



# IMPACTS OF SERVICE MANAGEMENT OF NEW GENERATION SERVICES ON FAULT MANAGEMENT SYSTEM

WHITE PAPER

Authors: Raghavendra Rao Tadepalli, Vinay Stephen Devadatta.

## Abstract:

*With the advent of new technologies, it has become technically possible to give a plethora of services and combination of services to the consumer. However it is becoming more and more difficult to be able to manage them in parallel. This has triggered a requirement for a full-fledged, end to end service management. Service Management is dependent on efficient and flexible support from resource management entities. This document envisages putting together the impact of service management on Fault management system of the Resource Management Layer.*

*The first section is an introduction, and talks about why the service management for new generation services needs to be different than traditional application working in silos scenario. Subsequent section deals with Service Management issues which can influence Resource management entities and their interface towards service management. This is followed by subsection dealing with specific requirements on the Fault Management System.*

## Table of Contents

INTRODUCTION .....	3
SCOPE.....	3
CONVENTIONS .....	5
IMPACTING CONSIDERATIONS .....	7
SUMMARY .....	10
APPENDIX – REQUIREMENTS TO A FAULT MANAGEMENT SYSTEM .....	11
Functional impacts.....	11
Information Model.....	17
GLOSSARY .....	19
REFERENCES.....	19
ABOUT THE AUTHORS.....	20

## Figures

FIGURE 1: APPLICATION FRAMEWORK ILLUSTRATING THE APPLICATIONS INVOLVED IN SERVICE PROBLEM MANAGEMENT AND RESOURCE TROUBLE MANAGEMENT.....	4
FIGURE 2: BUSINESS PROCESS FRAMEWORK HIGHLIGHTING THE SERVICE PROBLEM MANAGEMENT & RESOURCE TROUBLE MANAGEMENT PROCESSES. ....	5
FIGURE 3: SEQUENCE DIAGRAM DEPICTING HOW SPMs CAN DEFINE ALARM GROUPING CATEGORIES ON RTMs. ....	12
FIGURE 4: SEQUENCE DIAGRAM DEPICTING ACTIVATION OF ALARM CORRELATION RULES ON RTM FROM A SPM. ....	13
FIGURE 5: SPM SETTING UNIQUE IDENTIFIERS TO RTMs IN ITS DOMAIN.....	14
FIGURE 6: RTM INDICATING TO SPM THE NEED FOR ALARM RE-SYNCHRONIZATION BECAUSE OF A FAILURE IN NETWORK CONNECTIVITY WITH A SUB-NETWORK. ....	14
FIGURE 7: DELTA-SYNCHRONIZATION OF ALARMS BETWEEN SPM & RTM. ....	15
FIGURE 8: SPM RECLASSIFYING THE SEVERITY OF AN ALARM. ....	16
FIGURE 9: SPM PRIORITIZING THE FAULT FIXES BASED ON THE REPAIR TIME ESTIMATES FROM RTM AND THE SERVICE PRIORITIES. ....	17

## Introduction

In the recent years market deregulation, bandwidth abundance and relatively cheaper network equipments has given ample opportunities to various operators and service providers to venture in to wireless broadband space. Moreover, users are also looking for quicker, cost effective, reliable and self-manageable services. The key to sustain business and streamline revenue flow is how efficiently operators assure seamless services to Customers and promptness of operators to respond to Customer issues and network faults.

The next generation services will not only span across multiple technologies and communication domains but also multiple business models and operational support models. Hence management of these services can be a very complicated task. The Service Management entities (or SM&O processes) cannot work in isolation, and they depend a lot on resource management entities (or RM&O processes) in facilitating their operations.

It is the Service Assurance that an operator can provide to the Customers that differentiates the operators and hence has become the prime focus area today. Service Problem Management is a part of Service Assurance domain which comprises of set of processes, guidelines and best practices to manage different problems related to services and network resources.

