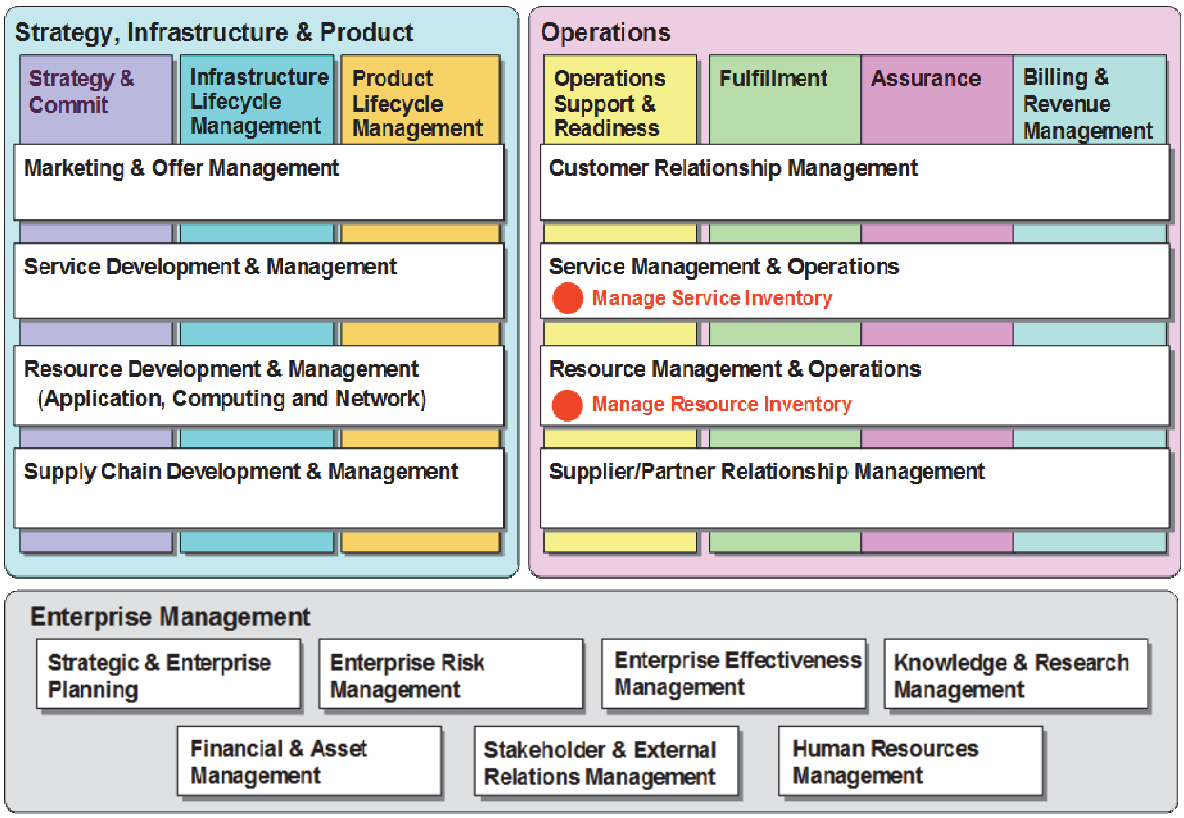

Figure 42: Key scope of InvM sub task in the eTOM framework

In the layered structure of eTOM it is regarded especially

- In the service management layer service Inventory Management provides benefits by
  - Managing all service related data
  - Providing abstraction layer on top resource management layer and via that enabling modular and componentized usage of resources as support of different services offered by the operator
  - Enabling flexible and componentized customer product offerings composed of different service entities and via that reducing time to market in new product launches or product offering changes

- In the resource management layer resource Inventory Management provides benefits by
  - Managing all resource related data
  - Provides accurate view of actual status of resources
  - Enabling flexible and componentized usage of resources as support for different services

Inventory Management will be essential to support Next Generation technologies enabling automation, and International optimization. Many of the desired improvements in efficiency from NGMN automation will not be achievable due to current inconsistent end-to-end management of inventory data.

To run the operations business of a service provider efficiently, his organization relies on accurate information provided in the form needed to do the work. The common data managed by inventories and respective processes have to ensure that the data providing that information is:

- managed according business requirements
- unique - there should be only one master copy
- correct and up to date
- of high integrity - you should be able to believe what you see, without any question
- delivered in the form needed

These goals will not be reachable without harmonizing current practices and processes for Inventory Management across the different parts of the technology organization to reflect the full information life cycle. The lack of a harmonized Inventory Management would mean:

- we don't know what data to hold
- we don't have all the required data
- data is inconsistently held in multiple systems
- data is missing or inaccurate
- data is not really "owned"
- data is not shared

6.4 Methodology and Main Concepts of Inventory Management

This chapter analyses a common reference model and the main concepts on the Inventory Management area. The analysis is presented in order to create a solid basis for Inventory Management requirements further work overall in the context of the NGMN NGCOR project. Also 'the full picture' of inventories is addressed spanning from BSS-level product Inventory Management to OSS with service and resource/network layer Inventory Management. Further on a common OSS architecture reference model focusing on Inventory Management is presented in chapter 6.4.4 summarizing the analysis.

The NGCOR project is supposed to build on previous work done in SDOs and other industry organizations. NGCOR Inventory Management uses TMF originated concepts (eTOM, SID and TAM) for structuring the manage-

ment and the role of different kind of inventories. The scope for setting requirements is to address widely both service management layer and resource management layer needs and seeing relations from Inventory Management perspective in a comprehensive OSS architecture context.

6.4.1 Resource Inventory Management

6.4.1.1 Main Functionality

This chapter addresses **Resource Inventory Management** as a holistic concept without any major attempt to consider possible approaches for implementations for needed applications and various data repositories. In broad sense the operators' concern is of extensive and high quality ***Resource Information Management*** which covers all resources and their features used to implement services and products. Fundamental principle is manage resource information in a uniform and organized way as a key part of OSS architecture. The resource information to be managed covers all physical and logical resources needed for service production including spare parts and, if applicable, extending customer premises equipment.

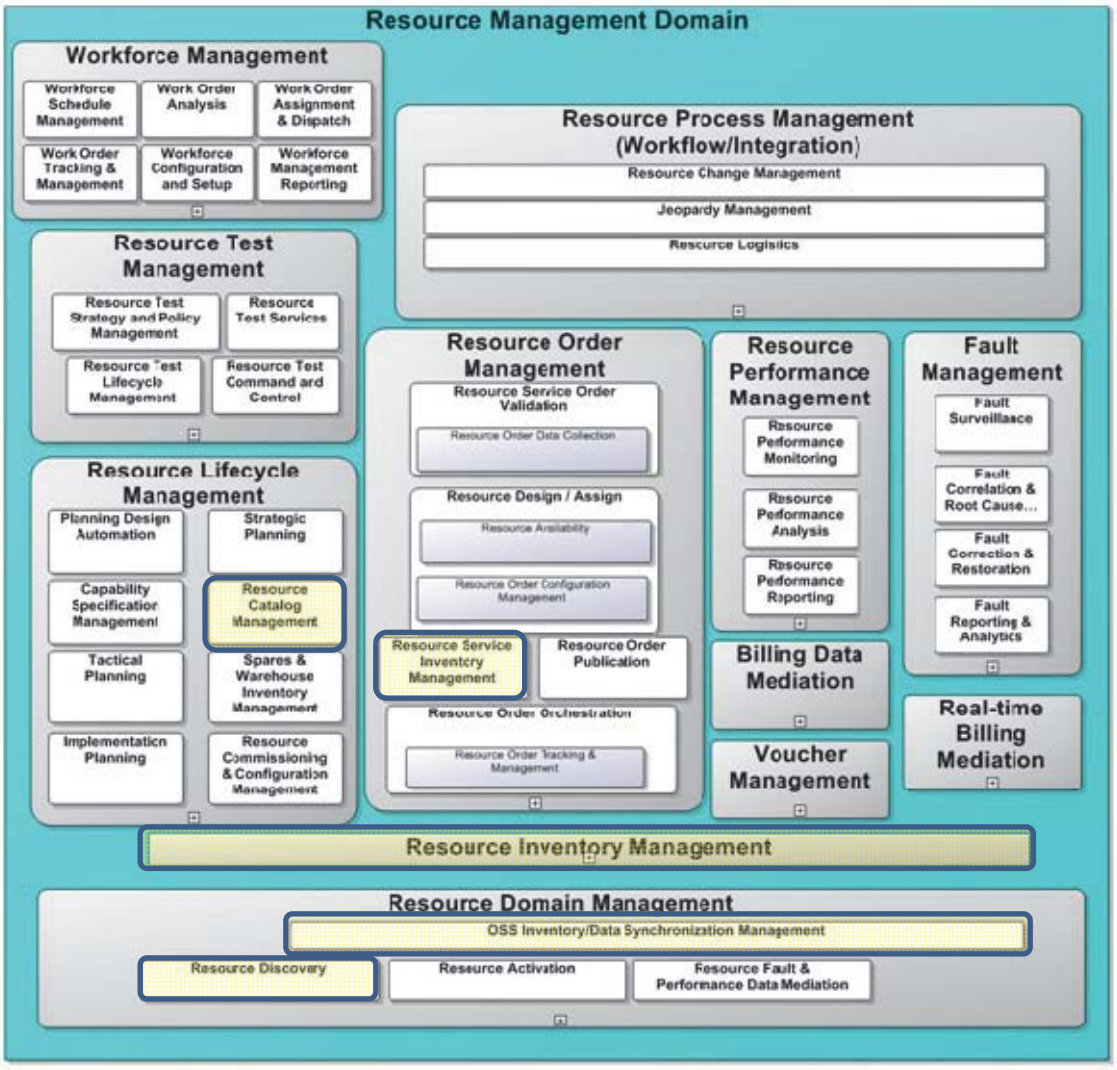

Figure 43: The constituents of NGCOR Resource Inventory Management reference model based on TMF TAM (v4.5) framework

As main logical capabilities and closely related functionalities of resource Inventory Management are

- Capabilities to manage, create, maintain and provide access to information of resource specifications/resource catalogs. The resource specifications are deployed by SI&P process functions (ref eTOM), and the resource catalog is initially populated by OS&R process functions (ref eTOM).
- Capabilities for providing and maintaining on-line resource instance information to automated and manual operation process functions. Resource instances are created based on resource specifications during fulfilment process and updated according usage assignment status of resources. All physical and logical configuration of the infrastructure including network elements and service systems (full e2e view: access, core, transport, control layer, application layer etc.) and their components as well as IT systems (SW and HW) are kept track on.
- Resource instance information is kept up to date with actual resource situation by resource discovery.
- Resource instance information is synchronized with other OSS applications keeping resource information up to date throughout OSS.

Considering the role of resource Inventory Management in management of dynamic information in the network – such as functioning of **Self Organized Network** (SON) features in the network elements, it can be generally characterized OSS and management environment needs (ref. NGMN Top 10 recommendations)

- OSS with SON needs to support of centralized, distributed and hybrid solution
- An NE can operate with SON function or without SON function and can easily be transferred between these two modes. The ability to suspend/ resume/ enable/ disable the SON function at determined break points shall be defined on a case by case basis
- Degree of automation to be configurable by the operator, spanning from operator controlled (open loop) to fully autonomous (closed loop).
- Support completely automated optimization cycle
- Support automated import of optimized settings
- OSS should provide a general SON monitoring & control application covering policy control, history log and switch on/off functionality. OSS shall be synchronized in real time with SON initiated network changes. Capability to monitor the specific results of each particular SON function needs to exist.

As regards to various optimization features enabled by SON (ANR, Cell Phy ID management, cell outage compensation, load balancing, etc) it is needed that

- OSS should provide analysis, alarms and user friendly visualization of the optimization feature in question
- OSS should provide the operator with resolution scenarios as suggestions for each specific optimization case which the operator can choose and select to solve the conflict resolution. Optionally these suggestions can be enabled automatically following operator policies

As a conclusion the dynamic and automatic behaviour of the network sets new requirements for both new types of OSS applications as well as keeping up-to-date information of the dynamic status of resources for Resource Inventory Management i.e. “automatic inventory”.

6.4.1.2 Resource Inventory interfacing with other OSS applications and with Resource Infrastructure

This chapter addresses various interfacing needs of resource Inventory Management. TMF TAM is here used as a generic model to present various applications/application areas of the OSS environment; more specifically NGCOR has used the latest framework model from TAM v4.5.

