Maintenance, Protection & Alarm Control Business Agreement

TMF_MPAC_BA

TM Forum Approved Version 1.2

September, 2011

Notice

This material, including documents, code and models, has been through review cycles; however, due to the inherent complexity in the design and implementation of software and systems, no liability is accepted for any errors or omissions or for consequences of any use made of this material.

Under no circumstances will the TM Forum be liable for direct or indirect damages or any costs or losses resulting from the use of this specification. The risk of designing and implementing products in accordance with this specification is borne solely by the user of this specification.

Direct inquiries to the TM Forum office:

240 Headquarters Plaza,
East Tower – 10th Floor,
Morristown, NJ 07960 USA
Tel No. +1 973 944 5100
Fax No. +1 973 944 5110
TM Forum Web Page: www.tmforum.org

Table of Contents

List of Requirements

List of Use Cases

List of Figures

Executive Summary

Harmonization work has been done on Alarm Management within TM Forum between OSS/J Fault Management API and MTOSI Resource Trouble Management DDP leading to the definition of the Resource Alarm Management (RAM) interface. For a true harmonization, it is needed to be able to phase out existing Fault Management interfaces from OSS/J and MTOSI when introducing the new one to avoid creating yet another FM interface.

During the initial migration discussions it was noted that the scope of MTOSI Resource Trouble Management DDP is slightly larger than the scope of RAM, which is only covering the Alarm Collection and Handling parts of RTM.

In order to complete the coverage of MTOSI RTM DDP and ease the migration to RAM, the missing pieces of RTM have been gathered in the Maintenance, Protection and Alarm Control (MPAC) interface.

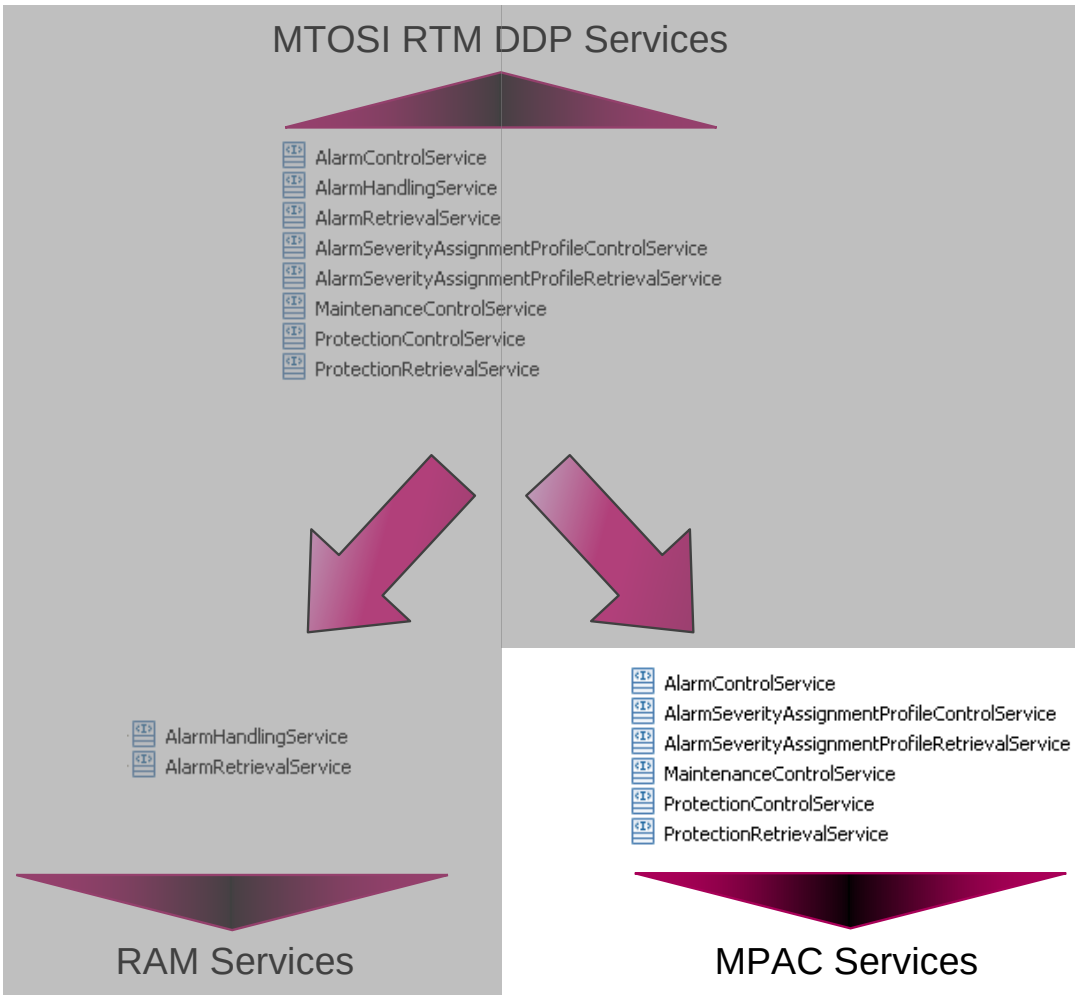

Figure 1 MPAC Scope

1 Introduction

1.1 Overview

This interface covers Maintenance, Protection, Alarm Control and Alarm Severity Assignment Profile (ASAP).

These services, as indicated in the Executive Summary, are the pieces of RTM that are not present in the Resource Alarm Management interface.

The sum of the MPAC and the RAM interfaces should allow phasing out the MTOSI RTM DDP.

It is not the goal of this interface to harmonize or enhance these services, but simply to migrate them to the TIP tooling and ecosystem.

Note that TIP interfaces do not separate objects and operations in separate kits (DDPs) while MTOSI does, so while operations related to this interface are coming from MTOSI RTM DDP, the corresponding data objects are coming from MTOSI NRA DDP.

Requirements in this document are directly coming from TMF518_NRA for the static and structural requirements and from TMF518_RTM for the dynamic requirements.

Use cases are coming from TMF518_RTM.

Traceability back to the corresponding TMF518_NRA or TMF518_RTM requirement or use case is indicated each time.

1.2 Interface Scope

The scope of this project concerns requirements, use cases, information model and a detailed interface specification for the Maintenance, Protection and Alarm Control.

The scope covers the following MTOSI Service Interfaces, which are part of the MTOSI RTM DDP:

- Alarm Control
- ASAP Control
- ASAP Retrieval
- Maintenance Control
- Protection Control
- Protection Retrieval

1.3 Document Structure

The following sections are contained in this document:

- Section 1 is the document introduction

- Section 2 defines the business problem description and supported scenarios
- Section 3 covers the project scope and the relationship to other TMF activities
- Section 4 includes all the requirements by category
- Section 5 defines the use cases
- Section 6 traceability matrices between use cases and requirements
- Section 7 outlines future directions
- Section 8 lists references and any Intellectual Property Right (IPR) claims
- Section 9 contacts, acknowledgements and other administrative items

1.4 Terminology Used In This Document

2 Business Problem Description

2.1 Problem Statement

This interface covers Maintenance, Protection, Alarm Control and ASAP.

These functionalities are part of the MTOSI Resource Trouble Management DDP and are needed to be able to migrate the MTOSI RTM DDP to TIP.

2.2 Benefits

The following table summarizes the key elements of this specification and the associated benefits:

Key Element	Benefit
MPAC requirements and use cases	Can be used to service providers in their RFP and RFIs Used (internal to this project) to drive the Information Agreement (IA) and Interface Implementation Specification (IIS) work.
SID extensions for ASAP and protection management	Linkage to the comprehensive SID model, allowing service providers to build on their existing SID information models in the area of MPAC
MPAC interface	Can be used by OSS suppliers to provide interoperable resource alarm management products Provide guidelines for Service Providers and vendors to adhere to Closer integration between NMSs and with other OSS/BSS systems Cost benefits of standardized and harmonized interfaces Provide in conjunction with the RAM interface a migration path for users of MTOSI RTM interface

3 Relationship to other TMF Groups

3.1.1 Business Process Framework (eTOM)

As the MTOSI DDP are organized by eTOM processes, this interface covers sub-parts of the eTOM level 2 process Resource Trouble Management as described in GB921_D.

It is important to emphasize that the eTOM defines processes and this document covers interfaces. So, the explanation that follows will indicate which of the eTOM processes has interface implications on the interface at hand.

Interface implications for the various eTOM level 3 processes within Resource Trouble Management (RTM) are as follows:

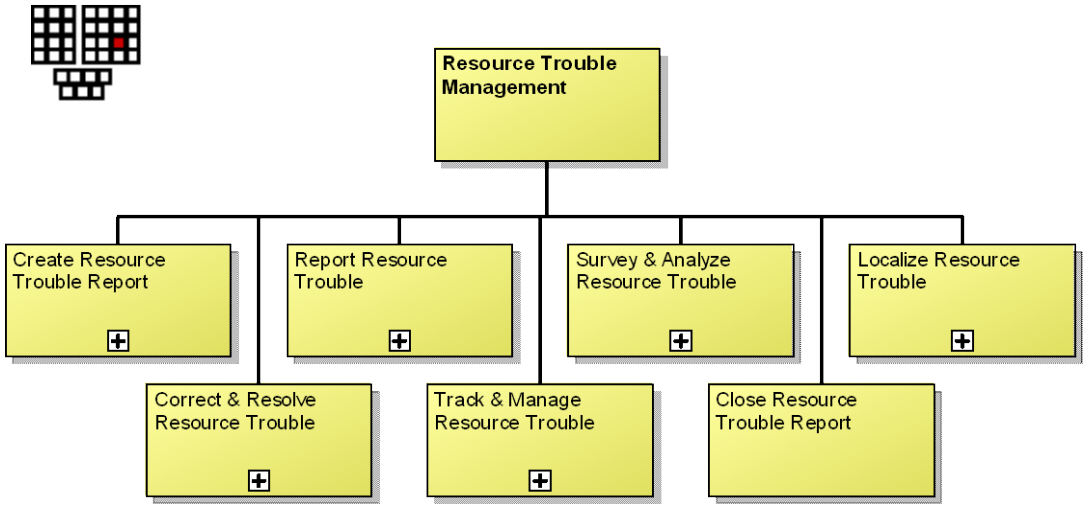

Figure 2 Resource Trouble Management decomposition into level 3 processes

- Create Resource Trouble Report – The Alarm Control and ASAP Control interfaces are related to this process, used on the EMS or on the NE to decide to generate or not an alarm and assign its severity. These interfaces might be called to initiate the generation of alarms from the NE. The ASAP Retrieval interfaces might be used as an ancillary process here.
- Report Resource Trouble – This process appears to be out of scope for the MPAC interface.
- Survey & Analyze Resource Trouble – This process might trigger calls to Maintenance Control, Protection Control or Retrieval as part of the analysis process.
- Localize Resource Trouble – This process might trigger calls to Maintenance Control or Protection Retrieval as part of the analysis process.
- Correct & Resolve Resource Trouble – The Maintenance Control and Protection Control are related to this process as the resolution of the resource trouble might imply using these interfaces.
- Track & Manage Resource Trouble – This process might trigger calls to Maintenance Control, Protection Control or Retrieval as part of the tracking process.