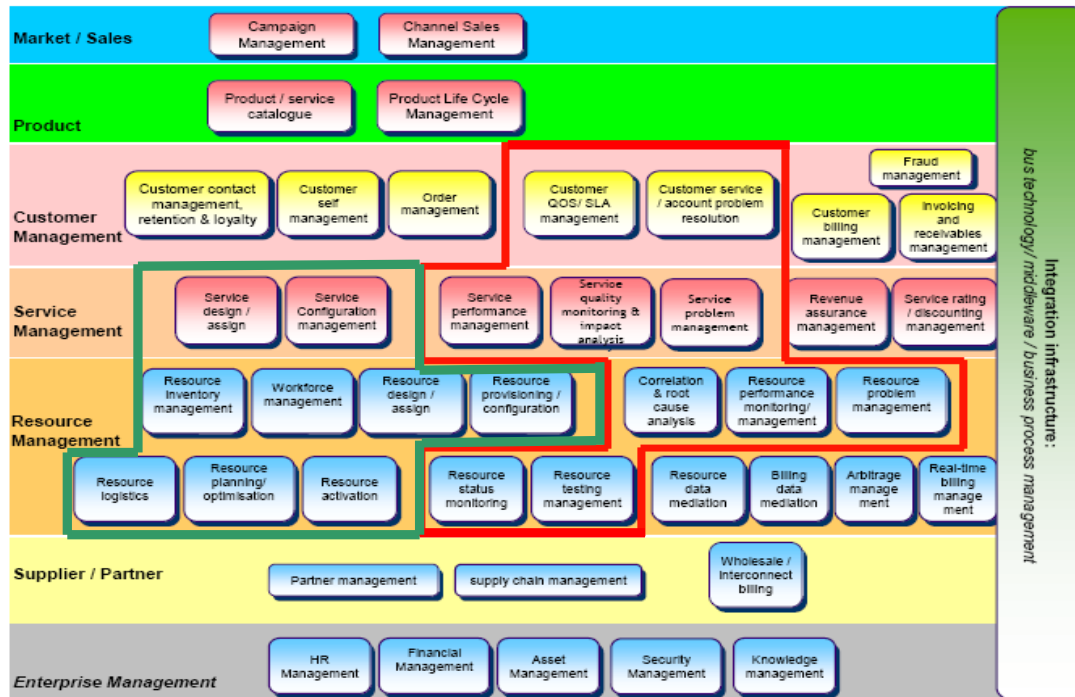
Service Problem Management processes respond immediately to customer affecting service problems or failures in order to minimize their effects on customers, and invoke the restoration of the service as soon as possible. These processes encompass the reporting of problems, making a temporary fix or workaround, isolating the root cause and acting to resolve it.

## Scope

The scope of this document is currently restricted to Service Problem Management (SPM) and Resource Trouble Management entities and their interaction. The interaction is limited to facilitating SM processes to respond immediately to customer affecting service problems failures in order to minimize their effects on customers, and invoke the restoration of the service as soon as possible.

This document tries to emphasize that Fault management (RTM) needs to support all the SM&O FAB functions, and hence the N-bound interface offered by the RTM should accommodate all needed functions for such support. SPM needn't have to extract and replicate information from RTM just to pass it on to other SM&O functions, rather it should only retrieve that information that is required by it to perform the problem management function. If SM&O require such information they can (and should) directly access it from the RTM. This paper tries to give a overview of the N-bound interface to be offered by a RTM so that it can directly cater to the various needs of the SM&O functions.

The following figure shows the applications that are involved in the fault management process as well as the applications that are dependant on fault management.



**Figure 1: Application Framework illustrating the applications involved in Service Problem Management and Resource Trouble Management.**