Operations Support & Readiness and closely resource Inventory Management related

- The Resource Inventory stores information on available capacity of logical and physical resources to be accessible **for service Inventory Management** in order to design a service. Service Inventory Management also uses information stored in the Resource Inventory to understand the infrastructure layer components and relations
- **Resource discovery** function provides means to upload and reconcile the Resource Inventory information with the actual network element information. The interface is either via element management systems or directly to network elements
- **Resource Inventory synchronization** function provides a common inventory view across the OSS applications in resource management and ensures OSS inventory data generated is available for other applications as required
- **Resource catalogue management** function is a repository of resource listing within a service provider and include the ability to design, create, augment and map new entities and supporting data

Fulfilment (Order Management, Provisioning, Activation)

- **Resource Order Management** retrieves equipment and connectivity details from the Resource Inventory in order to create requests to provision the network. It also stores intended and scheduled changes to the infrastructure in the Resource Inventory. Resource activation can also create in the Resource Inventory logical resources (e.g. connections) in support of services

Assurance

- **Fault Management** retrieves information from Resource Inventory in order to correlate resource faults with resource topology information to be used in various functionalities e.g. displaying operational status of resources, root cause analysis, fault correction and fault reporting
- **Service Problem Management/Trouble Ticketing** retrieves information from Resource Inventory to correlate service problems with resource topology information
- **Service Quality Management** retrieves information from Resource Inventory to correlate service quality with resource topology information
- **Performance Management** accesses the Resource Inventory for having topology information to identify the appropriate performance data collection points in order to accurately represent the performance of the resource

Resource Lifecycle Management

- **Resource Lifecycle Management** applications/functions such as resource planning, and Resource Deployment Management produce and consume Resource Inventory data
- **Resource Configuration** performs the equipment configuration to bring resources into operation. It performs initial equipment configurations triggered by SI&P processes (eTOM), and keeps the configuration data up to date.

Billing mediation

- **Billing data collection and mediation** accesses the Resource Inventory in order to retrieve topology information to identify the appropriate usage data collection points

Resource test management

- **Resource test management** accesses Resource Inventory for obtaining the resource information under testing

Resource process management

- Resource Inventory information is utilized in various workflows and process e.g. win change management and resource logistics

6.4.2 Service Inventory Management

6.4.2.1 Main Functionality

This chapter addresses service Inventory Management as a holistic concept without any attempt to consider possible approaches for implementations. The main function of **service Inventory Management** is to manage and store information of all service specifications (service catalogues) and service instances. The **Service Inventory** implements an abstraction layer between products (owned & managed by BSS) and resources (owned & managed by OSS). To enable collaboration between different domains, service inventories need to be harmonized. An agreement on a common service model (service specifications) for all involved domains is essential in that case.

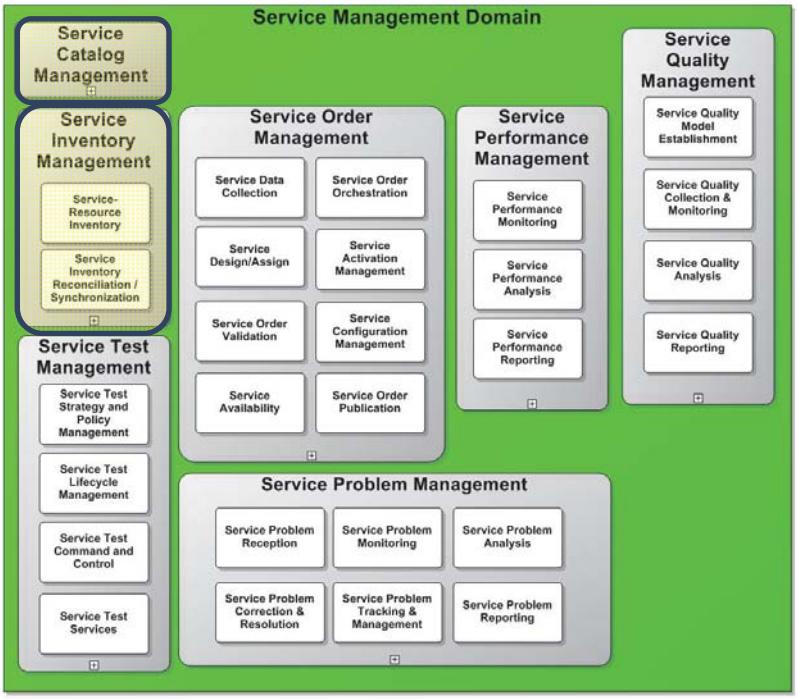

Figure 44: The constituents of NGCOR Service Inventory Management reference model based on TMF TAM (v4.5) framework

As main logical capabilities of service Inventory Management needs to include:

- **Service catalogue**: Captures the engineering view of the service offering and consists of collections of service descriptions as **Customer Facing Service Specifications** (CFSS) and **Resource Facing Service Specifications** (RFSS) including their relationships. RFSS are associated with resource specifications, stored in the resource catalogue, thus capturing the relationship between a service and the set of resources supporting this service.

  CFSS are associated with product specifications, stored in the product catalogue, thus capturing the relationship between a service and the product that is supported by this service.

Furthermore, related engineering characteristics for provisioning and monitoring can be included, e.g. a production plan that covers the activation sequence and timing considerations, which have to be ensured during instantiation.

The service specifications are deployed by SI&P process functions (eTOM), and the service catalogue is initially populated by OS&R process functions (eTOM).

- **Service instances** are created from service specifications during fulfilment processes, as Customer Facing Services (CFS) and Resource Facing Services (RFS), including their relationships among each other as well as with resource instances (RFS concerned) and product instances (CFS concerned).

6.4.2.2 Service Inventory interfacing with other OSS Applications

This chapter addresses various interfacing and integration needs of service Inventory Management. TMF TAM is here used as a generic model to present various applications/application areas of OSS environment; more specifically NGCOR has used the latest framework model from TAM v4.5.

Operations support & readiness

- **Service discovery** checks services (service instances) which have been discovered against the Service Inventory to validate data quality, and to trigger the reconciliation process in case of discrepancy
- **Resource Inventory implements - together with the Service Inventory -** the complete linkage between resources and services needed for the fulfilment, assurance, and mediation functions
- Service catalogue is a subset of general cross-domain catalogue management. A service catalogue deploys and stores service specifications as basis for Service Inventory information model definitions

Fulfilment (order management, provisioning, activation)

- Creates the service instances based on BSS requests
- Creates, updates and stores specific engineering properties, e.g. a production plan that covers the activation sequence and timing considerations, which have to be ensured during instantiation of services
- Implements information brokering towards BSS on service related matters

Assurance

- **Service Problem Management/Trouble Ticketing** retrieves service instance information, and navigates the Service Inventory for impact analysis
- **Service quality management** reads the service specification and service tree, and uses the information to set the desired monitoring thresholds
- **Test & diagnostics** retrieves service instance information, reads the test plans and stores test results

Billing Mediation

- Uses information from the Service Inventory for proper grouping of the Call Detail Records (CDR) as they are forwarded to BSS

Catalogue Management

- Catalogue management provides general, full lifecycle entity management capabilities cross domains, multilayer and acting as master repository for componentized entities of products, services and/or resources within one or more domains of a service provider's environment. Catalogue management includes the abilities

to create and design new entities, map entity definitions, manage complex rules, support componentization of entities and manage their relationships and dependencies. In service management layer context the consistency of service specifications mastered has to be ensured within the SM layer and SM with other layers in the catalogue. For example, how product definition translate to different services provisioning rules, and so on.

6.4.3 Product Inventory Management

6.4.3.1 Main Functionality

This chapter addresses product Inventory Management as a holistic concept without any attempt to consider possible approaches for implementations.

Figure 45: The constituents of NGCOR Product Inventory Management reference model based on TMF TAM (v4.5) framework

The main responsibility of the **Product Inventory** is to manage the **product catalogue** and keep track of the product subscriptions. The product catalogue defines the product offering from marketing perspective and consists of a collection of **product specifications**. Each product specification describes a **product type**. Several product specifications may be defined for the same product type. Product specifications are associated with service specifications, stored in the service catalogue, thus capturing the relationship between a product and the set of services bundled by this product.

Each subscription is captured in the Product Inventory through a product instance associated with the corresponding specification in the catalogue. The product instance is also associated with the subscriber of the product and the related subscriber account information.

6.4.3.2 Product Inventory Interfacing with other BSS/OSS Applications / Functions

- Customer SLA Management, Service Problem Management/Trouble Ticketing, and Billing and Customer Order Management use the information stored in the Product Inventory.
    - **Customer Order Management** function stores in the Product Inventory customer details, order and product detail, and account information acquired when a new order is created. Customer Order Management also retrieves product specifications from the product catalogue in order to create product instances and to decompose the product orders
    - **Service Problem Management/Trouble Ticketing** function may access the product inventory to correlate a subscriber to a service, and to retrieve details about the subscriber, when creating a trouble ticket
    - **Customer SLA Management** retrieves subscribers for given products and the subscriber contact information, using the product inventory

- Service Inventory Management retrieves product inventory information for capturing the relationship between a service and the product that is supported by this service

6.4.4 OSS Architecture reference model, emphasizing Inventory Management

In the following figure a common OSS architecture reference model is presented emphasizing the central role of Inventory Management within OSS. The model is aligned and adapted from TAM v4.5 focusing the key features of Inventory Management and related applications.

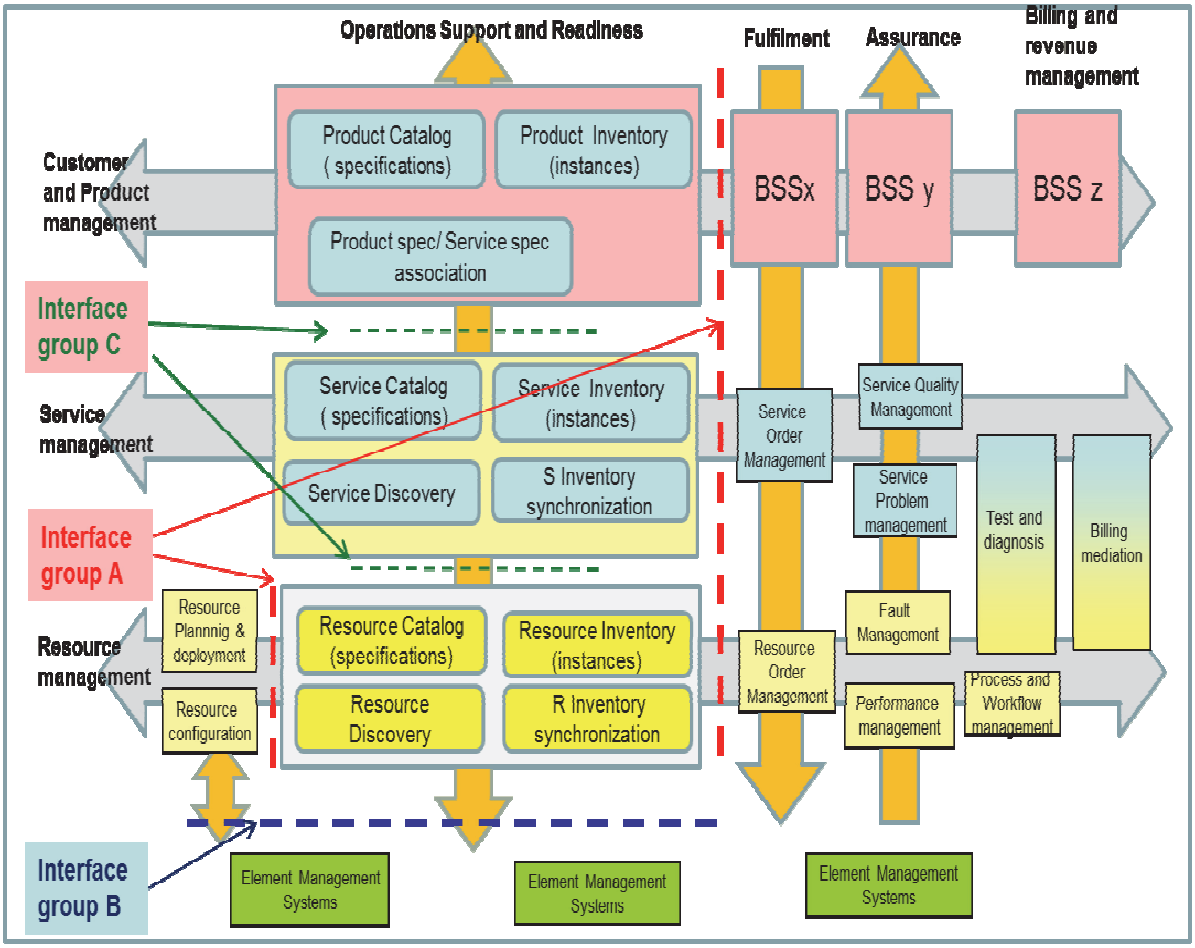

Figure 46: OSS reference architecture emphasizing Inventory Management

As a summary the key aspects of inventory focused OSS architecture reference model are