- Close Resource Trouble Report – This process appears to be out of scope for the MPAC interface.

It is worth noting that the addition of RAM and MPAC covers all RTM level 3 processes.

3.1.2 Information Framework (SID)

All the data objects of a TIP interface are part of the SID. Only ASAP and Protection Management have data objects. It is proposed to create an Alarm Severity Assignment Profile ABE and a Protection ABE.

The Alarm Severity Assignment Profile ABE will be a sub-ABE of the Resource Trouble ABE, under the Resource Domain. An ABE is an Aggregate Business Entity, which is the SID term for a logical and coherent grouping of objects. ABEs are used in the SID to structure information.

The Protection ABE will be a sub-ABE of the Logical Resource ABE, as the Protection Group and Equipment Protection Group will be logical resources. So it is natural to put this ABE under the Logical Resource ABE.

As part of the resource harmonization between MTOSI and SID, the NRF DDP was moved to the SID as the NRF ABE (under Logical Resource ABE/ TIP Logical Resource ABE). NRF is using some objects from NRA, so an NRA ABE has been created under Resource ABE/ TIP Resource ABE. This NRA ABE does not contain all NRA objects, but only the ones needed for NRF. The 2 artifacts related to MPAC present in NRA ABE identified today are the AlarmSeverityAssignmentProfile object class and the ProtectionSchemeState datatype. These artifacts would be moved to the corresponding sub-ABEs.

3.1.3 Application Framework (TAM)

In terms of the TAM 4.0, the interface fits the “Resource Domain Management Applications” area in the Resource Management Domain (see Figure 1).

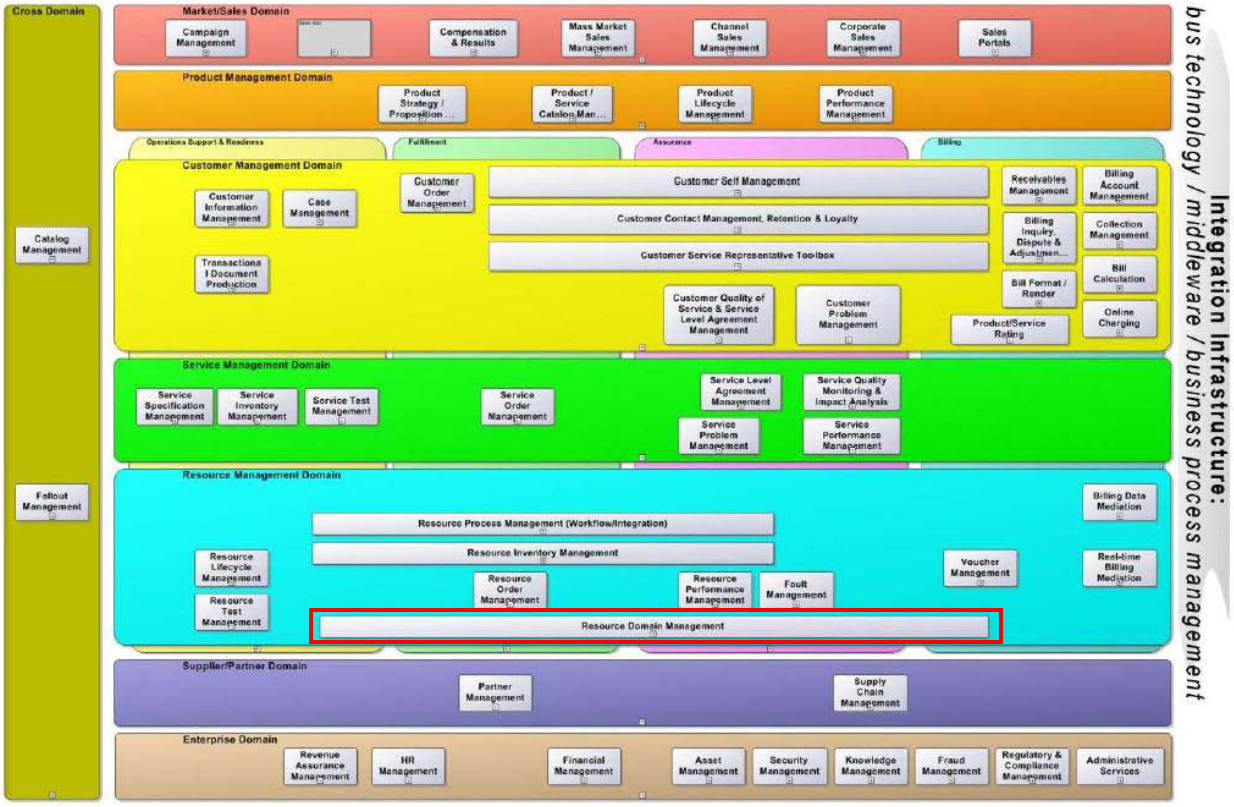

Figure 3 Telecom Application Map (TAM)

The following item from the TAM Resource Domain Management Applications area (see Figure 4) is to be covered:

- Resource Fault Mediation

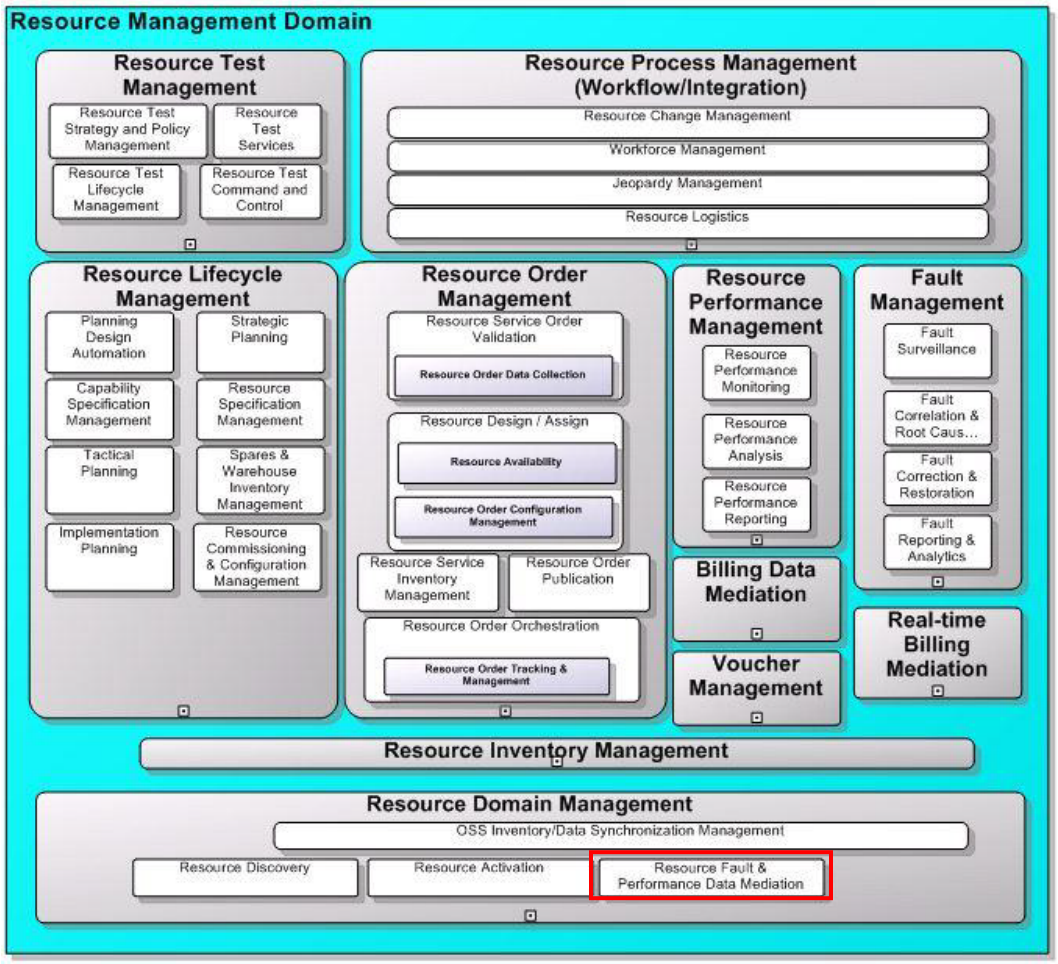

Figure 4 Telecom Application Map (TAM) Resource Management Domain

3.1.4 Relationship to other TMF Groups

This interface is made to ease the migration from MTOSI RTM DDP to the TIP tooling and ecosystem.

The sum of this interface (MPAC) and of the RAM interface should completely replace the MTOSI RTM DDP.

For the NRA interface, the replacement is only partial as NRA also included objects related to Performance Management.