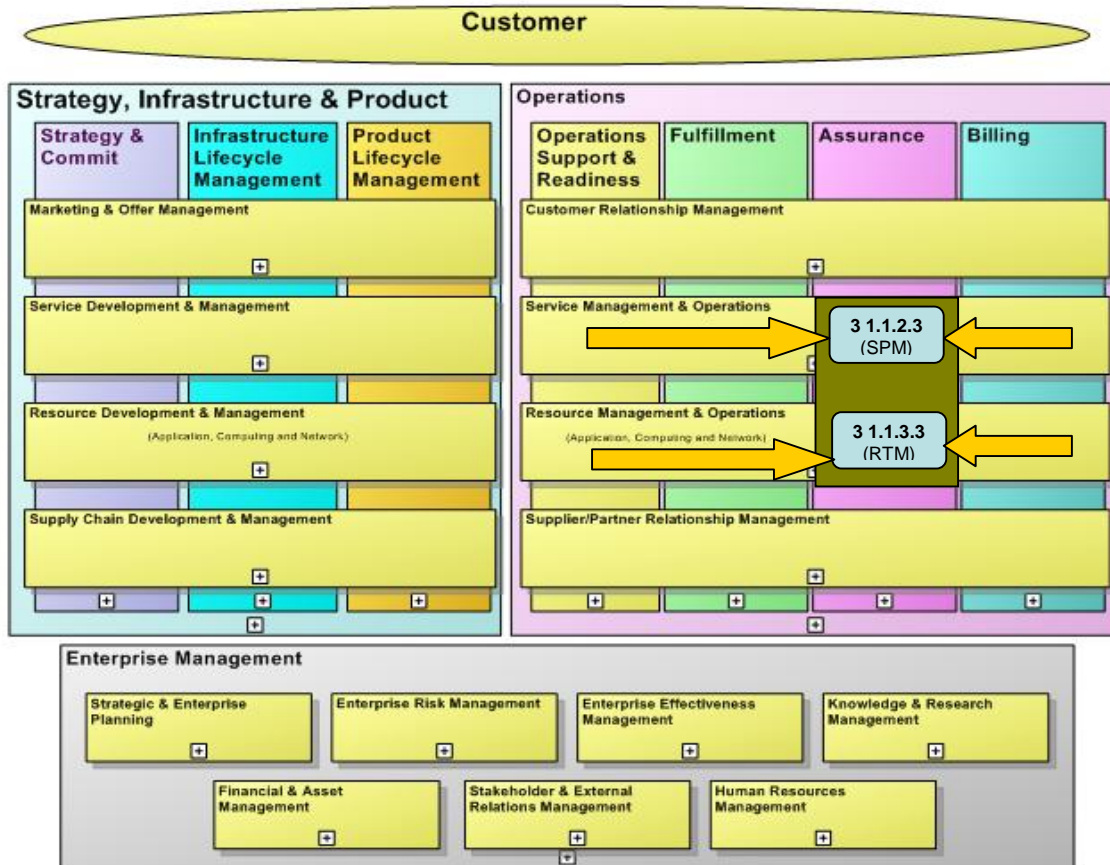
**Legend:**

	Applications involved in Service Problem Management & Resource Trouble Management Processes.
	Applications dependant on Service Problem Management & Resource Trouble Management Processes.

## Conventions

The process names used in this document are in accordance with the Framework prescribed nomenclature.

This document mainly deals with 2 of the processes defined by Business Process Framework:



**Figure 2: Business Process Framework highlighting the Service Problem Management & Resource Trouble Management processes.**

**Legend:**

**3 1.1.2.3 – Service Problem Management (SPM)**

**3 1.1.3.3 – Resource Trouble Management (RTM)**



## Impacting Considerations

The following are the possible aspects of Next Generation Services which can potentially affect the Resource Trouble Management interaction with Service Problem Management. The order of enumeration has no particular significance.

### Discovery of Resource Trouble Management Systems

Service management is usually aware of the network elements involved in a given service / group of services but is not aware of which OSS domain it belongs to. Thus its request for information and commands to Network elements will not have domain information. Hence it is important to have a communication mechanism available for the Service Problem Management that doesn't require the domain information to be supplied by the SPM. Such abstraction will facilitate the SPM to focus on the service level problems and enable easy integration with multiple Resource Trouble Management solution. This is especially important in multi-vendor network scenarios.

### Hierarchical Fault Management:

As new network technologies are emerging, there is an increasing need from the operators to unify the different management systems under a single umbrella. This implies large network element volumes have to be managed by a single service management application. It is not practical to capture/analyze/correlate all faults on all network elements. The fault information required from network management/sub network management perspective can be different from service management perspective. This means that the service problem management should have the ability to inform its context information to the resource trouble management systems. The Resource Trouble Management systems should in-turn have the ability to co-relate and abstract the lower level details from the Service Problem Management system.

### Normalization of alarm information model:

SM will need to use information from across domain managers. The fault information collected by each domain manager could be different. For example the probable cause of alarm could be different at each domain manager. Hence fault information needs to be normalized when it reaches service management. In most of the systems such normalization has to be done in the service management layer. Much of the processing in the Service Management layer is currently focusing on normalization of data rather than the service level functions. To overcome this, it should be possible for the Service Problem Management to inform the underlying Resource Trouble Management systems about the expected format of the data and the Resource Trouble Management systems should guarantee sending of such normalized data to Service layer. If this is not possible there is a need for a separate SPM to RTM conversion layer that would take care of such normalization, so that the SPM can focus on actual identification, analysis, correlations etc of the service level faults.