For Resource Inventory Management

- Storing of resource specifications (Resource Catalogue)
- Storing of resource instances (Resource Inventory)
- Resource instance information is kept up to date with actual resource situation by resource discovery. (Resource Discovery)
- Resource instance information is synchronized with other OSS applications keeping resource information up to date throughout OSS. (Resource Inventory Synchronization)

- Resource Inventory exposes services to external systems for
    - to modify the content of the repository or
    - to query the repository in order to collect specific information that it contains

For Service Inventory Management

- Storing of service specifications (Service Catalogue)
- Storing of service instances (Service Inventory)
- Service specifications are associated with resource specifications, stored in the resource catalogue, thus capturing the relationship between a service and the set of resources supporting this service. (Service Discovery).
- Service instance information is synchronized with other OSS applications keeping service information up to date throughout OSS. (Service Inventory Synchronization)
- Service Inventory exposes services to external systems for
    - to modify the content of the repository or
    - to query the repository in order to collect specific information that it contains

For Product Inventory Management

- Storing of product specifications (Product Catalogue)
- Storing of product instances (Product Inventory)
- Storing associations between product and service specifications

Inventory interfaces

- Interface group A: Interfacing between Inventory Management area (generally Resource, Service and Product Inventory Management) and other OSS applications. For each interfacing requirement presented in chapters 6.5 and 6.6 the respective positioning within the OSS reference architecture is indicated. Each interface of group A requires
    - a standardised information model of the data exchanged between the interworking OSS applications
    - a standardised operations model including the methods and parameters transferred over the interface
    - standardised notifications transferred over the interface

- Interface group B: Interfacing between Resource Inventory Management area and EMS layer. For each interfacing requirement presented in chapters 6.5 and 6.6 the respective positioning within the OSS reference architecture is indicated. Each interface of the group B requires
    - a network resource model representing the different underlying infrastructures which shall be compliant with the federated network information model (FNIM, ref. NGCOR Modelling and Tooling general requirements) for inventory
    - a standardised operations model including the methods and parameters transferred over the interface
    - standardised notifications transferred over the interface

- Interface group C: Indication of potential internal interfacing between different Inventory Management area building blocks. For each interfacing requirement presented in chapter 6.5 the respective positioning within the OSS reference architecture is indicated. For this Interface group it is however to be noted that internal structure and functionality may differ depending on the implementation model.

It is to be noted that Figure 46: OSS reference architecture emphasizing Inventory Management structure does not imply any implementation model. Which means that implementation models derived from this reference model can include variants e.g.

- Service and Resource Inventory may be implemented together or separately
- Discovery and synchronization may be implemented as separate applications or jointly with inventories
- Needed databases can be centralized or distributed and federated

Moreover it is to be noted some aspects which were not analysed in detail within this NGCOR project and thus potential items to consider for Inventory Management future work:

- Overall needs for common data management processes, represented by inventories, involving all lifecycle phases of Inventory Data Management. This is addressed by high level requirement (see REQ-InvM (9))
- Resources configuration data is in generic way regarded as part Resource Information Management, i.e. part of Resource Inventory Data, for example configuration information and parameters to setup and restore devices and applications of the SP's Production Infrastructure. However details for preferred model for implementation of needed data stores are not analysed further in NGCOR Inventory Management subtask. One possible implementation approach is illustrated in figure Figure 2: OSS architecture - agreed OSS Architecture: 80% based on Frameworx, 20% operator specific in a form of specific configuration inventory.
- Inventory Management as a subject of overall policy management framework of operators. A Policy Management Framework provides the capability to govern the observed behaviour of objects within the framework, e.g. defining access to information, resources, services, and the frame of administrative procedures. For example TMF Catalogue management descriptions expand the catalogue concept to include in addition to product/service/resource specifications also policy specifications. These policy specifications are to be utilized when evaluating the rules in policy decision s and enforcing the rules within the OSS architecture. One possible implementation approach is illustrated in Figure 2: OSS architecture - agreed OSS Architecture: 80% based on Frameworx, 20% operator specific in a form of a specific policy inventory.

6.4.5 Considerations Related to Other Reference Models

Figure 42: Key scope of InvM sub task in the eTOM framework shows the key scope of the NGCOR inventory sub task in terms of the **TMF business process framework** (eTOM). The relevant level 3 processes concerned by the project's work are "**Manage Service Inventory**" (MSI) and **Manage Resource Inventory** (MRI). MRI and MSI are part of the operations process area. Vertically they are included in the **Operations Support & Readiness** processes. Horizontally they are covered by the service management & operations processes (for MSI), and by the **Resource Management & Operations** processes (for MRI). Both MSI and MRI are defined to have wide interaction horizontally and vertically.

In relation to **ITIL framework** it is considered generally that ITIL practices and related system solutions share an analogue problem with telecom inventories on how information about IT infrastructure components and services can be managed. A respective key concept in ITIL framework is the **Configuration Management System** (CMS); a coherent logical model of the IT organization's infrastructure, typically made up of several **Configuration Management Databases** (CMDBs) as physical sub-systems. It is used to store information on all configuration items (CIs) under the control of configuration management. CIs are mainly hardware or software items and are characterized by their attributes (recorded in the CI's Configuration Record) and their relationships to other CIs. Similarly like telecom inventory information is used e.g. by other operations process the ITIL CI information is utilized by e.g. ITIL incident management, problem management and change management processes. It is notable that TMF and itSMF have done a joint technical work for converging TMF and ITIL concepts – the report is: TR143 Building bridges ITIL and eTOM.

The main characteristics of CMDB and also differences with inventory can be highlighted as follows

- CMDB maintains the relationships between all service components and any related incidents, problems, known errors, changes and release documentations
- CMDB may contain:
    - relationships between applications and server
    - SW version history trace for network equipment and applications in order to allow to restore previous version in case of rollback
    - Records with content of a release linked to all configuration Items that are affected by the release different type of CIs:
        - Service lifecycle CIs such as the business case, service management plans, service lifecycle plans, service design package, release, change plans and test plans. These CIs provide a picture of the service provider's services, how these services will be delivered, what benefits are expected, at what cost, and when they will be realized
        - Service CIs such as:
            - Service capability assets: management, organization, processes, knowledge, people
            - Service resource assets: financial capital, systems, applications, information, data, infrastructure and facilities, financial capital, people
            - Service model
            - Service package
            - Release package
            - Service acceptance criteria
        - Organization CIs: organization's business strategy or other policies that are internal to the organization but independent of the service provider. Regulatory or statutory requirements
        - Internal CIs comprising those delivered by individual projects, including tangible (data centre) and intangible assets such as software that are required to deliver and maintain the service and infrastructure
        - External CIs such as external customer requirements and agreements, releases from suppliers or sub-contractors and external services
        - Interface CIs that are required to deliver the end-to-end service across a service provider interface (SPI)
- CIs include also the details such as supplier, cost, purchase date and renewal date for licences and maintenance contracts and the related documentation such as SLAs and underpinning contracts

Inventory that is considered in OSS architecture provides to CMDB only information related to network configurations and service configurations linked to network resources and not information related to cost, licenses, contracts, etc. CMDB can be considered as a federated DB that takes from inventory only a set of information and takes from other sources additional information needed to support other ITIL processes.

Considering scoping with regards to 3GPP specifications it is to be noted that it is not possible to show direct match. 3GPP specifications do not model distinct management layers and structures for upper layer NMS/OSS (service management, resource management). Both resource infrastructure information and service related information is defined via NRM IRPs and interface IRPs.

Inventory Management IRP from 3GPP is defining the main task of the Inventory Management function at Itf-N to provide an efficient access for network management systems to the static inventory data of all related managed network elements. This is regarded as an essential part of overall Inventory Management reference model providing standard inventory data to be uploaded to NMS/OSS concerning the network elements in the scope of 3GPP.

6.5 High Level Inventory Management Requirements

This chapter outlines the high level Inventory Management requirements identified based on the analysis about the roles and functions of resource Inventory Management and service Inventory Management within the OSS architecture.

The focus of NGCOR Inventory sub task in the phase 1 was to get a common view on Inventory Management area in broad sense; the main Inventory Management concepts, the main roles and characteristics of inventories within OSS/BSS environment of operators. This was presented as high level Inventory Management requirements. In phase 2 of the NGCOR inventory sub-task during 2011 selected prioritized areas of high level requirement were worked out as more detailed use cases and requirements and presented in chapter 6.6.

The high level requirements deal with functional, information/operations modelling and interfacing aspects for Resource Inventory and Service Inventory. With regards to general information/operations modelling requirements and guidelines for information modelling arte facts the NGCOR section for Modelling and Tooling provides extensive set more detailed requirements and viewpoints.

6.5.1 Functional requirements

6.5.1.1 Resource Inventory

REQ-InvM (1) **Capability to manage resource models of variety of technology infrastructure domains and areas of converged fixed-mobile environment**
In order to be able to act in a centric role in managing and storing resource data in a converged fixed-mobile environment all different resources models from e2e management perspective shall be possible to manage.

REQ-InvM (2) **Capability to offer and maintain resource data to/with the different applications supporting planning & implementation, fulfilment, assurance and billing (generally SI&P, OSR, FAB), and with resource infrastructure**
Resource Inventory shall store and manage common data for other OSS applications and synchronized and reconciled with actual resource data.

REQ-InvM (3) **Capability to organize and offer ownership of resource information/data among applications, functions and processes.**
Mechanisms to have organized data master ships and ways for CRUD (creation/reading/updating/deleting) of Resource Inventory data.

REQ-InvM (4) **Capability to model and document the horizontal relationship (on physical and logical level) between resources, spanning all types of resource – technologies.**
Mechanisms to organize the horizontal relationship between resources. It must be possible to analyse the interworking of resources which delivers the E2E network service. The logical layer is needed to understand the ability of the network which delivers the E2E network service as a prerequisite for the Impact Analysis function in service management capabilities. The physical layer (including the documentation of redundancy) is a prerequisite for the impact analysis as well (e.g. to understand the impact of an outage on the E2E network service, and it is a prerequisite for root cause analysis in NMS.

REQ-InvM (5) **Capability to model and document the life cycle & usage state of network resources in line with the ITU-T Recommendation X.731 – Amendment 2.**
Inventoried resources shall have a life cycle attribute so that their deployment can be planned, tracked, and managed. Logical resources, e.g. connection, are also inventoried such that their deployment can be planned, tracked, and managed using a lifecycle state attribute.

6.5.1.2 Service Inventory

REQ-InvM (6) **Capability to manage service models of different domains and areas for converged fixed-mobile services.**
In order to be able to act in a centric role in managing and storing service data in a converged fixed-mobile environment all different services shall be possible to model and manage.

REQ-InvM (7) **Capability to offer and maintain service data to/with the different applications supporting planning & implementation, fulfilment, assurance and billing (generally SI&P, OSR, FAB).**
Service Inventory shall store and manage common data for other OSS applications.

REQ-InvM (8) **Capability to organize and offer ownership of service information/data among organization functions and processes.**
Mechanisms to have organized data master ships and ways for CRUD (Creation / Reading / Updating / Deleting) of Service Inventory data.

6.5.1.3 Resource and Service Inventory Data Management

REQ-InvM (9) **Capability to ensure high quality of Inventory data identification, control, status accounting & reporting, verification and audit.**
Mechanisms to ensure that inventory data is consistent and high quality throughout all data lifecycle including e.g. following; Resource & Service specifications will be agreed based on the respective SP business needs and the infrastructure technical needs, Inventory data storage and usage is controlled and authorized, inventory data can be reported and traced, Inventory data can be verified and audited.