The introduction of MPAC should phase out the following object classes from the MTOSI NRA DDP:

- AlarmSeverityAlignmentProfile
- EquipmentProtectionGroup
- ProtectionGroup
- EquipmentProtectionSwitchNotification
- ProtectionSwitchNotification

Note as a reminder that the introduction of the RAM interface should phase out the following MTOSI NRA notifications:

- AlarmNotification
- TCANotification

4 Requirements

4.1 Business Requirements

R_TMF_MPAC_BA_BR_0001	**Control of Alarm Reporting** The Interface shall support the control of alarm reporting in terms of activating and deactivating alarm reporting for a given managed entity or a specified set of managed entities.
Source	TMF518_RTM, R_TMF518_RTM_BR_0002

R_TMF_MPAC_BA_BR_0002	**Retrieval of protection information** The Interface shall support the retrieval of protection information such as protection groups and the reporting of protection events.
Source	TMF518_RTM, R_TMF518_RTM_BR_0004

R_TMF_MPAC_BA_BR_0003	**Perform protection commands** The Interface shall support requests to perform protection switch commands.
Source	TMF518_RTM, R_TMF518_RTM_BR_0005

R_TMF_MPAC_BA_BR_0004	**Perform maintenance commands** The interface shall support requests for maintenance and diagnostic tests.
Source	TMF518_RTM, R_TMF518_RTM_BR_0006

4.2 Category I: Static and Structural Requirements

4.2.1 Alarm Severity Assignment Profile (ASAP) Management

R_TMF_MPAC_BA_I_0005	**Alarm Severity Assignment Profile (ASAP)** The ***Alarm Severity Assignment Profile (ASAP)*** object shall represent a set of severities that can be assigned to specific alarm probable causes.

	An ***ASAP*** is contained within an OS.
Source	TMF518_NRA, R_TMF_NRA_I_0001

R_TMF_MPAC_BA_I_0006	**Alarm Severity Assignment Profile (ASAP) Attributes** An ***ASAP*** object shall have, in addition to the attributes identified in requirement R_TMF_MPAC_BA_I_0005, the following attributes: • ***fixed*** - this attribute shall indicate whether the ***ASAP*** is modifiable by an OS. If not, the ***ASAP*** can be neither modified nor deleted by an OS, but only assigned/de-assigned. • ***alarm severity assignment list*** - this attribute shall represent a list of Alarm Severity Assignments (ASA) as defined in R_TMF_MPAC_BA_I_0007.
Source	TMF518_NRA, R_TMF_NRA_I_0002

R_TMF_MPAC_BA_I_0007	**Alarm Severity Assignment (ASA)** The ***Alarm Severity Assignment (ASA)*** object shall represent the specific severities for the various service affecting conditions that are to be assigned to a specific alarm probable cause. An ***ASA*** has the following attributes: • ***probable cause*** - this attribute shall represent the name of a specific probable cause to which the severities are to be assigned. • ***specific problems*** - this attribute shall represent the specific problems and shall be present if the probable cause attribute is not sufficient to uniquely identify an alarm. OPTIONAL • ***service affecting severity*** - this attribute shall represent the value to be assigned in the case where the reportable alarm is service affecting. • ***non-service affecting severity*** - this attribute shall represent the severity value to be assigned in the case where the reportable alarm is non-service affecting. • ***service independent severity*** - this attribute shall represent the severity value to be assigned in the case where the reportable alarm is service independent. This severity value may also be assigned in the case where the reporting OS is unable to determine whether the alarm is service affecting or not.
Source	TMF518_NRA, R_TMF_NRA_I_0003

4.2.2 Protection Management

4.2.2.1 Equipment Protection Group (EPG)

R_TMF_MPAC_BA_I_0008	**Equipment Protection Group (EPG)** The ***Equipment Protection Group (EPG)*** object shall represent Equipment protection.
Source	TMF518_NRA, R_TMF_NRA_I_0007

R_TMF_MPAC_BA_I_0009	**Equipment Protection Group (EPG) Attributes** An ***EPG*** object shall have the following attributes: • ***protection type*** - this attribute shall represent the type of the ***EPG*** (e.g. M:N). • ***protection scheme state*** -this attribute shall indicate the current state of the protection scheme (i.e. whether it is active or locked). • ***reversion mode*** - this attribute shall indicate whether the protection scheme is revertive or not. • ***protected equipment list*** - these attribute shall represent a list of the protected Equipment instances. • ***protecting equipment list*** - this attribute shall represent a list of the protecting Equipment instances. • ***pg parameter list*** - this attribute shall represent the ***EPG*** specific parameters. For example SwitchMode, SwitchPosition, wait to restore time, etc. • ***alarm severity assignment profile*** - this attribute shall represent the name of the Alarm Severity Assignment Profile (ASAP) that has been assigned to the ***EPG***.
Source	TMF518_NRA, R_TMF_NRA_I_0008

4.2.2.2 Protection Group

R_TMF_MPAC_BA_I_0010	**Protection Group (PG)** The ***Protection Group (PG)*** object shall represent trail protection schemes.
Source	TMF518_NRA, R_TMF_NRA_I_0009

R_TMF_MPAC_BA_I_0011	**Protection Group (PG) Attributes** A ***PG*** object shall have the following attributes: • ***type*** - this attribute shall represent the type of the ***PG***. • ***protection scheme state*** - this attribute shall indicate the current state of the protection scheme (i.e. whether

	it is active or locked). • ***reversion mode*** - this attribute shall indicate whether the protection scheme is revertive or not. • ***layer rate*** - refer to requirement R_TMF518_NRB_I_0003. • ***protection related PTP list*** - this attribute shall represent a list of the Physical Termination Points (PTP) related by the ***PG***. • ***pg parameter list*** - this attribute shall represent the ***PG*** specific parameters (e.g. switch mode, switch position, wait to restore time, etc.). • ***aps protocol type*** - this attribute shall indicate the type of APS protocol supported by the ***PG***. • ***alarm severity assignment profile*** - this attribute shall represent the name of the Alarm Severity Assignment Profile (ASAP) that has been assigned to the ***PG***.
Source	TMF518_NRA, R_TMF_NRA_I_0010

4.2.2.3 Protection Notifications

R_TMF_MPAC_BA_I_0043	**Protection Switch Notification Attributes** A ***Protection Switch Notification*** is an event used across the Interface to indicate that a protection switch has occurred. A ***Protection Switch Notification*** shall have the following specific attributes: • ***protection type*** – this attribute shall represent the type of the protection for which the switch has occurred. • ***switch reason*** – this attribute shall represent the reason for the switch. • ***layer rate*** – this attribute shall represent the layer at which the switch has occurred. • ***protection group*** – this attribute shall represent the name of the Protection Group (PG) in the case of a trail switch. Not used if the protection type is Subnetwork Connection Protection (SNCP). • ***protected TP*** – this attribute shall represent the name of the Termination Point (TP) being protected. • ***switch away from TP*** – this attribute shall represent the name of the TP being switched away from. • ***switch to TP*** – this attribute shall represent the name of the TP that is switched to.
Source	TMF518_NRA, R_TMF_NRA_I_0027

R_TMF_MPAC_BA_I_0044	**Equipment Protection Switch Notification Attributes** An ***Equipment Protection Switch Notification*** is an event used across the Interface to indicate that an equipment protection switch has occurred. An ***Equipment Protection Switch Notification*** shall have the following specific attributes: • ***protection type*** – this attribute shall represent the type of the protection for which the switch has occurred. • ***switch reason*** – this attribute shall represent the reason for the switch. • ***equipment protection group*** – this attribute shall represent the name of the Equipment Protection Group (EPG). • ***protected equipment*** – this attribute shall represent the name of the Equipment being protected. • ***switch away from equipment*** – this attribute shall represent the name of the Equipment being switched away from. • ***switch to equipment*** – this attribute shall represent the name of the Equipment that is switched to.
Source	TMF518_NRA, R_TMF_NRA_I_0028

4.3 Category II: Normal Sequences, Dynamic Requirements

4.3.1 Control of Alarm Reporting

R_TMF_MPAC_BA_II_0012	**Activation of Alarm Reporting** The Interface shall allow the requesting OS to activate (allow, or turn on) alarm reporting for a particular Termination Point (TP). Alarm reporting for the TP is to be turned "on" at the specific layerRate provided by the requesting OS. However, setting of this parameter is best-effort. If the target OS does not support this granularity, it is acceptable for the target OS to turn on or off alarm reporting for all the layers of the TP regardless of the layerRate specified by the requesting OS. It is also acceptable for the target OS to turn on or off alarm reporting for the contained CTPs, if the ME does not support finer granularity.
Source	TMF518_RTM, R_TMF518_RTM_II_0012

R_TMF_MPAC_BA_II_0013	**Deactivation of Alarm Reporting** The Interface shall allow the requesting OS to deactivate (inhibit, or turn off) alarm reporting for a particular Termination Point (TP). Alarm reporting is to be turned "off" at the layer represented by the Termination Point (TP). See also the exceptions to this rule noted inR_TMF_MPAC_BA_II_0012.
Source	TMF518_RTM, R_TMF518_RTM_II_0013

In order to provide SNC alarm reports, the reporting OS has to correlate TP related information into "arc" related information. Note: How to provide this correlation is behavior of the reporting OS and is therefore outside the scope of the Interface. The activation / de-activation do not imply anything on the alarm reporting flag of any of the related TPs of the SNC / topological link. The requesting OS shall be able to retrieve the status of the activation / de-activation.