### Service oriented segmentation of the network:

SM will use segmentations /hierarchies of its own to manage the network from perspective of different services , which means it should be possible for SM to define NE groupings of its own ( which could be very different from network hierarchical grouping done at network management ) while extracting information from DMs. For example the type of services used at suburbs can be different from that in downtown and hence the fault co-relations that need to be carried out in the downtown cells can be different from that of suburb cells. Hence there should be a mechanism available for the SPM to query the co-relation rules used by the RTM and also the ability to modify such co-relation rules on the RTM.

**Service driven configuration changes spanning multiple domains:**

Services can potentially span over the multiple sub networks being managed by different Domain Managers. In the fulfillment sub-process configuration changes may need to be done across NEs belonging different DMs, where the requirement would be to make either all or none changes. Hence there can be requirement that SM can request for a coordinated configuration change across DMs.

**Service priority driven Alarm processing:**

It might be necessary to manage individual instances (sessions) of a service, (example - very high availability needs to be maintained for services involving stock market ...). In contrast currently for voice calls instance specific monitoring is carried out for diagnostic and not for management purpose. This implies that faults related to a particular service may be of higher priority from the service perspective. Hence the RTM should allow SPM to reassign severity to the faults based on the impact to the service.

**Service Problem Management spanning multiple domains (RTMs):**

A service might involve multiple technologies, in fact a single instance of a service (or a single session) could very well involve both wireless and wire line access. Incases where there are different RTM solutions for managing the different network fault; it might be necessary that fault information of wireless domain be relatable to fault information from wire line domain. Thus RTMs should provide necessary information related to the fault so that SPM can correlate such faults and identify the root-cause.

**Alarm Archival & Statistics:**

It might be required to carry out decisions and operation by Service Management Layer based on information gathered at similar situation in past. This means that there should be consistency in storing and compressing of historical data. It might also be necessary that this information is available online.

**Evolving Management Models:**

New models of management can emerge wherein part of the service management is carried-out by the consumer himself , and some type of management information is shared or management is carried out by different external parties hosting the services.

**Creation of New Alarms:**

It is possible that SPM does some additional fault co-relation and wants to create a new alarm on the corresponding RTM. RTM should provide means to create such faults to the SPM.

**Protected Services:**

It might be necessary for the SPM to retrieve the managed elements that support protected services associated with a given protection group. RTM should provide means to retrieve such information to the SPM.

**Diagnostic Test capability:**

It might be necessary for the SPM to trigger certain diagnostic tests or retrieve the results of such a test triggered by the RTM on the managed elements. RTM should provide means to trigger such actions or retrieve such information to the SPM.

**Suspending/Resuming Alarm Surveillance:**

In certain scenarios when a particular service is faulty, for isolation of the problem it might be required that the SPM might want to request the RTM to stop/start alarm surveillance for a part of the network. The RTM should provide means to the SPM to make such requests.



**Auto-correction capabilities:**

With the advent of decision support systems and their use the fault management systems, there are some RTM solutions that now have the capability to take remedial actions on the occurrence of faults. However in certain scenarios the remedial action may not be the appropriate one from a service layer perspective. Since the remedial actions are defined in the resource layer, the service layer may not be aware of such faults as they are automatically corrected by the resource layer entities. Hence there is a need for the RTM to provide information about its auto-correction capabilities to the SPM. It should also be possible for the SPM to enable/disable some of these capabilities on the RTM.

**Reclassification of alarm severities:**

Network faults by nature have varying severities, however the severity assigned to a fault by the originator of the fault (typically the network resource itself) seldom captures the business impact of the fault. Hence it should be possible to re-classify the alarm severity at different levels. Say an RTM can with the help of inventory/topology information re-classify the fault from the network perspective, or a SPM can re-classify the fault based on the service criticality and the business impact of the service. RTMs should offer such capabilities to the SPM so that the fault severities can be reclassified.