6.5.2 Information / Operations Model Requirements

6.5.2.1 Resource Inventory

REQ-InvM (10) **A common harmonized and consistent resource information model covering different infrastructure domains of converged fixed-mobile environment.**
It is crucial that the data managed centrally in the Resource Inventory is comprehensive covering all different resources of a converged fixed-mobile environment and modelled in consistent way. Resource modelling characteristics and extensive details are presented in the section from “Modelling and Tooling” sub task of NGCOR.

REQ-InvM (11) **A common, harmonized, and consistent resource information model agreed between interworking OSS applications/areas for resource management.**
Resource Inventory manages and stores centrally common information for various other OSS applications. The other OSS applications producing or consuming Resource Inventory data shall have a common information model with Resource Inventory. Resource modelling characteristics

and extensive details are presented in the section from “Modelling and Tooling” sub task of NGCOR. The identification of object instances in the Resource Inventory shall be consistent with the network resource models used for all involved applications throughout OSS.

6.5.2.2 Service Inventory

REQ-InvM (12) **A common harmonized and consistent service information model covering different services of converged fixed – mobile environment.**
It is crucial that the data managed centrally in the Service Inventory is comprehensive covering all different services of a converged fixed-mobile environment and modelled in consistent way. Service modelling characteristics and extensive details are presented in the section from “Modelling and Tooling” sub task of NGCOR.

REQ-InvM (13) **A common, harmonized, and consistent service information model agreed between interworking OSS/BSS applications/areas for service management.**
Service Inventory manages and stores centrally common information for various other OSS applications. The other OSS applications producing or consuming Service Inventory data shall have a common information model with Service Inventory. Service modelling characteristics and extensive details are presented in the section from Modelling and Tooling sub-task of NGCOR.

REQ-InvM (14) **Vertical service information model, which contains the relationship of services to resource/product/customer – layers.**
Service Inventory manages and stores the relationship of services downwards to the resources they are built upon and upwards to the products and customer which make use of these services. This is a prerequisite for the impact analysis capability of the service management functions.

6.5.3 Interfacing Requirements

6.5.3.1 Resource Inventory

Abstract
In the following requirements the purpose of interfacing of Resource Inventory with different other OSS applications are explained. TMF TAM is used as a generic model to present various applications/application areas of OSS environment.

REQ-InvM (15) **Resource Inventory interfacing with Service Inventory Management.**
The Resource Inventory stores information on available capacity of logical and physical resources which needs to be accessible for service Inventory Management in order to design a service. This interface is represented by Interface group C in the Figure 46. Resource information models used are objects for standardization, but if a communication interface will be needed are dependent on how Resource Inventory/Service Inventory combined concept is implemented.

REQ-InvM (16) **Resource Inventory interfacing with resource order management.**
The Resource Order Management retrieves equipment and connectivity details from the Resource Inventory in order to create requests to provision the network. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (17) **Resource Inventory interfacing with Fault Management.**
Fault Management retrieves information from Resource Inventory in order to correlate resource faults with resource topology information. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (18) **Resource Inventory interfacing with Service Problem Management.**
Service Problem Management retrieves information from Resource Inventory to correlate service problems with resource topology information. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (19) **Resource Inventory interfacing with Service Quality Management.**
Service Quality Management retrieves information from Resource Inventory to correlate service quality with resource topology information. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (20) **Resource Inventory interfacing with performance management.**
Performance Management accesses the Resource Inventory for having topology information to identify the appropriate performance data collection points. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (21) **Resource Inventory interfacing with resource discovery.**
Resource discovery function provides means to upload and reconcile the Resource Inventory information with the actual network element information. The interface is either via element management systems or in some cases directly to network elements. Resource discovery interfaces towards network using interface is represented by Interface group B in the Figure 46 and is an object for standardization.

REQ-InvM (22) **Resource Inventory synchronization.**
Resource Inventory synchronizing function provides a common inventory view across the OSS management applications and ensures Resource Inventory data generated in each application is available to other applications as required. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (23) **Resource Inventory interfacing with billing mediation.**
Billing mediation accesses the Resource Inventory in order to retrieve topology information to identify the appropriate usage data collection points using standardized formats and protocols. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (24) **Resource Inventory interfacing with Resource Configuration.**
Resource Configuration performs the equipment configuration to bring resources into operation. It performs initial equipment configurations triggered by SI&P processes, and keeps the configuration data up to date. Resource Configuration interface towards network is represented by Interface group B in the Figure 46 and is an object for standardization.

REQ-InvM (25) **Resource Inventory interfacing with resource testing.**
Resource test management accesses Resource Inventory for obtaining the resource information under testing. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (26) **Resource Inventory interfacing with other Resource Lifecycle Management.**
Resource Lifecycle Management applications/functions such as Resource Planning, Resource Change Management and Resource Catalogue Management produce and consume Resource Inventory data. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

6.5.3.2 Service Inventory

Abstract
In the following requirements the purpose of interfacing/integration of Service Inventory with different other OSS applications is explained. TMF TAM is used as a generic model to present various applications/application areas of OSS environment.

REQ-InvM (27) **Service Inventory interfacing with fulfilment.**
Fulfilment creates the service instances based on BSS requests. It creates updates and stores specific engineering properties, e.g. a production plan that covers the activation sequence and timing considerations, which have to be ensured during instantiation of services. It implements information brokering towards BSS on service related matters. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (28) **Service Inventory interfacing with Service Problem Management / trouble ticketing.**
Service Problem Management (including service monitoring functions) / trouble ticketing retrieves service instance information, and navigates the Service Inventory for impact analysis. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (29) **Service Inventory interfacing with Service Quality Management.**
Service Quality Management reads the service specification and service tree, and uses the information to set the desired monitoring thresholds. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (30) **Service Inventory interfacing with SLA management.**
SLA management reads the service specification and service tree, and uses the information to set the desired SLA thresholds. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (31) **Service Inventory interfacing with test & diagnostics.**
Test & diagnostics retrieves service instance information, reads the test plans, and stores test results. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (32) **Service Inventory interfacing with billing mediation.**
Billing mediation accesses to information in the Service Inventory for proper grouping of the CDR as they are forwarded to BSS, using standardized formats and protocols. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (33) **Service Inventory interfacing with service discovery.**
Service discovery checks services (service instances), which have been discovered, against the Service Inventory to validate data quality, and to trigger the reconciliation process in case of discrepancy. This interface is represented by Interface group A in the Figure 46 and is an object for standardization.

REQ-InvM (34) Service Inventory interfacing with Resource Inventory.
Resource Inventory implements, together with the Service Inventory, the complete linkage between resources and services needed for the fulfilment, assurance, and mediation functions (OSS). This interface is represented by Interface group C in the Figure 46. Service and Resource information models used are objects for standardization, but if a communication interface will be needed are dependent on how Resource Inventory/Service Inventory combined concept is implemented.

REQ-InvM (35) Service Inventory interfacing with product / customer inventory.
Service Inventory implements, together with the product / customer inventory, the complete linkage between services and products and customers, needed for the fulfilment and assurance functions (OSS). This interface is represented by Interface group C in the Figure 46. Service and Product/customer information models used are objects for standardization, but if a communication interface will be needed are dependent on how Service Inventory/Product inventory combined concept is implemented.

REQ-InvM (36) Service Inventory interfacing with catalogue management.
Service catalogue is a subset of general cross-domain catalogue management. Service catalogue deploys and stores service specifications as basis for Service Inventory information model definitions supporting full lifecycle of services including e.g. test plans. This interface is internal within Inventory Management area. Information models used are objects for standardization.

6.6 Use cases and related detailed requirements

In this chapter several architecture scenarios are presented to exemplify how Inventory Management described by OSS architecture reference model, Figure 46, can support effectively some key operational and lifecycle processes. The scenarios deal use cases for Resource Inventory Management and showing benefits to have uniform and well-structured Information Management for all resources throughout the full lifecycle of resources. From each use case are then derived more detailed requirements to complement the high level requirements presented in chapter 6.5.

6.6.1 Architecture Scenario: Resource Inventory Management Support for Fault Management

In this scenario focus is on two key applications of the OSS architecture reference model, Figure 46, Resource Inventory and Fault Management and their interrelation. This scenario highlights the benefits to have all information related to resource infrastructure; all physical and logical resources of a converged infrastructure, their naming, interrelations and topologies formed etc. managed in a uniform and structured way. Fault Management and users of it don't need to manage and administrate all resource information, only to have relevant information which is needed in its tasks e.g. for processing the alarms, enriching the alarm information, correlating single alarm in relation to whole topology and visualizing alarms to users.

Following use cases are described

- Alarm handling capabilities: how Resource Inventory supports Fault Management to get initial resource information (it is assumed that all possible domains of converged infrastructure are present and included in the models)
- Enrichment of Alarm info & Alarm Prioritization; how Resource Inventory information provided supports in enriching single alarm message information for prioritization and visualization & presentations purposes (it

is assumed that alarm message content includes which resource instance is source of alarm and not every alarm cause a query to Resource Inventory)

- Alarm correlation and root cause analysis; how Resource Inventory information is used to analyze group of simultaneous alarms, correlating between those and searching the root cause. How resource data included in Fault Management is synchronized with the master data in Resource Inventory
- How the potential conflicts between resource instance information included in the alarm message content and information stored in the Fault Management are solved assisted by Resource Inventory

	Alarm handling capabilities	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	Saving operational costs and increasing service quality through fast fault clearance is essential for operation of the NGMN network. All alarms from all NEs in the Access-, Core-, and Transmission network and IT resources need to be received, diagnosed, solved and managed efficiently.	
Actors and roles (*)	Typically staff in network operation centres	
Telecom resources	Operational network and service production Operational OSS system environment including Resource Inventory and Fault Management system	
Assumptions	For efficiency gains and cost reduction it is recommended to have a harmonized interface between the EMS level and the NMS level where discovery & reconciliation functionality is placed.	
Pre-conditions		
Begins when	Resource instance information is created or updated in the Resource Inventory, after which they can be provided to Fault Management application	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)	Fault Management application is provided with an up to date resource information and it is ready for operation	
Exceptions		
Post-conditions		
Traceability (*)		

The resulting requirements / capabilities:

REQ-InvM (37) Resource Inventory shall model the resource information of the elements and the topology.

REQ-InvM (38) Resource Inventory shall provide actual resource information (not later than n hours after a change of a configuration has happened) to the Fault Management.

REQ-InvM (39) Resource Inventory shall provide the topology information of the network to the Fault Management.

REQ-InvM (40) Resource Inventory shall support the required data modelling and data entry (manual as well as via discovery & reconciliation).

	Enrichment of Alarm info & Alarm Prioritisation	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	Reduction of high of work expenses in the Fault Management process caused by manual work. (Resource and cost perspective as well as data quality issue). When having high number of alarms it is essential to prioritize incoming alarms based on their business impact. Incident-Tickets for IP-Hardware-Components (e.g. Router, Server, Switches, and Storages etc.) have to be enriched during the Incident Detection & Recording phase. In many cases alarm priorities from 1 to n are derived from the combination of a network element classification and the criticality of the alarm.	
Actors and roles (*)	Typically staff in network operation centres	
Telecom resources	Operational network and service production Operational OSS system environment including Resource Inventory and Fault Management system	
Assumptions		
Pre-conditions	Information input during the planning phase, during the deployment phase and during the operation phase of the NE life-cycle has to deliver a Resource Inventory with high data quality. Network Elements have unique identifiers.	
Begins when	Alarm record concerning a specific NE is received by FM Application.	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)	Alarm record is enriched and categorized according its priority class	
Exceptions		
Post-conditions	Incident-Ticket populated with relevant information.	
Traceability (*)		
NOTE – Fields marked with "*" are mandatory for all use case specifications. Other fields are only mandatory when relevant for the specific use case.		