R_TMF_MPAC_BA_II_0014	**Activation of Alarm Reporting for a specific Object** The Interface shall allow the requesting OS to activate (allow, or turn on) alarm reporting for a particular Equipment, Equipment Holder, Equipment Protection Group, Flow Domain, Flow Domain Fragment, Group Termination Point, Managed Element, Matrix Flow Domain, Multi-Layer Subnetwork, OS, Protection Group, Subnetwork Connection (SNC) and Topological Link.
Source	TMF518_RTM, R_TMF518_RTM_II_0014

R_TMF_MPAC_BA_II_0015	**Deactivation of Alarm Reporting for a specific Object** The Interface shall allow the requesting OS to de-activate (inhibit, or turn off) alarm reporting for a particular Equipment, Equipment Holder, Equipment Protection Group, Flow Domain, Flow Domain Fragment, Group Termination Point, Managed Element, Matrix Flow Domain, Multi-Layer Subnetwork, OS, Protection Group, Subnetwork Connection (SNC) and Topological Link.
Source	TMF518_RTM, R_TMF518_RTM_II_0015

4.3.2 Alarm Severity Assignment Profile (ASAP) Management

R_TMF_MPAC_BA_II_0016	**Retrieving all ASAPs for a given OS** The Interface shall allow the requesting OS to retrieve the attributes of all the Alarm Severity Assignment Profiles (ASAPs) that are being managed by the target OS.
Source	TMF518_RTM, R_TMF518_RTM_II_0007

R_TMF_MPAC_BA_II_0017	**Retrieving a given ASAP** The Interface shall allow the requesting OS to retrieve the attributes of a given Alarm Severity Assignment Profile (ASAP).
Source	TMF518_RTM, R_TMF518_RTM_II_0009

R_TMF_MPAC_BA_II_0018	**Retrieving all APAPs of a given object** The Interface shall allow the requesting OS to retrieve all the Alarm Severity Assignment Profiles (ASAPs) that are assigned to a given object. The requesting OS shall be able to specify the list of resource layer rates for which assigned ASAPs are to be retrieved. If an empty list is specified, then all ASAPs assigned to the addressed resource will be replied. The list shall also be empty if the addressed resource is not a Termination Point. Note that only Termination Point (TPs) can refer to more than one ASAP, with at most one ASAP per encapsulated layer rate.
Source	TMF518_RTM, R_TMF518_RTM_II_0010

R_TMF_MPAC_BA_II_0019	**Creating an ASAP** The Interface shall allow the requesting to create an Alarm Severity Assignment Profile (ASAP) in the target OS. The following parameters are supplied by the requesting OS in conjunction with the ASAP creation request : • Alarm severity assignments – This attribute shall represent the set of alarm severity assignments (refer to R_TMF_MPAC_BA_I_0007).
Source	TMF518_RTM, R_TMF518_RTM_II_0022

R_TMF_MPAC_BA_II_0020	**Modifying an ASAP** The Interface shall allow the requesting OS to modify an Alarm Severity Assignment Profile (ASAP) in the target OS. The target OS shall refuse/fail this request if the ASAP is fixed, i.e., it can neither be modified nor deleted by the requesting OS. The following parameters are supplied by the requesting OS in conjunction with the ASAP modification request : • ASAP name – this parameter shall represent the name of the ASAP that is to be modified. • Alarm severity assignments – this attribute shall represent the new set of alarm severity assignments that are to be applied to the ASAP (refer to R_TMF_MPAC_BA_I_0007).

Source	TMF518_RTM, R_TMF518_RTM_II_0023

R_TMF_MPAC_BA_II_0021	**Deleting an ASAP** The Interface shall allow the requesting OS to delete a given Alarm Severity Assignment Profile (ASAP). The target OS shall refuse/fail this request if at least one object is pointing to this ASAP instance, or the ASAP cannot be deleted, i.e., neither can be modified nor deleted by the requesting OS.
Source	TMF518_RTM, R_TMF518_RTM_II_0024

R_TMF_MPAC_BA_II_0022	**Assigning an ASAP** The Interface shall allow the requesting OS to assign an Alarm Severity Assignment Profile (ASAP) to an instance of any of the following object classes: • Equipment • Equipment Holder • Equipment Protection Group (EPG) • Group Termination Point (GTP) • Managed Element (ME) • Management Domain (MD) • Operations System (OS) • Protection Group (PG) • Subnetwork Connection (SNC) • Termination Point (TP) • Topological Link (TL). The Interface shall allow the requesting OS to specify the following parameters when it requests that a target OS assign an Alarm Severity Assignment Profile (ASAP) to an object: • ASAP name – this parameter shall represent the name of the ASAP that is to be assigned. • Resource ref – this parameter shall represent the name of the object to which the ASAP is to be assigned. • Layer rate – this parameter shall represent the layer rate to which the ASAP is applicable. This shall be need when the addressed object is a Termination Point (TP).
Source	TMF518_RTM, R_TMF518_RTM_II_0025

	TMF518_RTM, R_TMF518_RTM_II_0044

R_TMF_MPAC_BA_II_0023	**De-Assigning an ASAP** The Interface shall allow the requesting OS to de-assign an Alarm Severity Assignment Profile (ASAP) from an instance of any of the object classes listed in R_TMF_MPAC_BA_II_0022. The target OS shall refuse/fail this request if the ASAP is assigned in a fixed way to the object. The Interface shall allow the requesting OS to specify the following parameters when it requests that a target OS de-assign an Alarm Severity Assignment Profile (ASAP) from an object: • Resource Ref – this parameter shall represent the name of the object from which the ASAP is to be de-assigned. • Layer rate – this parameter shall represent the layer rate to which the ASAP is applicable. This shall be need when the addressed object is a Termination Point (TP)
Source	TMF518_RTM, R_TMF518_RTM_II_0026

4.3.3 Protection Management

4.3.3.1 TP Protection Inventory

R_TMF_MPAC_BA_II_0024	**Retrieving all PGs for a given ME** The Interface shall allow an OS to retrieve all the Protection Group (PGs) available in a specified Managed Element (ME).
Source	TMF518_RTM, R_TMF518_RTM_II_0048

The capability stated in R_TMF_MPAC_BA_II_0024 can be used by an OS to manage protected trails between subnetworks. In the case of MSSPRing (BLSR), these protection groups also contain information about the, SPRING_NODE_ID which is needed at the time of subnetwork connection creation (i.e. the ingress/egress nodes of a ring).

R_TMF_MPAC_BA_II_0025	**Retrieving a given PG** The Interface shall allow an OS to retrieve a given Protection Group.
Source	TMF518_RTM, R_TMF518_RTM_II_0067

R_TMF_MPAC_BA_II_0026	**Retrieving all unprotected CTPs** The Interface shall allow an OS to retrieve the names of all the

	Connection Termination Points (CTPs) that support Non-Preemtible Unprotected Traffic (NUT) services associated with a given Protection Group (PG).
Source	TMF518_RTM, R_TMF518_RTM_II_0049

R_TMF_MPAC_BA_II_0027	**Retrieving all protected CTPs** The Interface shall allow an OS to retrieve the names of all the Connection Termination Points (CTPs) that support protected services associated with a given Protection Group (PG).
Source	TMF518_RTM, R_TMF518_RTM_II_0050

R_TMF_MPAC_BA_II_0028	**Retrieving all CTPs supporting preemptible traffic** The Interface shall allow an OS to retrieve the names of all the Connection Termination Points (CTPs) that support preemptible extra traffic (unprotected services that may be preempted by other services) associated with a given Protection Group (PG).
Source	TMF518_RTM, R_TMF518_RTM_II_0051

R_TMF_MPAC_BA_II_0029	**Retrieving all PGs for a given PTP** The Interface shall allow the requesting OS to retrieve the names of the Protection Groups (PGs) containing a given Physical Termination Point (PTP).
Source	TMF518_RTM, R_TMF518_RTM_II_0069

R_TMF_MPAC_BA_II_0030	**Notifications on PGs** The Interface shall allow for the delivery of and subscription to lifecycle notifications (e.g., object creation and deletion) with respect to TP protection groups.
Source	TMF518_RTM, R_TMF518_RTM_II_0052

4.3.3.2 Equipment Protection Inventory

R_TMF_MPAC_BA_II_0031	**Retrieving all EPGs for a given ME** The Interface shall allow an OS to retrieve the attributes of all the Equipment Protection Groups (EPGs) available in a Managed Element (ME).
Source	TMF518_RTM, R_TMF518_RTM_II_0053

R_TMF_MPAC_BA_II_0032	**Retrieving a given EPG**

	The Interface shall allow an OS to retrieve a given Equipment Protection Group.
Source	TMF518_RTM, R_TMF518_RTM_II_0068

R_TMF_MPAC_BA_II_0033	**Notifications on EPGs** The Interface shall allow for the delivery of and subscription to lifecycle notifications (e.g., object creation and deletion) with respect to equipment protection groups.
Source	TMF518_RTM, R_TMF518_RTM_II_0054

4.3.3.3 Trail and Subnetwork Connection Protection

This section addresses the interface requirements that enable an OS to discover and manage trail and subnetwork connection protection and the switching of both trails and the subnetwork connection protection.

The basic principle is one of discovery of trail protection rather than to manage protection switching via the interface.

This section only applies to SONET/SDH.

R_TMF_MPAC_BA_II_0034	**Discovering all trail protection schemes** The Interface shall allow an OS to discover all trail protection schemes (both linear and ring configurations) that exist in the underlying network known to the target OS to the extent known by the target OS. It is possible that the resources of a ring (or a linear system) are split among more than one managing OS. The Interface shall not indicate if the ring is a complete ring, a portion of a complete ring or an open ring that is still in the process of being provisioned (or any linear system). The ordering of Network Elements within a ring is not explicitly indicated across the Interface. Such information may be inferred from the Topological Links passed across the Interface.
Source	TMF518_RTM, R_TMF518_RTM_II_0055

R_TMF_MPAC_BA_II_0035	**Determining traffic source of a PG or SNCP** The Interface shall allow an OS to determine the traffic source of a Protection Group (PG) or a Subnetwork Connection Protection (SNCP). In addition, the requesting OS can determine the following over the interface: • The current protection switch state (whether protection switching is locked, automatic or forced). • The protection attributes (e.g. whether the scheme is

	unidirectional or bi-directional (also known as single or dual ended) or the protocol used for MSSPRING). • If the switching is revertive or not. • Support for 1+1 (with no extra traffic capability) or 1:N which does support extra traffic on the protection resources.
Source	TMF518_RTM, R_TMF518_RTM_II_0056

R_TMF_MPAC_BA_II_0036	**Notifications on switching events related to trails and SNCPs** The Interface shall allow a subscribing OS to register for and the target OS to send notifications in case of switching events related to trail and subnetwork connection protection (SNCP).
Source	TMF518_RTM, R_TMF518_RTM_II_0057

R_TMF_MPAC_BA_II_0037	**Executing protection switch commands** The Interface shall allow an OS to request the execution of protection switch commands that are supported by a Connection Termination Point (CTP) or a Protection Group (PGP) that is currently able to perform a protection switch. CTPs are used only for protection switch commands that cannot be performed via the PGP object. For example for SNCP no PGP object exists and the protection switch operation is applied directly to a CTP. The following are the known values for SDH APS and VC Trail Protection schemes: • Lockout • Clear • Forced Switch • Manual Switch • Exerciser. See ITU-T Recommendation G.841 for definitions of the above commands.
Source	TMF518_RTM, R_TMF518_RTM_II_0058

R_TMF_MPAC_BA_II_0038	**Querying for persistent protection switch commands** The Interface shall allow a requesting OS to query a target OS to determine if any persistent protection switch commands have been invoked. This query shall be supported on a Connection Termination Point (CTP) and on a Protection Group (PG) basis.