**Multi-tenancy of RTM/SPM solutions:**

The cloud computing trend is fast catching up the telecom industry, mainly because of the huge CAPEX/OPEX savings that it promises. Most of the current RTM/SPM solutions are not inherently multi-tenant which implies that they cannot leverage on the benefits offered by a cloud paradigm (especially the PAAS/SAAS models). The interface between the RTM & SPM should also consider the multi-tenancy aspects i.e. it should be feasible for a SPM (with proper authorization) to access the faults belonging to the network of a particular operator. Security & data integrity are also vital aspects to be factored in evolution of such interfaces.

## Summary

In summary this document tries to highlight the fact that there is a need for changes in the standard FM solutions if it has to give full-fledged support to SM Layer entities.

From the requirements that are discussed in this document, it is evident that there is need for software blocks, which need to be added to standard solutions that exist today. Some of these software blocks can be added at DM level and some have to be implemented at SM&O level.

The communication and information model issues i.e. RM and SM interaction will also depend on the requirements from PM and CM.

## Appendix – Requirements to a Fault Management System

The considerations stated in this document impact the functionality of management entities at Resource Management level. The RM level management entities not only carryout their native functionality (i.e. from the resource management perspective) but also need to assist the service layer to carry out its functionality.

This appendix is a collection of requirements that can help choosing a fault management system. These can also be used as reference by architects/designers developing a new fault management system.

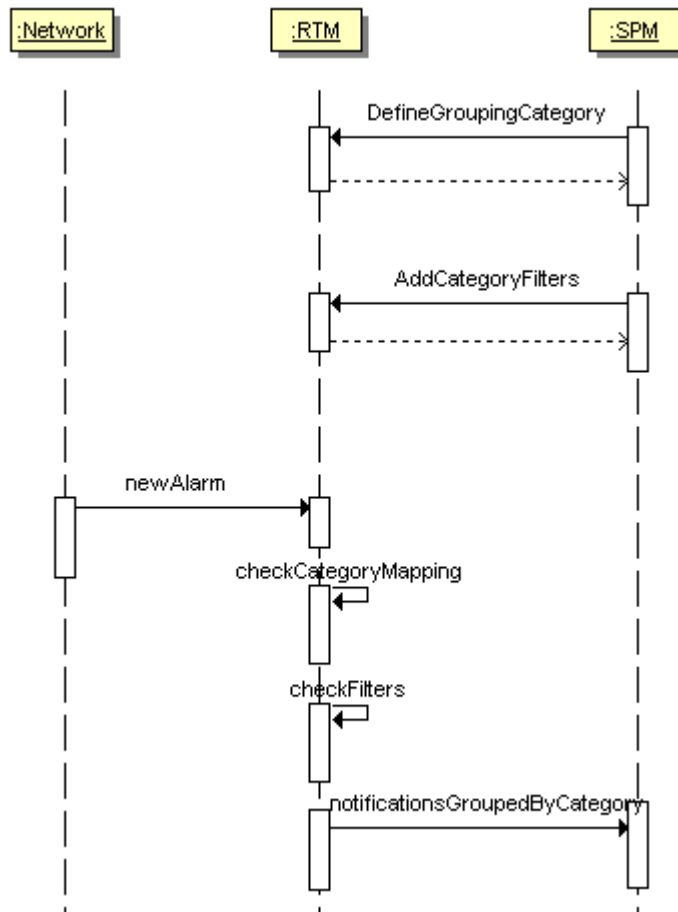
### ***Functional impacts***

Traditional FM solutions are deployed at sub-network management level or network management level in case it is a sort of “manager of managers” type of solution. The network was generally of one technology though it might be supplied in parts by different NEPs. In some cases they might be of different technologies, but from one domain (ex- wireless only).

Besides the earlier “Network is the service” concept meant that, FM solutions were basically built, for fulfilling network management/sub-network management requirements. The Service Management Layer function was not as important part (as it is today) and the support for it from the FM solutions was minimal. The dramatic changes being envisaged in near future due to the advent of next generation services, has propelled the Service Management Layer into prominence. Hence the FM solutions would not only have to work in a multi-domain environment but also be able to effectively support Service Management Function. The following are the new requirements for present day FM systems, based on the impacting considerations mentioned in the previous section. The current FM solutions may not be able to fulfill this due to the inherent constraints; however the requirements need to be fulfilled by the FM system as a whole. The requirements are in no particular order,

#### **Requirement FM\_FN\_001:**

It should be possible for the SPM to define alarm categorization rules on the RTM so that SPM is able to synchronize alarms related to a service.