The resulting requirements / capabilities:

REQ-InvM (41) **Interfaces between the Resource Inventory and Fault Management application have to be set up.**

REQ-InvM (42) **Near real-time data synchronization via these interfaces has to be implemented.**

REQ-InvM (43) **It should be configurable which attributes will be available for enrichment and which are synchronized between Resource Inventory and the related applications.**

REQ-InvM (44) **Enrichment of Incident-Tickets for IP-Hardware-Components (e.g. Router, Server, Switches and Storages etc.) needs well documented and actual information in the Resource Inventory**

REQ-InvM (45) **Incident-Tickets, created from an initiating Alarm, are to be populated with information (attributes: 1, 2, 3) from this initiating Alarm and also with information (attributes: a, b, c) from the Resource Inventory (Example for a, b, c: location, responsible person, accessibility,).**

	Alarm correlation and root cause analysis	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	Quick resolution of root cause of for a group of simultaneous alarms. Miscellaneous Comments / Useful hints: Further design work is required to detail these correlations. In most cases topology information provided by Inventory Management systems will be required.	
Actors and roles (*)	Typically staff in network operation centres	
Telecom resources	Operational network and service production Operational OSS system environment including Resource Inventory and Fault Management system	
Assumptions	Further design work is required to detail correlations rules and logic.	
Pre-conditions		
Begins when	Alarm record or group of alarms are received by Fault Management application	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)	Alarm information is processed according to correlation criteria, root cause is identified	
Exceptions		
Post-conditions		
Traceability (*)		

The resulting requirements / capabilities:

REQ-InvM (46) Interfaces between the Resource Inventory and Fault Management application have to be set up.

REQ-InvM (47) Near real-time data synchronisation via these interfaces has to be implemented.

REQ-InvM (48) Topology information is passed over to Fault Management

REQ-InvM (49) It should be configurable which attributes will be available in the Resource Inventory and which are synchronized between Resource Inventory and Fault Management.

6.6.2 Architecture Scenario: Resource Inventory Management Support for Resource Configuration

In this scenario focus is on two applications of the OSS architecture reference model, Figure 46, Resource Inventory and Resource Configuration and their interrelation. This scenario highlights the benefits to have all information related to resource infrastructure, configuration of it and its detailed features closely related to each other and centrally managed and in a uniform and structured way. In the architecture model the concept resource Inventory Management includes not only the resources, but also the configuration structure information of resources i.e. the parts and also configuration parameter information. The architecture model does not imply any directives or proposals of detail technical implementations, the different data storages and databases may be implemented as distributed or centralized ones.

Following use cases are described

- Initial configuration of parameter settings after first deployment of resources. This capability has to span over a wide set of converged infrastructure, actual parameters differ from resource to resource
- Managing Resource Configuration and parameter setting changes as a result of SON function, example self-configuration
- Self-Test & Automatic Inventory, example for eNodeB

	Initial configuration	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	Minimizing separate phases for manual entering of resource information by providing automated flow of usage of resource information produced by planning & deployment from Resource Inventory to Resource Configuration	
Actors and Roles (*)	Typically staff in network operation center or dedicated network implementation staff	
Telecom resources	Network and service production environment under preparation for Operational phase Operational OSS system environment including Resource Inventory and Resource Configuration	
Assumptions	Resource Inventory and Resource Configuration applications are implemented and operational	
Pre-conditions	Resources and their initial parameter settings are planned by planning and respective information instantiated in Resource Inventory Resources are deployed and connected to OSS	
Begins when	Human operator determines the object(s) for configuration and initiates configuration phase after planning and deployment	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)	The resource(s) as object for parameter setting have all been configured	
Exceptions		
Post-conditions	New parameter settings in the resources are ready for operational use	
Traceability (*)		

The resulting requirements / capabilities:

REQ-InvM (50) Configuration parameter settings for the resource as the object are retrieved from Resource Inventory by Resource Configuration

REQ-InvM (51) Resource Configuration send the configuration parameters to the resource as object for configuration

REQ-InvM (52) Resource Configuration notifies Resource Inventory about the results of configuration activity (successful or some problems)

	Support for Plug&Play Self Configuration, eNodeB	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	New eNodeBs have plug and play self-configuration capabilities. This saves specialized personnel from visiting the installation site and performing a manual set up of the eNodeB. This saves overall commissioning costs. Based on information delivered by the DHCP server/Configuration Server the eNodeB starts to establish a bidirectional, stable and secure end-to-end connection during its plug&play deployment phase. The eNodeB requests the configuration data from Resource Configuration. The configuration data matching with the same characteristics as the requesting eNodeB (unique eNodeB identifier is used to bind a configuration data with the actual eNodeB HW), is retrieved as the planned parameter set dedicated to the requesting eNodeB. This parameter set, consisting of dedicated radio- and IP-parameters plus a set of default parameters may have been aggregated into a configuration file based on policy or other selection criteria. This file is delivered back to the requesting eNodeB. The eNodeB reconfigures itself and comes up with its final IP addresses and a radio configuration.	
Actors and Roles (*)	Typically staff in network operation center or dedicated network implementation staff	
Telecom resources	Network and service production environment under preparation for Operational phase Operational OSS system environment including Resource Inventory and Resource Configuration	
Assumptions	The initial assignment of address, OSS and x-GWs, for a dedicated eNodeB is assumed to be a planning activity. Initial Data will be set up in the Planning Tools.	
Pre-conditions	The eNodeB is physically installed and all physical connectors are plugged in. A unique eNodeB identifier has been transferred into the eNodeB by appropriate medium latest during the onsite installation phase. It has a temporary IP Address assigned and has established secure end-to-end connections to the security servers and the element manager. There shall be no need to pre-configure the eNodeB by the vendor or the Operator. The configuration data maybe aggregated as a specific configuration file.	
Begins when	ENodeB initiates the self-configuration	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)	ENodeB has established its operational parameter settings	
Exceptions		
Post-conditions		
Traceability (*)		

The resulting requirements:

REQ-InvM (53) **Resource Configuration shall be provided by a bidirectional interface to Resource Inventory for parameter transfer (Basic set of parameters is defined by the planning tool (IP addresses, location, HW, transmission...))**

REQ-InvM (54) **Configuration data respective to planned resources, eNodeBs, has to be prepared in Resource Inventory to be addressed by Resource Configuration requests, Configuration data may be aggregated as configuration files.**

REQ-InvM (55) **Configuration data shall be transferred to eNodeBs in accordance with the northbound interface specification for SON enabled Plug & Play configuration of the eNodeB.**

	Self Test & Automatic Inventory, eNodeB	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	Self-testing of nodes supported by automatic status reporting saves specialized personnel from visiting the installation site and performing a manual report of the eNodeB characteristics. Following the final self-test the eNodeB delivers • a state change notification • details on its Resource Configuration Which information is updated in Resource Inventory for the respective resource.	
Actors and Roles (*)	Typically staff in network operation center or dedicated network implementation staff	
Telecom resources	Network and service production environment under preparation for Operational phase Operational OSS system environment including Resource Inventory and Resource Configuration	
Assumptions		
Pre-conditions	The eNodeB is physically installed and all physical connectors are plugged in. It has an IP Address assigned and has retrieved its configuration data / parameter set from Resource Inventory.	
Begins when	ENodeB has set up its confirmation and is ready for testing before put into operation	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)	Resource and its configuration data has been updated in the Resource Inventory	
Exceptions		
Post-conditions		
Traceability (*)		

The resulting requirements:

REQ-InvM (56) **Resource Inventory shall enable to discover/upload eNodeB data and reconciliate (between planned data and uploaded data) in real-time and respectively at dedicated intervals (<= 24h).**

- the resource data for each installed eNodeB
- the configuration data for each installed eNodeB

REQ-InvM (57) **Resource Inventory shall have access to these parameter sets on request via Itf.-N in accordance with the northbound interface specification.**

6.6.3 Architecture Scenario: Resource Inventory Management Support for Planning and Deployment

In this scenario focus is on is on two applications of the OSS general architecture reference model, Figure 46, Resource Inventory and Planning & deployment and their interrelation. Planning and deployment is a vast area where very often both operator's own staff and as well as external contractors are co-operating and using variety of OSS systems. The scenario highlights the benefits to have all information related to resource infrastructure

managed in a uniform and structured way. Planning & deployment systems and users of them don't need to maintain and administrate common resource information which is centrally stored can accessed via interaction with Resource Inventory. The main purpose for Resource Inventory support for planning and deployment is for technical issues, not for financial aspects of those.

Following use cases are described

- Planning of new resources or extending capacity and utilizing Resource Inventory providing the existing resource information; resource topology, geography, location, capacity etc. when
- Planning providing initial technical parameter configurations settings e.g. radio parameters or transmission equipment parameters to be used in technical configuration
- Resource deployment support; Resource Inventory providing resource information for various phases of deployment (network construction, implementation and changes), e.g. for roll-out work implementation planning, managing spare part stores and information on them, infra site acquisition and management, network technical implementation etc. as well as deployment providing updated or status information on executed work on resources indicating readiness for operation
- IP address management and planning / implementation support

	Planning of resources	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	Utilization and updating of Resource Inventory information when planning new resources or extending capacity	
Actors and Roles (*)	Planning staff	
Telecom resources	Network production environment under planning (new or changes) for operational phase Operational OSS system environment including Resource Inventory and Planning system	
Assumptions	Resource Inventory and planning systems are implemented and operational.	
Pre-conditions	Resource Inventory and planning system are interconnected in OSS environment	
Begins when	Planning of new resource is initiated	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)	Planning of new resources is considered completed	
Exceptions		
Post-conditions	New resource information successfully updated to Resource Inventory and available for further phase in deployment and operation	
Traceability (*)		

The resulting requirements / capabilities:

REQ-InvM (58) Planning systems need to retrieve resource information from Resource Inventory concerning current resources and/or their capacity

REQ-InvM (59) Planning systems need to update Resource Inventory with new information about planned resources and their characteristics and parameters

	Planning of basic (eNodeB) parameters for Plug&Play	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	Basic node parameters have to be provided as a pre-deployment activity. This allows to minimize detailed manual planning of neighbour relations, frequencies etc. This saves specialized personnel from visiting the installation site and performing a manual set up of the eNodeB. During the installation and commissioning phase each eNodeB has to be provided with a set of configuration data, this configuration data consist of the elements: • Site specific eNodeB parameters; • dummy cell parameter; • standard cell spec. parameters having a generic, net wide nature and underlying a change from time to time; • SP specific transport parameters having a generic, net wide nature;	
Actors and Roles (*)		
Telecom resources	Network and service production environment under preparation for Operational phase Operational OSS system environment including Resource Inventory and planning & deployment systems	
Assumptions	It is assumed that IP address and address range planning is internationally coordinated.	
Pre-conditions		
Begins when	Planning of new resource is initiated including the detailed parameters	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)	Resource Inventory is updated with new resource parameter information	
Exceptions		
Post-conditions		
Traceability (*)		

The resulting requirements:

REQ-InvM (60) **The Planning tool shall allow a consistent planning of all these parameter values, maintain them in its database and provide an interface to the Resource Inventory for parameter transfer.**

REQ-InvM (61) **The Resource Inventory shall allow maintaining and presenting the above mentioned set of dedicated parameters including ANR specific values for each planned eNodeB (normally prepared by the planning processes).**

REQ-InvM (62) **The Resource Inventory shall provide an interface to the Planning Tools for parameter transfer (Basic set of parameters is defined by the planning tool (IP addresses, location, HW, transmission...)).**

	Resource deployment (construction and implementation)support	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	Efficient resource construction and implementation and by utilization and having up to date Resource Inventory information when building or changing resources or capacity.	
Actors and Roles (*)	Implementation and constructions staff, may include operator's own staff and sub-contractors	
Telecom resources	Network production environment under implementation and deployment (new or changes) for operational phase Operational OSS system environment including Resource Inventory and construction and implementation support systems	
Assumptions	Resource Inventory and planning systems are implemented and operational.	
Pre-conditions	Resource Inventory is interconnected with necessary OSS environment	
Begins when	Deployment of the planned resources is initiated	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)	Resources are deployed ready for operational use	
Exceptions		
Post-conditions		
Traceability (*)		

The resulting requirements / capabilities:

REQ-InvM (63) Construction and implementations support systems need to retrieve resource information from Resource Inventory concerning resources planned to be deployed; information is for example about; equipment types, volumes, implementation sites and locations etc.

REQ-InvM (64) Resource Inventory information is updated with new information about implemented resources and their readiness for operation

REQ-InvM (65) Specific security and access control mechanism has to be established for external sub-contractors

Use case IP address management and planning / implementation support

Most SP and enterprise organizations will obtain public IP address space from their national or regional Internet Registry, e.g., xxx and RIPE. After a block of public IP address space has been obtained, it can then be allocated to address pools and from there be assigned to locations, subnets, devices and ports across the network. Similarly, private IP address space will be allocated in that way.

When planning to allocate IP addresses - whether private or public ones - planners and administrators must forecast the IP address capacity requirements in each subnet on the network. This is typically based on the number of devices and ports located at each site, or the number of dynamically active users or mobile users expected at the site (DHCP!), and the number of IP addresses required on average for each end user of a service. Another aspect is, for example, routers in the backbone that need to be configured to provide priority processing on VoIP packets versus best-effort data packets.