	The query on CTP is only applicable for protection schemes that do not employ a PG. For example for SNCP protection no protection group object exists and the protection switch operation and query is applied directly on a CTP. In particular, the following protection switch information shall be obtainable from the target OS: • Type – this attribute shall represent the type of the protection for which the switch has occurred. • Switch reason – this attribute shall represent the reason for the switch. • Layer rate – this attribute shall represent the layer at which the switch has occurred. • PG – this attribute shall represent the name of the Protection Group (PG) in the case of a trail switch. Not used if the protection type is Subnetwork Connection Protection (SNCP). • Protected TP – this attribute shall represent the name of the Termination Point (TP) being protected. • Switch away from TP – this attribute shall represent the name of the TP being switched away from. • Switch to TP – this attribute shall represent the name of the TP that is switched to.
Source	TMF518_RTM, R_TMF518_RTM_II_0059

4.3.3.4 Equipment and TP Protection Management

R_TMF_MPAC_BA_II_0039	**Determining active instances within an EPG** The Interface shall allow an OS to determine the active Equipment instances within an Equipment Protection Group (EPG). In addition, the OS can determine following (over the Interface): • The current protection switch state (whether protection switching is locked, automatic or forced). • The protection attributes. • If the switching is revertive or not. In particular, the Interface shall allow an OS to retrieve the following switch status information for a given Equipment Protection Group (EPG): • Type – this attribute shall represent the type of the protection for which the switch has occurred. • Switch reason – this attribute shall represent the reason

	for the switch. • EPG – this attribute shall represent the name of the Equipment Protection Group (EPG). • Protected Equipment – this attribute shall represent the name of the Equipment being protected. • Switch to Equipment – this attribute shall represent the name of the Equipment that is switched to.
Source	TMF518_RTM, R_TMF518_RTM_II_0060

R_TMF_MPAC_BA_II_0040	**Notifications on Equipment protection switch events** The Interface shall allow a subscribing OS to register for and the target OS to send notifications in case of an Equipment protection switch.
Source	TMF518_RTM, R_TMF518_RTM_II_0061

4.3.4 Maintenance and Diagnostic Test Management

R_TMF_MPAC_BA_II_0041	**Setting and releasing maintenance commands for a TP** The Interface shall allow the OS to request the set and release of maintenance commands that are supported by a Termination Point (TP). The following is a list of maintenance of operations that shall be supported: • Facility Loopback • Terminal Loopback • Facility Forced AIS (Upstream) • Terminal Forced AIS (Downstream) • Force RDI • Set as segment end point (ATM) – Note that un-set is provided by the already-included release action • Launch end-to-end loopback OAM cell (ATM) • Launch segment loopback OAM cell (ATM) • Local Loop Qualification (DSL) • DSL Line Supervision (DSL) See SD1-20 for further details on the specific maintenance operations. A distinct error message will be returned to distinguish between the case where a command is rejected because the current state of the target object does allow for the command to be

	executed and the case where the command is simply not supported.
Source	TMF518_RTM, R_TMF518_RTM_II_0062

R_TMF_MPAC_BA_II_0042	**Querying for persistent maintenance command invocation** The Interface shall allow an OS to query the target OS to determine if any persistent maintenance commands have been invoked. This query is supported with respect to the Managed Element (ME) and Termination Point (TP) objects.
Source	TMF518_RTM, R_TMF518_RTM_II_0063

4.4 Category III: Abnormal or Exception Conditions, Dynamic Requirements

No requirements in this category have been identified.

4.5 Category IV: Expectations and Non-Functional Requirements

No requirements in this category have been identified.

4.6 Category V: System Administration Requirements

No requirements in this category have been identified.

5 Use Cases

Note that all of the following use cases assume the OS (Re)starts use case has occurred as pre-condition. Use cases are only provided for the most complex requirements, so not all requirements are covered.

The corresponding TMF518_RTM use cases have been put in the summary section, as the traceability is used by the macros.

5.1 Provisioning

5.1.1 OS turns alarm reporting "on" for a TP

Use Case Id	UC_TMF_MPAC_BA_0001
Use Case Name	OS turns alarm reporting "on" for a TP
Summary	An OS requests the target OS to activate all alarm reporting on a termination point. Corresponds to TMF518_RTM, UC_TMF518_RTM_0001.
Actor(s)	Requesting OS
Pre-Conditions	All OSs involved in the use case have successfully executed the OS (Re)starts use case.
Begins When	The requesting OS sends the request to activate alarm reporting to the target OS.
Description	1. The requesting OS sends the request to activate alarm reporting "on" for a specified TP. 2. The target OS validates the TP reference (e.g., name). 3. The target OS enables alarm reporting on the specified TP. The alarm reporting state of the contained TP(s) may also be enabled. 4. The target OS replies with a success indication. 5. Attribute Value Change notification(s) for the specified TP and the contained TP(s), if any, are forwarded to the notification service indicating that alarm reporting has been activated for these TP(s).
Ends When	In case of success: The requesting OS receives an indication of success of the action. In case of failure: The requesting OS receives an indication of failure of the action.

Post-Conditions	In case of success: • Alarm monitoring is enabled on the specified TP. This does not mean that alarm is reported anyway, because Alarm Severity Assignment Profile may perform further filtering. • The target OS has forwarded an attribute value change notification if there was an attribute value change with the enabling of alarm monitoring on the TP. In case of failure: None.
Exceptions	Exceptions will be specified during IA Phase. Candidate ones are: 1. Processing failure: The requested operation could not be performed. 2. Invalid input: The TP reference is invalid. 3. Communication loss: It was not possible to reach the given ME(s).
Traceability	R_TMF_MPAC_BA_II_0012, R_TMF_MPAC_BA_BR_0001

5.1.2 OS turns alarm reporting "off" for a TP

Use Case Id	UC_TMF_MPAC_BA_0002
Use Case Name	OS turns alarm reporting "off" for a TP
Summary	The requesting OS asks that the target OS deactivate alarm reporting on a specified termination point (TP). Note: There are no side effects upon transmission behavior (propagated alarm signals e.g. AIS) associated with the TP. Corresponds to TMF518_RTM, UC_TMF518_RTM_0002.
Actor(s)	Requesting OS
Pre-Conditions	All OSs involved in the use case have successfully executed the OS (Re)starts use case.
Begins When	The requesting OS sends the request to deactivate alarm reporting to the target OS.
Description	1. The requesting OS sends the request to deactivate alarm reporting on the specified TP. 2. The target OS validates the TP reference (e.g., name). 3. The target OS disables alarm reporting on the specified TP. The alarm reporting state of the contained TP(s) may also be disabled. This disables alarm reporting even if an assigned Alarm Severity Assignment Profile would allow it. 4. The target OS replies with a success indication. 5. Attribute Value Change notification(s) for the specified TP and the

	contained TP(s), if any, are forwarded to the notification service indicating that alarm reporting has been deactivated for these TP(s).
Ends When	In case of success: The requesting OS receives an indication of success of the action. In case of failure: The requesting OS receives an indication of failure of the action.
Post-Conditions	In case of success: Alarm reporting is disabled on the specified TP and all the contained TP(s). The target OS has forwarded an attribute value change notification. In case of failure: None
Exceptions	Exceptions will be specified during IA Phase. Candidate ones are: 1. Processing failure: The requested operation could not be performed. 2. Invalid input: The TP reference is invalid. 3. Communication loss: It was not possible to reach the given ME(s).
Traceability	R_TMF_MPAC_BA_II_0013 , R_TMF_MPAC_BA_BR_0001

5.1.3 OS assigns an Alarm Severity Assignment Profile (ASAP) to a CTP

Use Case Id	UC_TMF_MPAC_BA_0003
Use Case Name	OS assigns an Alarm Severity Assignment Profile (ASAP) to a CTP (or some other object type that supports the assignment of ASAPs)
Summary	The requesting OS assigns an ASAP, either previously created by the requesting OS or created by some other OS (including, possibly, the target OS), to a CTP, at a specified layer rate. Corresponds to TMF518_RTM, UC_TMF518_RTM_0003.
Actor(s)	Requesting OS
Pre-Conditions	1. All OSs involved in the use case have successfully executed the OS (Re)starts use case. 2. The identified ASAP already exists in the target OS. 3. In case the resource is a TP: the provided layer rate is an encapsulated layer rate of the TP. 4. The identified object (to which the ASAP is to be assigned) has to exist. If not, the ASAP should be created before starting this use

	case. 5. The identified object has to support the ASAP pointer feature.
Begins When	The requesting OS sends the assign ASAP request to the target OS with the specified CTP.
Description	1. The requesting OS sends a request to assign the ASAP to the addressed CTP. 2. The target OS validates the assignment request. 3. If the target OS does not support assignment of ASAPs via this interface, an exception is thrown. 4. If the ASAP name does not refer to an ASAP object, or the specified layerRate is invalid for the addressed resource, i.e., it is not an encapsulated layer rate, then an exception is thrown. 5. If the ASAP name or the resource name reference a non-existent object, then an exception is thrown. 6. If there is a currently assigned ASAP, and this assignment is fixed on target OS side, then an exception is thrown. 7. If the resource name refers to an object not supporting the ASAP pointer feature then an exception is thrown. 8. The requesting OS connects to the notification service and thus is able to receive notifications matching the filter conditions specified (if this has not been done earlier). Note: The main filtering criteria are on the notification type (i.e., alarm and/or threshold crossing alert). In addition, the requesting OS can request other filtering criteria. Any of the parameters of the parameters of the alarm can be used.
Ends When	The target OS sends a reply to the requesting OS.
Post-Conditions	In case of success: This operation causes an alarm re-evaluation of the already detected defects according to the following rules. If alarms are reportable (*): • if the severity changes from any of critical, major, minor, warning, to not alarmed, then an alarm notification with cleared is sent and the alarm is no longer available for any alarm retrieval operation. • if the severity changes from not alarmed to any of critical, major, minor, warning, then an alarm notification with the new perceivedSeverity is sent (with the current target OS/NE time) and the alarm is available for any alarm retrieval operation. • if the severity changes from any of critical, major, minor, warning, to any of critical, major, minor, warning, then