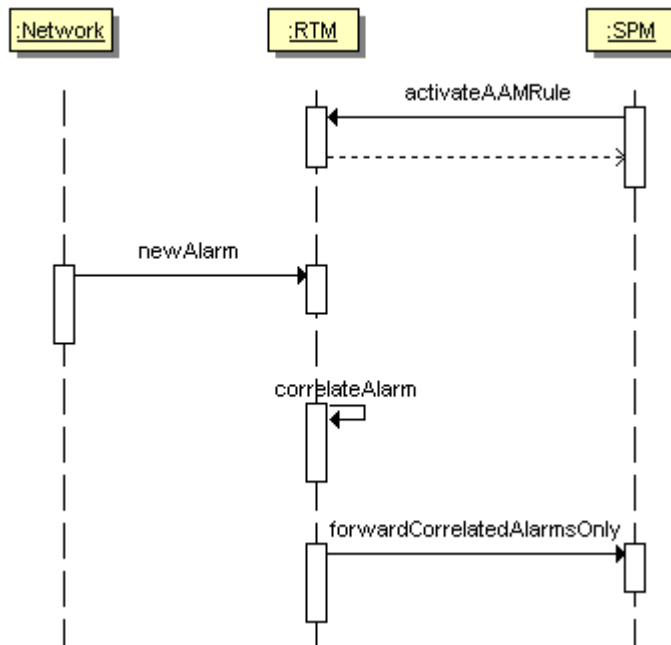
**Figure 3: Sequence diagram depicting how SPMs can define alarm grouping categories on RTMs.**

Most of the RTMs provide means to specify filters during alarm synchronization, however this is not sufficient for the SPMs as the Network Elements participating in a particular service do not necessarily qualify any filtering rules. If RTMs provide means for the SPM to define alarm categorization rules, then SPMs can specify such rules based on the service definitions on the SPMs.

Possible alarm categorization rule(s) may depend for example on the type of alarm, the environment, the time of day, the type of network element, the alarm severity, the location, position in the containment tree and many more.

#### **Requirement FM\_FN\_002:**

It should be possible for SPM to define the co-relation rules on the RTM system. This will help the SPM to define co-relations from a service perspective so that RTM system forwards alarms to the SPM system only if there is an impact to a service that it is interested in.



**Figure 4: Sequence diagram depicting activation of alarm correlation rules on RTM from a SPM.**

Since the RTM is not aware of the participating resources for a given service, currently the operator has to manually configure the co-relation rules in each of the RTM systems. Since the services offered by the operator itself are changing and evolving very often, such configuration should also adapt dynamically. This reduces the operational overhead to the operator and enables the operator to deploy new services easily. The other resource specific alarms that may not directly have an impact to a service as a whole can be filtered out in the RTM itself.

#### **Requirement FM\_FN\_003:**

It should be possible for the SPM to unambiguously correlate between the original alarm and its clear event, preferably using a single unique attribute of the event like notificationId

Currently available RTM systems use different identifiers (usually combination of attributes) to correlate between original alarm and its clear event. This imposes an overhead on the SPM to correlate alarms from different RTM using different techniques. This can be avoided if there is a unique and unambiguous identifier to correlate the original alarm with its clear event.