Address planning and assignment is best performed using a centralized Resource Inventory containing the IP addresses as logical resources. A centralized Resource Inventory provides a holistic view of the entire address space deployed over a number of sites and with address pools deployed on multiple DHCP and DNS servers throughout the network.

	IP address management and planning / implementation support	
Use case stage	**Evolution/Specification**	**<<Uses>> Related use**
Goal (*)	Efficient, consistent and centralized handling of the IP address space by having up to date Resource Inventory information when building or changing resources and assigning / reassigning IP addresses.	
Actors and Roles (*)	Planning and deployment staff, may include operator's own staff and sub-contractors	
Telecom resources	Network production environment under implementation and deployment (new or changes) for operational phase Operational OSS system environment including Resource Inventory with IP address pools as logical resources	
Assumptions	Resource Inventory and planning systems are implemented and operational.	
Pre-conditions	Resource Inventory is interconnected with necessary OSS environment.	
Begins when	Obtaining IP address space from Registry	
Step 1 (M|O)	Deposit IP addresses in the Resource Inventory IP address pool	
Step 2 (*) (M|O)	IP addresses are assigned to resources	
Step 3 (*) (M|O)	IP addresses are assigned to resources	
Step n (M|O)		
Ends when (*)	IP addresses are reconciled between the network and the Resource Inventory	
Exceptions		
Post-conditions	The set of IP addresses assigned to resources + the set of IP addresses assigned to DHCP servers + the set of IP addresses remaining in the IP address pool is id to the IP address space obtained from Registry	
Traceability (*)		

The resulting requirements / capabilities:

REQ-InvM (66) **IP address space (logical resources) is part of the Resource Inventory – Resource Inventory provides capabilities for obtaining and defining public and private IP address space, and allocating parts of that address space to locations, subnets, devices, ports and address pools**

REQ-InvM (67) **Resource Inventory provides capabilities for defining subnets and VLANs**

REQ-InvM (68) **IP address allocations (whether manual or automatic) have to be recorded in a log and as attribute of the target object**

REQ-InvM (69) **A periodical reconciliation of actual IP-related data from the network with the Resource Inventory has to be performed - Resource Inventory information can be updated with information about assigned IP addresses and planning & design faults in the network can be recognized**

7 REFERENCES

[1] NGMN Alliance NGMN TOP OPE Requirements Version 1.0
[2] NGMN NGCOR Consolidated Requirements V0.93
[3] University of Southern California - Center for Software Engineering - COTS Software Integration Cost Modelling Study 1997
[4] COCOTS (COnstructive COTS) - a cost estimation model to capture most important costs associated with COTS component integration, October 2002
[5] “Next-generation service assurance improves operational efficiency” in TM Forum CaseStudy Handbook 2012
[6] 3GPP TR 32.828 version 1.5.0. Study on Alignment of 3GPP Generic NRM IRP and TMF Shared Information/Data (SID) Model
[7] 3GPP TS 32.140. Subscription Management (SuM) requirements
[8] 3GPP TS 32.101 Telecommunication management; Principles and high level requirements
[9] 3GPP TS 32.300 Configuration Management; Name convention for Managed Objects.
[10] 3GPP TS 32.341/2/6. File Transfer (FT) Integration Reference Point (IRP); Requirements
[11] 3GPP TS 32.611/2/5 v10 Configuration Management (CM); Bulk CM Integration Reference Point (IRP): Requirements
[12] 3GPP TS 32.622. Configuration Management (CM); Generic network resources Integration Reference Point (IRP); Network Resource Model (NRM)
[13] 3GPP TS 32.690 V10 Release 10. Inventory Management (IM); Requirements
[14] 3GPP TS 32.691/2/6 V10.x.0 Release 10. Inventory Management (IM) network resources Integration Reference Point (IRP): Requirements
[15] 3GPP TS 32.692. Inventory Management (IM) network resources Integration Reference Point (IRP): Network Resource Model (NRM)
[16] 3GPP TS 32.xyz series on NRM.
[17] ATM Forum, Technical Committee, Network Management, M4 Network View CMIP MIB Specification, CMIP Specification for the M4 Interface, Sep, 1995.
[18] JOSIF Guidebook. Source: http://sourceforge.net/apps/mediawiki/openoss/index.php?title=JOSIF_Guidebook
[19] NGWW 3GPP SA5-TM Forum model alignment JWG meeting in Budapest, April 4-6, 2011.
[20] NGWW Fixed Mobile Convergence (FMC) Network Management – Federated Network model (FNM) Umbrella, Version 1.2 JWG meeting in Budapest, April 4-6, 2011.
[21] S5-102610 S5vTMFa033 E NSN Proposed enhancement of Generic NRM IOCs v3.
[22] TM Forum (2008a, Mai). DDP BA, TMF518_MRI, Version 1.1.
[23] TM Forum (2008b, Mai). DDP BA, TMF518_MSI, Version 1.0.
[24] TM Forum (2011, January). TM Forum Interface Program, Inventory Interface, Progress Status at TAW Paris.
[25] TM Forum GB922, Information Framework (SID) Suite, Release 9.0. Source: http://www.tmforum.org/browse.aspx?catID=9285&artf=artf2048
[26] TMF MTOSI 2.0. Source: http://www.tmforum.org/MTOSIRelease20/MTOSISolutionSuite/35252/article.html
[27] TM Forum MTOSI 2.0: Network Resource Fulfillment DDP IA, TMF612_NRF, Version 1.0.
[28] TM Forum Information Framework (SID) Suite; Release 9.5. Source: http://www.tmforum.org/Guidebooks/GB922InformationFramework/45046/article.html
[29] TM Forum MTOSI Rel. 2.1 supporting document SD2-5_Communication_Styles.
[30] TM Forum SID Rel. 9.5.
[31] TMF & itSMF TR 143 Building bridges ITIL and eTOM.
[32] TR143 Abgerufen Juli 18, 2011, von about:blank
[33] TR166 - Federated Information Framework - Concepts and Principles - v0.1.docx.
[34] UML Superstructure Specification, v2.1.1.

[35] 3GPP TS 32.300 Telecommunication management; Configuration Management; Name convention for Managed Objects
[36] S5-102610 S5vTMFa033 E NSN Proposed enhancement of Generic NRM IOCs v3
[37] S5vTMFa169 (3GPP/TM Forum Concrete Model Relationships and Use Cases) from 3GPP SA5-TM Forum Resource Model Alignment JWG ftp://ftp.3gpp.org/tsg_sa/WG5_TM/Ad-hoc_meetings/Virtual-TMF-Align/S5vTMFa169.zip
[38] TR166 - Federated Information Framework - Concepts and Principles - v0.1.docx
[39] Fixed Mobile Convergence (FMC) Network Management – Federated Network Model (FNM) Umbrella, Version 1.2 JWG meeting in Budapest, April 4-6, 2011
[40] TM Forum MTOSI Release 2.1 (http://www.tmforum.org/MTOSIRelease21/11998/home.html)
[41] TM Forum Information Framework (SID) Suite; Release 9.5 (http://www.tmforum.org/Guidebooks/GB922InformationFramework/45046/article.html)
[42] TM Forum MTOSI Release 2.1: Supporting document SD2-5_Communication_Styles (http://www.tmforum.org/MTOSIRelease21/11998/home.html)
[43] JOSIF Guidebook (http://sourceforge.net/apps/mediawiki/openoss/index.php?title=JOSIF_Guidebook)
[44] OMG Unified Modeling Language (OMG UML), Superstructure, Version 2.3 (http://www.omg.org/spec/UML/2.3/Superstructure/PDF)
[45] TM Forum MTOSI Release 2.1: Supporting document SD0-2_Guidelines_BA (Business Agreement Guidelines) (http://www.tmforum.org/MTOSIRelease21/11998/home.html)
[46] TM Forum Business Process Framework (eTOM) Release 9 (http://www.tmforum.org/StandardsPacks/8175/home.html)
[47] NGMN TOP OPE Requirements Version 1.0
[48] NGCOR Consolidated Requirements V0.93
[49] CCITT Rec. X.733 specification
[50] CCITT Rec. X.210 | ISO/TR 8509
[51] CCITT Rec. X.710 | ISO/IEC 9595
[52] eTOM Release 9.0, GB921 Addendum D,, TM Forum, August 2010
[53] TM Forum TAM Release 4.5, TMF, April 2011
[54] SID Release 9.5, GB922 Concepts and principles, TMF, March 2011
[55] TM Forum TR143, eTOM and ITIL, Building Bridges
[56] NGMN Top OPE recommendations
[57] This concept is explained further in TM Forum document SD2-1, MTOSI Implementation Statement (see section 2.5.1, Publisher Notification Suppression).
[58] TM Forum Manage Resource Inventory - DDP BA, TMF518_MRI, Version 1.1, May 2008.
[59] TM Forum Manage Service Inventory - DDP BA, TMF518_MSI, Version 1.0, May 2008.
[60] OSS/J Inventory API, JSR-142 Overview, Release 1.0, TMF888, TM Forum Approved Version 1.3, January 2010
[61] TM Forum comparison study of OSS/J, MTOSI and 3GPP inventory interface approaches
[62] TMForum Interface Program, Inventory Interface, Progress Status at TAW Paris (Jan 2011).
[63] TM Forum Product, service and resource inventory retrieval for cloud and IT
[64] TM Forum Product, service and resource inventory update for cloud and IT
[65] in 3GPP TR 32.828 version 1.5.0
[66] 3GPP TS 32.341/2/6
[67] TMForum TR 146 Lifecycle Compatibility Release 1-0
[68] ITIL v3
[69] TM Forum, Catalog Management FDD v1.12
[70] 3GPP TS 32.171 Subscription Management

8 APPENDIX

8.1 Glossary and Abbreviations

Abbreviation	Meaning & Terms	Further explanation
2G/3G/LTE	Standards for mobile communication network and devices capabilities	
3GPP	3rd Generation Partnership Project	http://www.3gpp.org
3GPP SA5	Telecom Management group within 3GPP	http://www.3gpp.org/SA5-Telecom-Management
AAA	Authentification and Authorization & Accounting	Function providing a network service related to billing & charging system
ABR	Asynchronous Batch Response	Is a message exchange pattern. This is a multiple response pattern. The response of the first invocation returns an acknowledgement. The result set will then be sent in chunks to the service consumer (via the call back receptacle) as the data becomes available in the service producer. The consumer usually has control over the size of the chunks specified in the initial call.
ADSL	Asynchronous Digital Subscriber Line	
AFB	Asynchronous (File) Bulk Response	Is a message exchange pattern. The initial request is non-blocking and the service consumer gets notified when the transfer is completed.
AFI	Automonic Future Internet	ETSI's pre-standardization body
AKA	also known as	
AN	Asynchronous Notification	Is a message exchange pattern. It facilitates the dissemination of notifications.
ANR	Automatic Neighbourhood Relation	
API	Application Programming Interface	
ARPU	Average Revenue Per User	Commercial KPI used in business plan
ARR	Asynchronous Request/Reply	Is a message exchange pattern. This is a simple response pattern involving a request/reply with a single result message.
ASCII	American Standard Code of Information Interchange	ASCII
ASN.1	Abstract Syntax Notation One	
ASP	Application Service Provider	
ATM	Asynchronous Transfer Mode	ATM technology
B2B	Business-To-Business	
BA	Business Agreement (TM Forum)	Requirements and usage scenario specification.
BBF	Broadband Forum	http://www.broadband-forum.org
BER	Bit Error Ratio	Is the number of bit errors divided by the total number of transferred bits during a studied time interval.
BNG	Broadband Network Gateway	It's an evolution of the existing BRAS the Gatway for Fixed Access Network
BSS	Business Support Systems	Business Support Systems
CAPEX	Capital Expenditures	costs to set up/ change a network
CBE	Common Business Entity	TMF SID term

Abbreviation	Meaning & Terms	Further explanation
CCV	Common Communications Vehicle	A communication infrastructure connecting Operations Systems (e.g., CORBA platform, JMS platform)
CDR	Call Details Records	
CFS	Customer Facing Service	TMF SID term
CFSS	Customer Facing Service Specification	TMF SID term
CI	Configuration Item	ITIL term
close loop	Autonomous Operated SON Function	
CM	Configuration Management	
CMDB	Configuration Management Data Base	ITIL term
CMIP	Common Management Information Protocol	CMIP is a protocol for network management.
CMS	Configuration Management System	ITIL term
CN	Core Network	
CORBA	Common Object Request Broker Architecture	CORBA
CORBA	Common Object Request Broker Architecture	CORBA is a standard defined by the Object Management Group (OMG) that enables software components written in multiple computer languages and running on multiple computers to work together.
COTS	Commercial Off the Shelf	COTS
CPE	Customer Premises Equipment	
CRUD	Create, Read, Update, Delete	
csv	Comma Seperated Value	
CTK	Compliance Test Kit	Part of TM Forum interface specification.
DDP	Document Delivery Package	The MTOSI interface specification is structured in DDPs based on eTOM level 2/3 processes.
DSLAM	Digital Subscriber Line Access Multiplexer	
DT	Deutsche Telekom (Operator)	
e2e	end-to-end	
EM	Element Management	EM
EMS	Element Management System	EMS
eNB	Enhanced NodeB	
EPC	Evolved Packet Core	Mobile Core Network for 4G
eTOM	Enhanced Telecommunication Operations Map	eTOM
ETSI	European Telecommunications Standards Institute (SDO)	
FAB	Fullfillment, Assurance and Billing	
FCAPS	Fault, Configuration, Assurance, Performance	FCAPS
FDD	Feature Description Document	TMF concept
FIM	Federated Information Model	A Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. The Information Model part of these models contains the static data; i.e., the object classes with their attributes and the content of the notifications."