	the alarm re-evaluation process is not performed. (*) an alarm is reportable by ME/target OS when • AlarmReporting = “on” (for PTP, CTP, FTP) • alarmReportingIndicator = true (for SNC, TopologicalLink, Equipment, EquipmentHolder, GTP) • always reportable for all other objects which do not have any alarm reporting attribute. Moreover, once an alarm becomes reportable by ME/target OS then the following procedure is performed: • If the managed object has a valid aSAPpointer, then the referenced ASAP is searched for an entry that satisfies the following conditions: i) The probableCause value is the same in the alarm and in the entry, AND ii) The probableCauseQualifier value is the same in the alarm and in the entry (or the probableCauseQualifier value in the entry is empty) AND iii) The nativeProbableCause value is the same in the alarm and in the entry (or the nativeProbableCause value in the entry is empty). E.g., if the reportable alarm has LOS probableCause and an ASAP entry is found with LOS probableCause and both probableCauseQualifier and nativeProbableCause are empty strings, then that ASAP entry is accepted. If the search is successful then the associated severities are assigned. There are three possible cases: o If the alarm is service affecting, it is assigned the severity specified in the serviceAffecting attribute, if any. If no severity is explicitly assigned, i.e. the value of serviceAffecting attribute is ANY, then see below (*) o If the alarm is non service affecting, it is assigned the severity specified in the serviceNonAffecting attribute, if any. If no severity is explicitly assigned, i.e. the value of serviceNonAffecting is attribute is ANY, then see below (*) o If the alarm is service independent, or if the target OS does not know whether the alarm actually affects the service or not, it is assigned the severity specified in the

	serviceIndependentOrUnknown attribute, if any. If no severity is explicitly assigned, i.e. the value of serviceIndependentOrUnknown attribute is ANY, then see below (*) • If the corresponding probableCause is not found in the ASAP, or the managed object has no aSAPpointer (or the aSAPpointer value is invalid) then: (*) the alarm is assigned the default / native severity at target OS/NE side, if any, otherwise; the INDETERMINATE severity is assigned. Once a severity (including the INDETERMINATE) has been assigned, the alarm notification is emitted, except in the case of the "NOTALARMED" - cleared severity, which causes the non emission of the alarm notification. Any operation of alarm retrieval will not include such "NOTALARMED" alarms. In case of failure: Either the currently assigned ASAP is maintained, e.g. because the assignment is fixed on target OS side, or no ASAP is assigned.
Exceptions	Exceptions will be specified during IA Phase. Candidate ones are: 1. Not implemented: The target OS does not support this service. 2. Processing failure: The requested operation could not be performed. 3. Invalid input: The aSAPName does not refer to an ASAP object, or layerRate is invalid for the addressed resource, i.e. it is not an encapsulated layerRate. 4. Entity not found: The aSAPName or resourceName reference an object that does not exist. 5. Unable to comply: The currently assigned ASAP object cannot be de-assigned, or resourceName refers to object not supporting ASAP pointer feature.
Traceability	R_TMF_MPAC_BA_II_0019, R_TMF_MPAC_BA_II_0022, R_TMF_MPAC_BA_I_0005, R_TMF_MPAC_BA_I_0006, R_TMF_MPAC_BA_I_0007

5.2 Protection Management

5.2.1 OS retrieves all the Protection Groups of a Managed Element

Use Case Id	UC_TMF_MPAC_BA_0004
Use Case Name	OS retrieves all the Protection Groups of a Managed Element

Summary	The requesting OS attempts to learn about the existence of all protection groups that exist in a network element. This use case applies to both TP and equipment protection groups. Corresponds to TMF518_RTM, UC_TMF518_RTM_0004.
Actor(s)	Requesting OS
Pre-Conditions	1. All OSs involved in the use case have successfully executed the OS (Re)starts use case. 2. The Managed Element exists within the control of the target OS.
Begins When	Requesting OS inquires about the existence of the protection groups in a Managed Element.
Description	1. The requesting OS asks for the list of protection groups in a Managed Element. The requesting OS will send the name of the Managed Element as input. Note that the requesting OS can ask for all TP protection groups or all Equipment protection groups, but not both in the same request. 2. The target OS returns the list of all the protection groups contained in the Managed Element. 3. In the case of non-Equipment Protection Groups the target OS orders the protection group TPs in the list as follows: • The ProtectedTPs are always presented ahead of the protecting TP. • The TPs in the East direction are always presented contiguously ahead of the West directions. • In case of 4-fiber rings, there are three groups presented, two span groups and one 4-fiber ring group. • This ordering and scheme is applicable to all technologies. 4. If the target OS does not know the reversion Mode or the protection Scheme state, a value of UNKNOWN is returned. 5. For BLSR and 1:N MSP, non Pre-emptible traffic shall be ALLOWED, or NOT_ALLOWED. 6. The applicable parameters of each protection group type is returned. If not known, a value of UNKNOWN is returned. 7. The ProtectionScheme State is identified to be AUTOMATIC or FORCED_OR_LOCKED_OUT to switch. This indicates whether the protection scheme is free to switch or is constrained from switching. The protection scheme is constrained from switching when it is forced or locked. 8. The wtrTime is provided in seconds. If the target OS cannot obtain that value, a value of -1 is returned.
Ends When	The target OS completes the service.
Post-Conditions	The requesting OS is aware of the protection groups in a Network

	Element.
Exceptions	Exceptions will be specified during IA Phase. Candidate ones are: 1. Processing failure: The requested operation could not be performed. 2. Invalid input: The name of the Network Element in the request does not reference a managedElement object. 3. Entity not found: The name of the Network Element references object which does not exist. 4. Communication loss.
Traceability	R_TMF_MPAC_BA_I_0010, R_TMF_MPAC_BA_I_0011 R_TMF_MPAC_BA_II_0024, R_TMF_MPAC_BA_II_0026, R_TMF_MPAC_BA_II_0027, R_TMF_MPAC_BA_II_0028, R_TMF_MPAC_BA_BR_0002

5.2.2 Protection Switch Notification for Equipment, Trail and SNC Protection

Use Case Id	UC_TMF_MPAC_BA_0005
Use Case Name	Protection Switch Notification for Equipment, Trail and SNC Protection
Summary	This use case describes events that occur at the network level and how the requesting OS learns of them. Corresponds to TMF518_RTM, UC_TMF518_RTM_0005.
Actor(s)	Requesting OS
Pre-Conditions	1. All OSs involved in the use case have successfully executed the OS (Re)starts use case. 2. The requesting has executed UC_TMF_MPAC_BA_0007.In the case of equipment protection, the requesting OS has registered to receive equipment protection switch notifications. 3. In the case of Trail and SNC Protection the Termination Points in question are in a protection configuration. 4. In the case of Equipment, the Equipment instances in question are in a protection configuration (only M:N equipment protection has been identified, so far)
Begins When	Either a network fault has occurred or a user triggers a switch from the target OS or the Craft creating a switch in the traffic source or the requesting OS triggers a switch.
Description	1. In case of Trail protection switch (including the span switch in a 4-fiber ring configurations), the traffic source has switched from the protected to protecting or vice versa. 2. In case of a ring switch, the traffic has switched from the protected

	channels of a span to the protecting channels of the other span. 3. In case of a SNC protection switch, the traffic being received at the reliable TP (the output of the service selector), is switched from the worker TP to the protection TP or switched back. 4. The 1+1 and 1:N Trail protection (including the span switch in a 4-fiber ring) notification is raised against the Trail protection groups. 5. In the case of M:N equipment protection, the notification is raised against the equipment protection group. 6. In case of a ring switch the notification is raised against the Ring groups. 7. In case of a SNC protection switch, the notification is raised against the reliable TP. The target OS provides the following information to the requesting OS in the notification: • The protection type shall be provided to identify whether a protection switch is an Equipment protection, Trail protection or an SNC protection. • The switch reason shall be provided, which shall be Restored, Signal Fail, Signal Mismatch, Signal Degrade, Automatic Switch, Manual Switch, or Not Applicable. • In the case of Trail or SNC protection the layer rate shall be provided to which this switch is related. • The group name shall be provided, which identifies the protection group for which protection switch status is being reported. The group name shall be NULL if the protection type is SNC protection. • The protected TP shall be provided. For a SNC, this is always the reliable TP. For a 2F MSSP ring notification, this is the TP that is/was inactive during the switch. For a 4F MSSP ring switch notification, this is the worker TP that is/was inactive during the switch. For a 1:N MSP switch notification, this is the worker TP for which the protection switch occurred. For a revertive 1+1 MSP, this is always the worker TP. For a non-revertive 1+1 MSP switch notification, this is the TP that is inactive after the switch. In the case of equipment protection, the protected equipment instance shall be provided. For an M:N group, the protected equipment instance always identifies the worker equipment instance for which the switch occurred. • The switchAwayFromTP shall be provided. For a 2F MSSP ring switch, this is the TP that switched. For a 4F MSSP ring span switch, this is one of the TPs in the Trail1:N groups (worker or protection). In the case of equipment protection, the switchAwayFromEquipment is provided (this identifies the equipment instance being

	switched away from). • The switchToTP shall be provided, which identifies the TP that is the active source after the switch, or currently active if no protection switch is currently active. In the case of equipment protection, the switchToEquipment is provided (this identifies the equipment instance which is being switched to).
Ends When	The requesting OS is notified of the switch.
Post-Conditions	Subject to filter conditions, the requesting OS knows of the present traffic source.
Exceptions	Not applicable.
Traceability	R_TMF_MPAC_BA_II_0040, R_TMF_MPAC_BA_BR_0002

5.2.3 OS retrieves the protection switch information for Equipment, Trail and SNC Protection

Use Case Id	UC_TMF_MPAC_BA_0006
Use Case Name	OS retrieves the protection switch information for Equipment, Trail and SNC Protection
Summary	This use case describes how an OS learns about the traffic source of the protection groups and protected SNCs. Corresponds to TMF518_RTM, UC_TMF518_RTM_0006.
Actor(s)	Requesting OS
Pre-Conditions	1. All OSs involved in the use case have successfully executed the OS (Re)starts use case. 2. The Termination Points in question are in a protection configuration (Trail or SNC Protection). 3. In the case of Equipment, the equipment instances in question are in a protection configuration.
Begins When	The requesting OS wishes to discover the present traffic source of a Trail or a SNC Protection configuration, or the active equipment instance in an Equipment protection group.
Description	The target OS provides the following information to the requesting OS in the response to a query regarding the current protection switch status of a protection group or a SNC: 1. The protection type shall be provided to identify whether a protection switch is a Trail protection switch or a SNC protection switch. 2. The switch reason shall be provided, which shall be Restored, Signal Fail, Signal Mismatch, Signal Degrade, Automatic Switch, Manual Switch, or Not Applicable. 3. The layerRate shall be provided, to which this switch is relevant (not applicable for equipment protection).