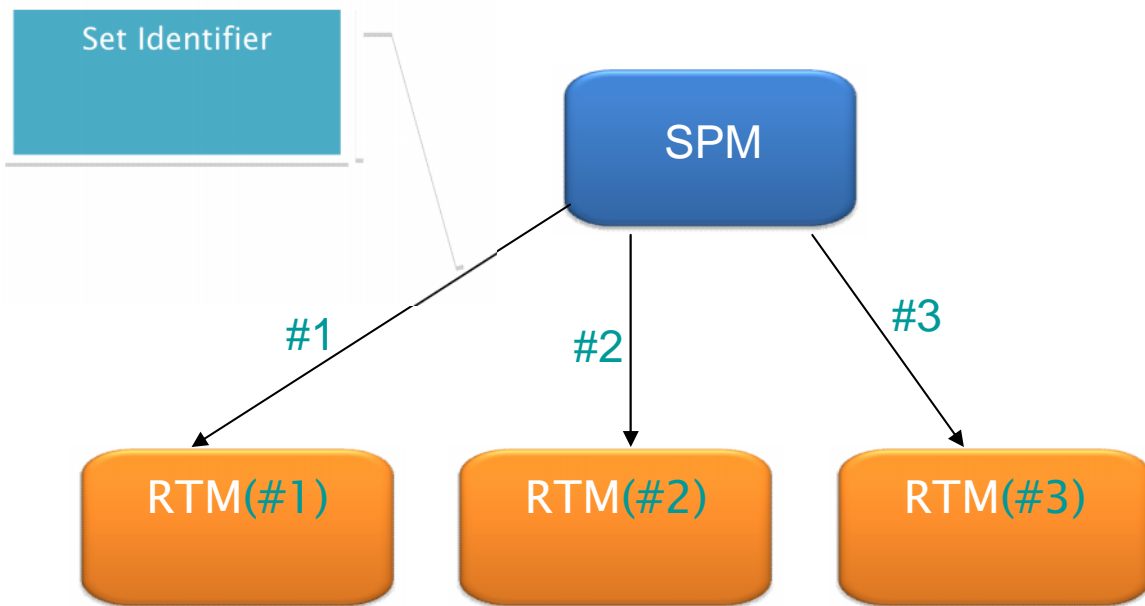
#### **Requirement FM\_FN\_004:**

It should be possible for the SPM to retrieve alarms from the RTM without any dependency on the availability of topology information in the RTM.

Most of the RTM solution available today, have a dependency on the availability of the topology information about the alarming objects. However, in certain scenarios it may be necessary to use an RTM solution with networks (or parts of networks) where the topology information is not available to the RTM. There might be a different inventory management solution in these scenarios and integration with the RTM may not be available. In order to ensure that all alarms from the network are available to the SPM, RTM should be able to operate without dependency on the availability of topology information.

#### **Requirement FM\_FN\_005:**

It should be possible for the SPM to configure the unique identifier of the RTM.

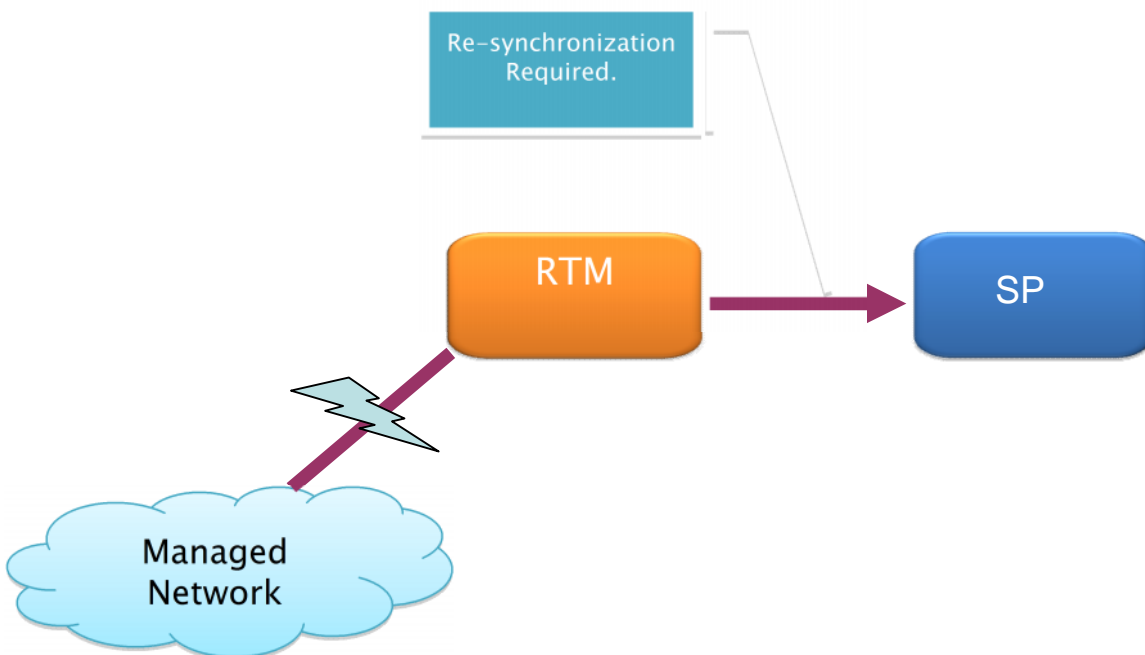


**Figure 5: SPM setting unique identifiers to RTMs in its domain.**

Typically, the RTM provide their identifier to the SPM when requested. However since SPMs might be connected to multiple RTM solutions, it is not possible for the RTM to provide a unique identifier within the scope of the SPM. Hence it should be possible for the SPM to configure such identifier on the RTM so that uniqueness of such identifier can be ensured by the SPM.