Abbreviation	Meaning & Terms	Further explanation
FM	Fault Management	Fault Management
FMC	Fixed Mobile Convergence	http://en.wikipedia.org/wiki/Fixed-mobile_convergence
FOM	Federated Operations Model	A Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. The Operations Model part of these models contains the dynamics; i.e., operations (and their parameters) grouped in service interfaces which allow the transport of the data defined in the FIM through the management interfaces.
FRU	Field Replaceable Unit	
FT	France Telecom (operator)	
FT IRP	File Transfer Integration Reference Point	
GDMO	Guidelines for the Definition of Managed Objects	GDMO is a specification for defining managed objects of interest to the Telecommunications Management Network for use in CMIP.
GEN	Generic Next Generation Operational Requirements	
GPON	Gigabit-capable Passive Optical Network	
GWCN	Gateway Core Network	A variant of core network sharing model
HLR	Home Location Register	
HO	handover	
HSS	Home Subscribe Server	It's an evolution of the current HLR used as a location server for 2G/3G networks
HTTP	Hyper Text Transfer Protocol	
HW	Hardware	Hardware
IA	Information Agreement (TM Forum)	UML model specification
IDL	Interface Definition Language	OMG IDL
IETF	Internet Engineering Task Force (SDO)	IETF
IIS	Interface Implementation Specification (TM Forum)	Protocol specification; e.g., using XML or CORBA
IM	Information Management	
IMS	IP Multimedia Subsystem	http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem
InvM	Inventory Management	
IP	Internet Protocol	http://en.wikipedia.org/wiki/Internet_Protocol
IPR	Intellectual Property Rights	
IRP	Integration Reference Point (3GPP term)	3GPP 32.103
ISG	Industry Specification Group	ETSI's pre-standardization instrument
ITIL	Information Technology Infrastructure Library	
itSMF	IT Service Management Forum	
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector (SDO)	ITU-T
JMS	Java Message Service	JMS is a Java Message Oriented Middleware API for sending messages between two or more clients.
JPA	Java Persistence API	JPA is a Java programming language framework managing relational data in applications using a Java Platform.
JVT	Java Value Types	

Abbreviation	Meaning & Terms	Further explanation
LCC	Lower Camel Case	An approach to indicate word boundaries using medial capitalization, thus rendering "two words" as "twoWords". This convention is commonly used in Java.
LTE	Long Term Evolution	http://en.wikipedia.org/wiki/3GPP_Long_Term_Evolution
MEF	Metro Ethernet Forum (SDO)	MEF
MEP	Message Exchange Pattern	The combination of a communication pattern and a communication style which fully identifies the messages and the choreography (sequencing and cardinality) of messages through a management interface.
MME	Mobility Management Entity	
MMS	Multimedia Messaging Service	
MO	Managed Object	Managed_object
MOCN	Multi-Operator Core Network	Model of Network sharing which does not share the Core Networks
MOM	Message Oriented Middleware	
MORAN	Multi-Operator Radio Access Network	A model of Network sharing at Radio access level
MPLS	Multi Protocol Label Switching	MPLS
MRI	Manage Resource Inventory	
MSI	Manage Service Inventory	
MT	Modelling and Tooling	Project sub stream of NGCOR
MTNM	Multi Technology Network Management	
MTOSI	Multi Technology OS interface	TM Forum interface product. It is an XML-based Operations System (OS)-to-OS interface suite. The Network Management System-to-Element Management System communication is also covered as a special case.
MVNE	Mobile Virtual Network Environment	
MVNO	Mobile Virtual Network Operator	
MW	Management World	TM Forum event
MW	TM Forum Management World	
NE	Network Element	Network_element
NBI	Northbound Interface	Interface between EMS and NMS
NGCOR	Next Generation Converged Operations Requirements	NGMN project
NGMN	Next Generation Mobile Network	http://www.ngmn.org
NGN	Next Generation Network	http://en.wikipedia.org/wiki/Next_Generation_Networking
NGOSS	Next Generation Operation Systems and Software	
NM	Network Management	Network_management
NMS	Network Management System	Network_management_system
NOC	Network Operation Centre	
NRM	Network Resource Model (3GPP)	Contains the static data of an interface specification.
OA&M	Operation, Administration & Maintanance	OA&M
OC	Operating Committee (NGMN)	

Abbreviation	Meaning & Terms	Further explanation
OCL	Object Constraint Language	OCL is a declarative language for describing rules that apply to Unified Modeling Language (UML) models.
OPE	Operational Efficiency	Requirements specification from NGMN.
OPEX	Operational Expenditures	Costs of running a network
OS&R	Operation, Support and Readiness	Is a Level 1 process grouping of the Business Process Framework. OS&R contains processes for ensuring operational readiness in the fulfillment, assurance and billing areas.
OSA	Open Services Access	
OSS	Operations Support System	Operations_support_system
OSSJ	OSS through Java	
PBB-TE	Provider Backbone Bridges - Traffic Engineering	
PCC	Policy Charging and Control	
PCRF	Policy and Charging Rules Function	It's a functional block in the EPC network architecture for charging & Policy
PDF	Portable Document Format	
PDH	Plesiochronous Digital Hierarchy	
PM	Performance Management	http://en.wikipedia.org/wiki/FCAPS
PT	Portugal Telecom (operator)	
QoS	Quality of Service	QoS
RAM	Resource Alarm Management	Used as an abbreviation for the FM Interface specification workstream of the TMForum
RAN	Radio Access Network	http://en.wikipedia.org/wiki/Radio_access_network
RAT	Radio Access Technology	
RFS	Resource Facing Service	
RFSS	Resource Facing Service Specification	
RI	Reference Implementation	Part of TM Forum interface specification.
Rinv	Resource Inventory	
RM	Resource Mangement	
RM&O	Resource Management & Operations	
RPC	Remote Procedure Call	RPC is an inter-process communication that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction.
SACM	Service Asset and Configuration Management	
SDH	Synchronous Digital Hierarchy	SDH technology
SDO	Standards Developing Organisation	All committes, fora and partnerships that create standards, recommendations and technical reports.
SecM	Security Management	
SFB	Synchronous (File) Bulk Response	Is a message exchange pattern. The service consumer requests a response set to be uploaded to a storage server and the blocking call returns when the transfer is complete.
S-GW	Serving Gateway	

Abbreviation	Meaning & Terms	Further explanation
SI&P	Strategy, Infrastructure & Product	
SID	Shared Information & Data model (TM Forum)	http://www.tmforum.org/InformationFramework/1684/home.html
SIT	Synchronous Iterator	Is a message exchange pattern. This is a multiple response pattern. This is the classical Iterator design pattern. The response of the first invocation returns a partial data set as well as a pointer to an Iterator interface. The service consumer will then invoke the Iterator to receive the subsequent result data set partitions. The consumer has control of the flow, the service provider needs to maintain the state related to the pending Iterator.
SLA	Service Level Agreement	KPI describing user requirements tro be translated into QOS objective at operator side within an agreement
SM	Security Management	http://en.wikipedia.org/wiki/FCAPS
SM&O	Service Management &Operations	
SN	Synchronous Notification	Is a message exchange pattern. It facilitates the dissemination of notifications.
SNMP	Simple Network Management Protocol	SNMP is an "Internet-standard protocol for managing devices on IP networks"
SOA	Service Oriented Architecture	Service-oriented_architecture
SOAP	Simple Object Access Protocol	
SON	Self Organizing Network	
SONET	Synchronous Optical Network	SONET
SP	Service Provider	Company, which provides access to telephone and related communications services
SPR	Subscription Profile Repository	It's a data base for user profiles
SQM	Service Quality Management	eTOM definition: "SQM encompasses monitoring, analyzing and controlling the performance of the service perceived by customers"
SRR	Synchronous Request/Reply	Is a message exchange pattern. This is a simple response pattern involving a request/reply with a single result message.
SuM	Subscription Management	
SW	Software	Software
TA	Tracking Area	
TAM	Telecom Appplications Map	TMF term
TMF	TM Forum	www.tmforum.org
TWG SC	Technical Working Group Steering Committee	NGMN group
UCC	Upper Camel Case	An approach to indicate word boundaries using medial capitalization, thus rendering "two words" as "TwoWords". This convention is commonly used in Java.
UDC	User Data Convergence	Evolution of unified data bases
UE	User Equipment	
UML	Unified Modelling Language	UML
UMTS	Universal Mobile Telecommunication System	UMTS
USIM	Universal Subscriber Identity Module	
VF	Vodafone (operator)	

Abbreviation	Meaning & Terms	Further explanation
WDM	Wavelength Division Multiplexing	WDM
WiMax	Worldwide Interoperability for Microwave Access	WiMAX
WLAN	Wireless Local Area Network	WLAN
WS	Web Service	Web Services
WSDL	Web Service Description Language	WSDL
XMI	XML Metadata Interchange	http://en.wikipedia.org/wiki/XMI
XML	Extensible Markup Language	XML
Xpath	XML Path Language	XPATH is a query language for selecting nodes from an XML document.
XSD	XML Schema	XSD
	alarm interface	An interface which transports alarm - informations between OSS systems
	Business Services	These are the operations in TM Forum terminology.
	Business Use Case	High level uses case driven by a business scenario.
	common architecture	All interfaces should be part of a common architecture
	Common Core Network	Business architecture Scenario
	Common Information Model	This term is used to reference information models like TMForum SID
	Communication Partners	OSS systems, which exchange information
	Converged Framework Model	Harmonised design guidelines for tooling.
	cross-domain	Cross mobile and fixed domains
	cross-domain	Cross mobile and fixed domains
	Domain	Related to the partioning of the network
	Dynamic Requirement	Requirements which describe the operations part of the management interface.
	Element Management Layer	EMS level in layering architecture
	Element Manager	Element Manager
	EMS (server)	The SW component which implements the interface in the OSS systems, which delivers a service to other OSS systems
	EMS-OSS layer	Summary of all OSS systems which deliver an EMS functionality
	eNodeB	Base Station for LTE
	entity	An entity is some tangible or conceptual thing , entity word is typically used when presenting things without a real name name or label. Entities are characterized by attributes and relationships.
	EPC Network	Mobile Core Network for 4G
	federated information / data model	See sub-task MT
	Federated Model	see Operations Model
	Federated Network Resource Model	see Operations Model
	femtoCell	Home NodeBB (Base Station deployed in the Home)
	implementation technology	Technology used to implement a functionality
	Infrastructure Domain	