	4. The group name shall be provided, which identifies the protection group for which protection switch status is being reported. The group name shall be NULL if the protection type indicates SNC protection. 5. TP Protection: The protected TP shall be provided. For a SNC protection, this is always the reliable TP. For a retrieval of a 2Fiber MS SP ring, each TP is protected, and two SwitchData structures are returned. For a retrieval of a 4Fiber MS SP ring, each worker TP is protected, and two SwitchData structures are returned. For a retrieval of a 1:N Trail protection, each worker TP is protected, and N SwitchData structures are returned. For a revertive 1+1 Trail protection, this is always the worker TP. For a retrieval of a non-revertive 1+1 Trail protection switch, this is the active TP. 6. Equipment Protection: For a retrieval of an M:N group, the protected equipment always identifies a worker equipment instance. In this case, N ESwitchData structures are returned as a result of retrieve ESwitchData request (one for each worker equipment instance). 7. The switchToTP shall be provided, which identifies the TP that is the active source after the switch, or currently active if no protection switch is currently active. 8. In the case of equipment protection, the protected equipment instance shall be provided. For an M:N group, the protected equipment instance always identifies the worker equipment instance for which the switch occurred.
Ends When	The requesting OS is presented with all the information.
Post-Conditions	The requesting OS knows about the traffic source.
Exceptions	Exceptions will be specified during IA Phase. Candidate ones are: 1. Not implemented: The target OS is unable to support this service. 2. Processing failure: The requested operation could not be performed. 3. Invalid input: The input object does not reference a protection group or a reliable CTP of a SNC object. 4. Entity not found: The input object does not exist. 5. Communication loss.
Traceability	R_TMF_MPAC_BA_II_0031 , R_TMF_MPAC_BA_II_0034, R_TMF_MPAC_BA_BR_0002

5.2.4 OS registers to receive protection switch notifications

Use Case Id	UC_TMF_MPAC_BA_0007

Use Case Name	OS registers to receive protection switch notifications
Summary	The requesting OS registers at the notification service related to the target, sets the appropriate filter to receive protection switch notifications, and connects to the notification service. Corresponds to TMF518_RTM, UC_TMF518_RTM_0007.
Actor(s)	Requesting OS
Pre-Conditions	1. All OSs involved in the use case have successfully executed the OS (Re)starts use case. 2. The requesting OS has a reference to the notification service used by the target OS.
Begins When	The requesting OS sends a request to register itself at the notification service related to the target OS.
Description	**Note:** The requesting OS registers at the notification service related to the target OS as a consumer of notifications (if this has not been done earlier). **Note:** The requesting OS sets the filter criteria needed to receive protection switch notifications from the target OS via the notification service. **Note:** The requesting OS connects to the notification service and thus is able to receive notifications matching the filter conditions specified (if this has not been done earlier). The main filtering criteria are on the notification type (i.e., protection switch). In addition, the requesting OS can request other filtering criteria. Any of the parameters of the filterable body of the protection switch notification (R_TMF_MPAC_BA_I_0043, R_TMF_MPAC_BA_I_0044) can be used.
Ends When	In case of success: The requesting OS receives a positive acknowledgement to its connection request to the notification service. In case of failure: The target OS returns an error indication.
Post-Conditions	In case of success: The specified filter(s) are set up or modified. In case of failure: The requesting OS receives a negative acknowledgement to a request for registration, filter building or connection or a request times out.
Exceptions	Exceptions will be specified during IA Phase. Candidate ones are: • Illegal consumer type • Consumer already connected

Traceability	R_TMF_MPAC_BA_I_0043, R_TMF_MPAC_BA_I_0044 R_TMF_MPAC_BA_II_0036 , R_TMF_MPAC_BA_II_0040

5.2.5 OS invokes protection switch lockout to an SNC

Use Case Id	UC_TMF_MPAC_BA_0008
Use Case Name	OS invokes protection switch lockout to an SNC
Summary	The requesting OS applies protection switch lockout to a reliable CTP of a SNC that is protected by SNCP. Corresponds to TMF518_RTM, UC_TMF518_RTM_0008.
Actor(s)	Requesting OS
Pre-Conditions	1. All OSs involved in the use case have successfully executed the OS (Re)starts use case. 2. The requesting OS has determined which CTPs participate in the SNCP switch.
Begins When	A request to apply a protection command is applied.
Description	The command is applied to the reliable CTP that is defined as being able to perform a protection switch.
Ends When	The target responds that the command was applied or an exception is thrown.
Post-Conditions	1. Traffic has been switched to the TP identified by toTPName. 2. The protection switch status of the reliable CTP has changed.
Exceptions	Exceptions will be specified during IA Phase. Candidate ones are: 1. Processing failure: The requested operation could not be performed. 2. Unable to comply: The CTP is not performing a protection switch in a SNCP. 3. Not implemented: The target OS does not support this service. 4. Invalid input: The input object does not reference a protection group or a reliable CTP of a SNC object. 5. Entity not found: The input object does not exist. 6. Communication loss.
Traceability	R_TMF_MPAC_BA_II_0037

5.3 Equipment Management

5.3.1 OS provisions alarm reporting on/off for equipment

Use Case Id	UC_TMF_MPAC_BA_0009
Use Case Name	OS provisions alarm reporting on/off for equipment
Summary	The requesting OS asks that the target OS activate/deactivate all alarm reporting on an equipment. Corresponds to TMF518_RTM, UC_TMF518_RTM_0025.
Actor(s)	Requesting OS
Pre-Conditions	All OSs involved in the use case have successfully executed the OS (Re)starts use case.
Begins When	The requesting OS sends the request to activate/deactivate alarm reporting to the target OS.
Description	1. The requesting OS sends a request to activate/deactivate alarm reporting for a specified equipment. 2. The target OS validates the equipment reference (e.g., name). 3. The target OS enables/disables alarm reporting on the specified equipment. 4. The target OS replies with a success indication. 5. Attribute Value Change notification(s) for the specified equipment are forwarded to the notification service indicating that alarm reporting has been activated/deactivated for the specified equipment.
Ends When	In case of success: The requesting OS receives an indication of success for the requested action. In case of failure: The requesting OS receives an indication of failure for the requested action.
Post-Conditions	In case of success: Alarm monitoring is enabled/disabled on the specified equipment. [Note: If alarm monitoring is enabled, this does not necessarily mean that alarms are reported, because an applied Alarm Severity Assignment Profile may perform further filtering. If alarm monitoring is disabled, then alarm reporting is disabled even if an applied Alarm Severity Assignment Profile would allow it.]

	The target OS has forwarded an AVC notification if there was an attribute value change associated with the enabling/disabling of alarm monitoring on the equipment. In case of failure: None.
Exceptions	Exceptions will be specified during IA Phase. Candidate ones are: 1. Invalid input: The equipment reference is invalid. 2. Communications loss. 3. Entity not found: The specified equipment object does not exist. 4. Processing failure: The requested operation could not be performed. 5. Unable to comply: Alarm reporting cannot be enabled/disabled for the give equipment instance
Traceability	R_TMF_MPAC_BA_II_0014 , R_TMF_MPAC_BA_II_0015, R_TMF_MPAC_BA_BR_0001

5.4 Craft Related

5.4.1 Craft/ Target OS creates a Protection Group

Use Case Id	UC_TMF_MPAC_BA_0011
Use Case Name	Craft/Target OS creates a Protection Group
Summary	The Craft creates a Protection Group on a network element via the target OS (e.g., an EMS) or on the network element itself, or the target OS detects a new protection group has been created on a network element. This use case is to cover both TP and equipment protection groups. Corresponds to TMF518_RTM, UC_TMF518_RTM_0027.
Actor(s)	Craft or target OS
Pre-Conditions	1. All OSs involved in the use case have successfully executed the OS (Re)starts use case. 2. The target OS and registered OSs are connected to the notification service.
Begins When	The target OS detects that a Protection Group was created on a Managed Element.
Description	1. The target OS identifies the protection group type. If the protection group identified pertains to a 4 fiber MS SP ring (BLSR) protection, the target OS sends three separate object creation notifications (one each for the span groups and one for the

	combined groups). In all other cases, a single group is identified to be sent to the registered OSs. 2. The object creation notification identifies the steady state switch status of the protection group. 3. Edge point Boolean is set for this notification if any of the TPs forming the protection group is an edge point.
Ends When	The target OS sends applicable notifications to the registered OSs.
Post-Conditions	The registered OSs are aware of the existence of the line level protection.
Exceptions	None
Traceability	R_TMF_MPAC_BA_II_0030 , R_TMF_MPAC_BA_II_0033

6 Traceability Matrices

6.1 Use Case – Requirements Matrix

{You MUST start with the UCs Matrix by using the createUCsMatrix button)