Abbreviation	Meaning & Terms	Further explanation
	Interfacing / Integration	
	inventory component	An instance of the objects in an inventory database
	logical resource	Logical resources are e.g., subnetwork connection, topological link, termination point etc..
	management architecture	Defines the architecture between Operations Systems and the between Operations Systems and the network.
	management area	These are e.g., alarm management, inventory, performance management etc..
	Management Interface	An instance of an interface between two OSes used for management.
	Management Model	Generic term for information model and operations model.
	management operation	Operations executed via the management interface.
	management recommendations	ITU-T standards are called Recommendations.
	management workflows	Specific sequence of operations executed via the management interface.
	multi-domain network	Domains are e.g., access, metro, backhaul, core.
	multi-technology network	Technologies are e.g., ATM, OTN, SDH, Ethernet, DSL, LTE, 2G, 3G, HSPA.
	Network Abstraction Layer	A logical layer between the network and the management layer which relay an abstracted view (from management point of view) of the network.
	network data	Data which describes - from management point of view - the underlying network in an abstract way. This data can be used by all different management areas.
	Network Level Interface	An interface which is able to provide an end-to-end view of the underlying network.
	network level management	A management function which is able to manage an end-to-end view of the underlying network.
	Network Operator	Company, which provides access to telephone and related communications services
	Network Resource Model	Data model representing the equipment of a network. It's 3GPP terminology
	network technology	For Mobile , it means 2G, 3G or 4G
	network type	The type of the network (e.g. UMTS- Radio, DWH, IP, etc. ..)
	NGOSS concepts	Concepts (like eTOM, SID, etc…) which are summarized within the "Next Generation Operation Support Systems" - concept of the TMForum
	NMS (client)	The SW component which implements the interface in the OSS systems, which requests a service from another OSS system.
	OA&M functional domain	It refers to ITU-T "FCAPS"
	open loop	Operator controlled SON function
	Operations Model	Contains the dynamic part of the model; i.e., operations (and their parameters) grouped in service interfaces which allow the transport of the data defined in the information model through the management interfaces.
	Operator	Role, responsible for the management of a network and/or service
	operator-wide OSS application	Applications developed by the operator to ensure FM, PM, CM,

Abbreviation	Meaning & Terms	Further explanation
	OSS application	An application which delivers a capability dedicated to the OSS domain
	OSS environment	
	OSS Interface	Interface between OSS systems
	physical resource	Physical resources are e.g., network elements, cables, fibres etc..
	primitive	Simplest element provided by a programming language
	resource	Resource is any physical or virtual component of a telecommunications network
	Resource Configuration Management	TMForum TAM definition: "The Resource Configuration Management application generates a resource plan to fulfill a resource order."
	Resource Fault Management	TMForum TAM definition: "Fault Management applications are responsible for the management of faults, or troubles, associated with the service provider's resources. "
	resource management layer	Covers all Resource Management processes as defined in the TM Forum Business Process Framework (eTOM) "Resource Management & Operations" (RM&O) layer within the operations & support, fulfillment, and assurance verticals. This process grouping maintains knowledge of resources (application, computing and network infrastructures) and is responsible for managing all these resources.(e.g. networks, IT systems, servers, routers, etc.) utilized to deliver and support services required by customers.
	service catalogue	Storage of all service specifications and instances
	service configuration and activitation	Operator process dealing with delivery
	Service Inventory	TMForum TAM definition: Service Inventory represents the applications which contain and maintain information about the instances of services in a telecom organization
	service management layer	Covers all Service Management processes as defined in the TM Forum Business Process Framework (eTOM) "Service Management & Operations" (SM&O) layer within the operations & support, fulfilment, and assurance verticals. This process grouping focuses on the knowledge of services (Access, Connectivity, Content, etc.) and includes all functionalities necessary for the management and operations of communications and information services required by customers.
	service platform	A resource, which delivers a telecommunication service
	service type	The type of a service (e.g. MMS or SMS - Service)
	shared network	Generic term which includes different model sharing (at core, access network)
	type acceptance	Type Acceptance is the process of verifying that a certain product has passed performance tests and quality assurance tests or qualification requirements stipulated in contracts, regulations, or specifications.
	Umbrella Model	Part of the model containing artefacts that can be used/inherited in both wireline and wireless network models.
	Usage Scenario	TMF term for "use case"; are defined for each required operation
	Use Case	It refers to Business architecture scenarios and Generic & Basic architecture scenarios

8.2 The NGCOR Requirements and their Addressees

The following chapters summarize the requirements that have been elaborated and collected per substream of the NGCOR project and show the addressees of these requirements.

8.2.1 Generic Requirements

GEN	Addressee / Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-GEN (1)	X	X	X
REQ-GEN (2)	X		
REQ-GEN (3)	X		
REQ-GEN (4)	X		
REQ-GEN (5)	X		
REQ-GEN (6)	X		
REQ-GEN (7)	X		
REQ-GEN (8)	X		
REQ-GEN (9)	X		
REQ-GEN (10)	X		
REQ-GEN (11)	X		
REQ-GEN (12)	X		
REQ-GEN (13)	X		
REQ-GEN (14)	X		
REQ-GEN (15)	X		
REQ-GEN (16)	X	X	X
REQ-GEN (17)	X	X	X
REQ-GEN (18)	X		
REQ-GEN (19)	X		
REQ-GEN (20)	X	X	X
REQ-GEN (21)	X	X	
REQ-GEN (22)	X		

Table 5: Generic Requirements - Whom these requirements are addressed to

8.2.2 CON Requirements

CON	Addressee / Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CON (1)	X	X	
REQ-CON (2)	X	X	
REQ-CON (3)	X	X	
REQ-CON (4)	X	X	
REQ-CON (5)	X	X	
REQ-CON (6)			X
REQ-CON (7)	X		
REQ-CON (8)			X
REQ-CON (9)	X		
REC-CON (10)	X		

Table 6: Converged Operations Requirements - Whom these requirements are addressed to

8.2.3 MT Requirements

MT	Addressee/ Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-MT (1)	X		
REQ-MT (2)	X		
REQ-MT (3)	X		
REQ-MT (4)	X		
REQ-MT (5)	X		
REQ-MT (6)	X		
REQ-MT (7)	X		
REQ-MT (8)	X		
REQ-MT (9)	X		
REQ-MT (10)	X	X	X
REQ-MT (11)	X		
REQ-MT (12)	X		
REQ-MT (13)	X		
REQ-MT (14)	X		
REQ-MT (15)	X	X	X
REQ-MT (16)	X		
REQ-MT (17)	X		
REQ-MT (18)	X		
REQ-MT (19)	X		
REQ-MT (20)	X		
REQ-MT (21)	X		
REQ-MT (22)	X		

MT	Addressee/ Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-MT (23)	X		
REQ-MT (24)	X		
REQ-MT (25)	X		
REQ-MT (26)	X		
REQ-MT (27)	X		
REQ-MT (28)	X		
REQ-MT (29)	X		
REQ-MT (30)	X		
REQ-MT (31)	X		
REQ-MT (32)	X		
REQ-MT (33)	X		
REQ-MT (34)	X		
REQ-MT (35)	X		
REQ-MT (36)	X		
REQ-MT (37)	X		
REQ-MT (38)	X		
REQ-MT (39)	X		
REQ-MT (40)	X		
REQ-MT (41)	X	X	X
REQ-MT (42)	X	X	X
REQ-MT (43)	X		
REQ-MT (44)	X		
REQ-MT (45)	X	X	X
REQ-MT (46)	X		
REQ-MT (47)	X		
REQ-MT (48)	X		
REQ-MT (49)	X		
REQ-MT (50)	X		
REQ-MT (51)	X		
REQ-MT (52)	X	X	X
REQ-MT (53)	X		
REQ-MT (54)	X		
REQ-MT (55)	X		
REQ-MT (56)	X		
REQ-MT (57)	X		
REQ-MT (58)	X		
REQ-MT (59)	X		
REQ-MT (60)	X		
REQ-MT (61)	X		
REQ-MT (62)	X		
REQ-MT (63)	X		
REQ-MT (64)	X		
REQ-MT (65)	X		
REQ-MT (66)	X		
REQ-MT (67)	X		
REQ-MT (68)	X		

MT	Addressee/ Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-MT (69)	X		
REQ-MT (70)	X		
REQ-MT (71)	X		
REQ-MT (72)	X		
REQ-MT (73)	X		
REQ-MT (74)	X		
REQ-MT (75)	X		
REQ-MT (76)	X		
REQ-MT (77)	X		
REQ-MT (78)	X		
REQ-MT (79)	X		
REQ-MT (80)	X		
REQ-MT (81)	X	X	X
REQ-MT (82)	X	X	X
REQ-MT (83)	X	X	X
REQ-MT (84)	X	X	X
REQ-MT (85)	X	X	X
REQ-MT (86)	X	X	X
REQ-MT (87)	X	X	X
REQ-MT (88)	X	X	X
REQ-MT (89)	X	X	X
REQ-MT (90)	X	X	X
REQ-MT (91)	X	X	X
REQ-MT (92)	X	X	X
REQ-MT (93)	X	X	X
REQ-MT (94)	X	X	X
REQ-MT (95)	X	X	X
REQ-MT (96)	X	X	X
REQ-MT (97)	X	X	X
REQ-MT (98)	X	X	X
REQ-MT (99)	X	X	X
REQ-MT (100)	X	X	X
REQ-MT (101)	X	X	X
REQ-MT (102)	X	X	X
REQ-MT (103)	X	X	X
REQ-MT (104)	X	X	X
REQ-MT (105)	X	X	X
REQ-MT (106)	X	X	X
REQ-MT (107)	X	X	X
REQ-MT (108)	X	X	X
REQ-MT (109)	X	X	X
REQ-MT (110)	X	X	X

Table 7: Modelling & Tooling Requirements - Whom these requirements are addressed to

8.2.4 FM Requirements

FM	Addressee/ Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-FM (1)	X		
REQ-FM (2)	X		
REQ-FM (3)	X		
REQ-FM (4)	X		
REQ-FM (5)	X		
REQ-FM (6)	X		
REQ-FM (7)	X	X	
REQ-FM (8)	X		X
REQ-FM (9)	X	X	X
REQ-FM (10)	X	X	
REQ-FM (11)	X	X	X
REQ-FM (12)	X	X	
REQ-FM (13)	X		X

Table 8: Fault Management Requirements - Whom these requirements are addressed to

8.2.5 InvM Requirements

InvM	Addressee / Receiver of Requirement		
	SDOs & Organsations	Equipment Vendors	OSS Vendors
REQ-InvM (1)			X
REQ-InvM (2)			X
REQ-InvM (3)			X
REQ-InvM (4)			X
REQ-InvM (5)			X
REQ-InvM (6)			X
REQ-InvM (7)			X
REQ-InvM (8)			X
REQ-InvM (9)			X
REQ-InvM (10)	X	X	X
REQ-InvM (11)	X	X	X
REQ-InvM (12)	X		X
REQ-InvM (13)	X		X
REQ-InvM (14)	X		X
REQ-InvM (15)			X
REQ-InvM (16)	X		X
REQ-InvM (17)	X		X
REQ-InvM (18)	X		X
REQ-InvM (19)	X		X
REQ-InvM (20)	X		X
REQ-InvM (21)	X	X	X
REQ-InvM (22)	X		X

REQ-InvM (23)	X		X
REQ-InvM (24)	X		X
REQ-InvM (25)	X		X
REQ-InvM (26)	X		X
REQ-InvM (27)	X		X
REQ-InvM (28)	X		X
REQ-InvM (29)	X		X
REQ-InvM (30)	X		X
REQ-InvM (31)	X		X
REQ-InvM (32)	X		X
REQ-InvM (33)	X		X
REQ-InvM (34)			X
REQ-InvM (35)			X
REQ-InvM (36)			X
REQ-InvM (37)	X		X
REQ-InvM (38)	X	X	X
REQ-InvM (39)	X		X
REQ-InvM (40)		X	X
REQ-InvM (41)			X
REQ-InvM (42)	X		X
REQ-InvM (43)			X
REQ-InvM (44)			X
REQ-InvM (45)			X
REQ-InvM (46)			X
REQ-InvM (47)	X		X
REQ-InvM (48)	X		X
REQ-InvM (49)			X
REQ-InvM (50)	X		X
REQ-InvM (51)	X		X
REQ-InvM (52)	X		X
REQ-InvM (53)			X
REQ-InvM (54)			X
REQ-InvM (55)	X	X	X
REQ-InvM (56)	X	X	X
REQ-InvM (57)	X	X	X
REQ-InvM (58)	X		X
REQ-InvM (59)	X		X
REQ-InvM (60)			X
REQ-InvM (61)			X
REQ-InvM (62)			X
REQ-InvM (63)	X		X
REQ-InvM (64)	X		X
REQ-InvM (65)			X
REQ-InvM (66)			X
REQ-InvM (67)			X
REQ-InvM (68)			X
REQ-InvM (69)		X	X

Table 9: Inventory Management Requirements - Whom these requirements are addressed to