Use Case Id	Use Case Name	Requirements
UC_TMF_MPAC_BA_0001	OS turns alarm reporting “on” for a TP	R_TMF_MPAC_BA_II_0012, R_TMF_MPAC_BA_BR_0001
UC_TMF_MPAC_BA_0002	OS turns alarm reporting “off” for a TP	R_TMF_MPAC_BA_II_0013 , R_TMF_MPAC_BA_BR_0001
UC_TMF_MPAC_BA_0003	OS assigns an Alarm Severity Assignment Profile (ASAP) to a CTP (or some other object type that supports the assignment of ASAPs)	R_TMF_MPAC_BA_II_0019, R_TMF_MPAC_BA_II_0022, R_TMF_MPAC_BA_I_0005, R_TMF_MPAC_BA_I_0006, R_TMF_MPAC_BA_I_0007
UC_TMF_MPAC_BA_0004	OS retrieves all the Protection Groups of a Managed Element	R_TMF_MPAC_BA_I_0010, R_TMF_MPAC_BA_I_0011 R_TMF_MPAC_BA_II_0024, R_TMF_MPAC_BA_II_0026, R_TMF_MPAC_BA_II_0027, R_TMF_MPAC_BA_II_0028, R_TMF_MPAC_BA_BR_0002
UC_TMF_MPAC_BA_0005	Protection Switch Notification for Equipment, Trail and SNC Protection	R_TMF_MPAC_BA_II_0040, R_TMF_MPAC_BA_BR_0002
UC_TMF_MPAC_BA_0006	OS retrieves the protection switch information for Equipment, Trail and SNC Protection	R_TMF_MPAC_BA_II_0031 , R_TMF_MPAC_BA_II_0034, R_TMF_MPAC_BA_BR_0002
UC_TMF_MPAC_BA_0007	OS registers to receive protection switch notifications	R_TMF_MPAC_BA_I_0043, R_TMF_MPAC_BA_I_0044 R_TMF_MPAC_BA_II_0036 , R_TMF_MPAC_BA_II_0040
UC_TMF_MPAC_BA_0008	OS invokes protection switch lockout to an SNC	R_TMF_MPAC_BA_II_0037
UC_TMF_MPAC_BA_0009	OS provisions alarm reporting on/off for equipment	R_TMF_MPAC_BA_II_0014 , R_TMF_MPAC_BA_II_0015, R_TMF_MPAC_BA_BR_0001
UC_TMF_MPAC_BA_0011	Craft/Target OS creates a Protection Group	R_TMF_MPAC_BA_II_0030 , R_TMF_MPAC_BA_II_0033

6.2 Requirements – Use Case Matrix

{Then you will create the Rqs Matrix by using the createRqsMatrix button)

Requirement Id	Use Case Name	Use Case Id
R_TMF_MPAC_BA_BR_0001	OS provisions alarm reporting on/off for equipment OS turns alarm reporting “off” for a TP OS turns alarm reporting “on” for a TP	UC_TMF_MPAC_BA_0009 UC_TMF_MPAC_BA_0002 UC_TMF_MPAC_BA_0001
R_TMF_MPAC_BA_BR_0002	OS retrieves the protection switch information for Equipment, Trail and SNC Protection Protection Switch Notification for Equipment, Trail and SNC Protection OS retrieves all the Protection Groups of a Managed Element	UC_TMF_MPAC_BA_0006 UC_TMF_MPAC_BA_0005 UC_TMF_MPAC_BA_0004
R_TMF_MPAC_BA_BR_0003		
R_TMF_MPAC_BA_BR_0004		
R_TMF_MPAC_BA_I_0005	OS assigns an Alarm Severity Assignment Profile (ASAP) to a CTP (or some other object type that supports the assignment of ASAPs)	UC_TMF_MPAC_BA_0003
R_TMF_MPAC_BA_I_0006	OS assigns an Alarm Severity Assignment Profile (ASAP) to a CTP (or some other object type that supports the assignment of ASAPs)	UC_TMF_MPAC_BA_0003
R_TMF_MPAC_BA_I_0007	OS assigns an Alarm Severity Assignment Profile (ASAP) to a CTP (or some other object type that supports the assignment of ASAPs)	UC_TMF_MPAC_BA_0003

R_TMF_MPAC_BA_I_0008		
R_TMF_MPAC_BA_I_0009		
R_TMF_MPAC_BA_I_0010	OS retrieves all the Protection Groups of a Managed Element	UC_TMF_MPAC_BA_0004
R_TMF_MPAC_BA_I_0011	OS retrieves all the Protection Groups of a Managed Element	UC_TMF_MPAC_BA_0004
R_TMF_MPAC_BA_I_0043	OS registers to receive protection switch notifications	UC_TMF_MPAC_BA_0007
R_TMF_MPAC_BA_I_0044	OS registers to receive protection switch notifications	UC_TMF_MPAC_BA_0007
R_TMF_MPAC_BA_II_0012	OS turns alarm reporting “on” for a TP	UC_TMF_MPAC_BA_0001
R_TMF_MPAC_BA_II_0013	OS turns alarm reporting “off” for a TP	UC_TMF_MPAC_BA_0002
R_TMF_MPAC_BA_II_0014	OS provisions alarm reporting on/off for equipment	UC_TMF_MPAC_BA_0009
R_TMF_MPAC_BA_II_0015	OS provisions alarm reporting on/off for equipment	UC_TMF_MPAC_BA_0009
R_TMF_MPAC_BA_II_0016		
R_TMF_MPAC_BA_II_0017		
R_TMF_MPAC_BA_II_0018		
R_TMF_MPAC_BA_II_0019	OS assigns an Alarm Severity Assignment Profile (ASAP) to a CTP (or some other object type that supports the assignment of ASAPs)	UC_TMF_MPAC_BA_0003
R_TMF_MPAC_BA_II_0020		
R_TMF_MPAC_BA_II_0021		
R_TMF_MPAC_BA_II_0022	OS assigns an Alarm Severity Assignment Profile (ASAP) to a CTP (or some other object type that supports the assignment of ASAPs)	UC_TMF_MPAC_BA_0003
R_TMF_MPAC_BA_II_0023		
R_TMF_MPAC_BA_II_0024	OS retrieves all the Protection Groups of a Managed Element	UC_TMF_MPAC_BA_0004

R_TMF_MPAC_BA_II_0025		
R_TMF_MPAC_BA_II_0026	OS retrieves all the Protection Groups of a Managed Element	UC_TMF_MPAC_BA_0004
R_TMF_MPAC_BA_II_0027	OS retrieves all the Protection Groups of a Managed Element	UC_TMF_MPAC_BA_0004
R_TMF_MPAC_BA_II_0028	OS retrieves all the Protection Groups of a Managed Element	UC_TMF_MPAC_BA_0004
R_TMF_MPAC_BA_II_0029		
R_TMF_MPAC_BA_II_0030	Craft/Target OS creates a Protection Group	UC_TMF_MPAC_BA_0011
R_TMF_MPAC_BA_II_0031	OS retrieves the protection switch information for Equipment, Trail and SNC Protection	UC_TMF_MPAC_BA_0006
R_TMF_MPAC_BA_II_0032		
R_TMF_MPAC_BA_II_0033	Craft/Target OS creates a Protection Group	UC_TMF_MPAC_BA_0011
R_TMF_MPAC_BA_II_0034	OS retrieves the protection switch information for Equipment, Trail and SNC Protection	UC_TMF_MPAC_BA_0006
R_TMF_MPAC_BA_II_0035		
R_TMF_MPAC_BA_II_0036	OS registers to receive protection switch notifications	UC_TMF_MPAC_BA_0007
R_TMF_MPAC_BA_II_0037	OS invokes protection switch lockout to an SNC	UC_TMF_MPAC_BA_0008
R_TMF_MPAC_BA_II_0038		
R_TMF_MPAC_BA_II_0039		
R_TMF_MPAC_BA_II_0040	OS registers to receive protection switch notifications Protection Switch Notification for Equipment, Trail and SNC Protection	UC_TMF_MPAC_BA_0007 UC_TMF_MPAC_BA_0005
R_TMF_MPAC_BA_II_0041		
R_TMF_MPAC_BA_II_0042		

7 Future Directions

7.1 Open Issues

{Describe issues that have not yet been resolved before the BA goes for approval}

8 References and Disclosures

8.1 References

Reference	Author	Description
TMF518_RTM	mTOP RM team	Resource Trouble Management (RTM) – DDP BA
TMF518_NRA	mTOP RM team	Network Resource Assurance (NRA) – DDP BA

8.2 IPR Releases and Patent Disclosure

This document may involve a claim of patent rights by one or more of the contributors to this document, pursuant to the Agreement on Intellectual Rights between the TM Forum and its members. Interested parties should contact the TM Forum office to obtain notice of current patent rights claims subject to this document.

9 Administrative Appendix

This Appendix provides additional background material about the TM Forum and this document.

9.1 About this document

This document has been generated from the TIP_BA.dot Word template, which itself is based on Version 6.0 of the TMF 402, BA Template.

9.2 Use and Extension of a TM Forum Business Agreement

This document defines the business problem and requirement model for Maintenance, Problem and Alarm Control. The Business Agreement is used to gain consensus on the business requirements for exchanging information among processes and systems in order to solve a specific business problem. The Business Agreement should feed the development of Information Agreement(s), which is a technology-neutral model of one or more interfaces. While the Business Agreement contains sufficient information to be a "stand alone" document, it is better read together with the Information Agreement document when the Information Agreement is available. Reviewing the two documents together helps in gaining a full understanding of how the technology neutral information model solution is defined for this requirement model. An initial Business Agreement may only deal with a subset of the requirements. It is acceptable for subsequent issues of the document to add additional requirements not addressed by earlier releases of the BA. Business Agreements are the basis for requirement traceability for information models.

It is expected that this document will be used:

- As the foundation for a TM Forum Information Agreement(s)
- To facilitate requirement agreement between Service Providers and vendors
- As input to a service Provider's Request for Information / Request for Proposal (RFI/RFP—RFX)
- As input for vendors developing COTS products
- As a source of requirements for other bodies working in this area

9.3 Document History

Version Number	Date Modified	Modified by:	Description of changes
V1.0	22-Feb-2010	M. Flauw	Initial version from TMF518 BAs
V1.1	11-May-2011	Alicja Kawecki	Notice updated, minor cosmetic corrections made prior to web posting and ME
V1.2	14-Sep-2011	Alicja Kawecki	Updated to reflect TM Forum Approved status

9.4 Company Contact Details

Company	Team Member Representative
Members of TIP Resource & Service Assurance team	

9.5 Acknowledgments

This document was prepared by the members of the TM Forum RSA team

- Marc Flauw, HP, **Editor**

Inputs from TMF518_NRA and TMF518_RTM were key for this BA. These documents were prepared by the following members of the TM Forum mTOP RM team:

- Keith Dorking, Ciena Corporation
- Steve Fratini, Telcordia Technologies
- Michel Besson, Amdocs

Additional input was provided by the following people:

- Bernd Zeuner, Deutsche Telekom
- Steve Fratini, Telcordia