**Requirement FM\_FN\_006:**

It should be possible for the RTM to provide hints to SPM when an alarm synchronization is required.

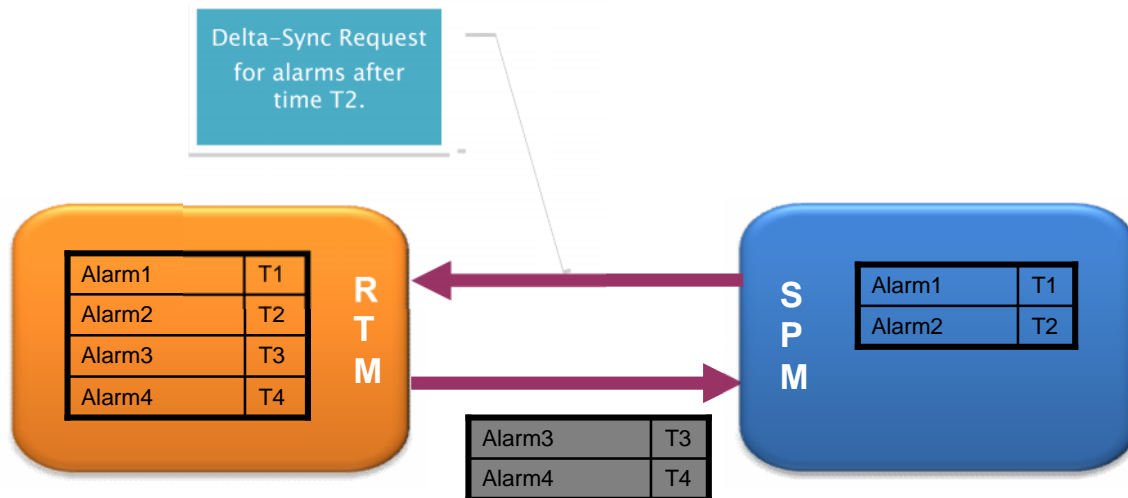


**Figure 6: RTM indicating to SPM the need for alarm re-synchronization because of a failure in network connectivity with a sub-network.**

Typically, RTMs provide an API to the SPM to trigger an alarm synchronization, however the decision when to trigger such a synchronization is left to the SPM. So usually whenever a network outage occurs etc, the SPMs trigger such synchronization which sometimes may not be required if there were no new alarms arriving during such outage. So apart from allowing the SPM to trigger an alarm synchronization, the RTM should also provide hints to the SPM wherever possible. Say if the RTM detects a faulty alarm list, or if it detects a loss and subsequent restoration of connection with SPM and finds that some of the alarms couldn't be forwarded to the SPM, it can provide hints to the SPM to perform an alarm synchronization.

**Requirement FM\_FN\_007:**

It should be possible for SPM to perform delta alarm synchronization with the RTM.



**Figure 7: Delta-synchronization of alarms between SPM & RTM.**

Usually alarm synchronizations are very time consuming mainly because of the volume of alarms in today's large networks. Often it is unnecessary as the result of synchronization could be just a few alarms. Considering that SPMs are dependant on multiple RTM solutions there may be scenarios where they have to perform alarm synchronization with multiple RTMs and this will be a very time consuming task. So RTMs should facilitate delta synchronization i.e. SPM can request for synchronization of only those alarms which have arrived after a particular instant of time. This will reduce the load on both the SPM as well as the RTM.

**Requirement FM\_FN\_008:**

It should be possible for RTM/SPM to indicate planned outage (say maintenance, out-of-service or new commissioning) of network resources.

There might be situations where a certain service may be temporarily disabled temporarily (say because of some billing system changes for that service etc). It should be possible for the SPM to indicate to the RTM about such outages so that RTM need not forward alarms from associated network elements to the SPM. Similarly there could be situations where there are certain maintenance activities or outages for the actual network resources. It should be possible for the RTM to indicate to the SPM that alarms from such objects are not going to be forwarded to the SPM for that duration.

**Requirement FM\_FN\_09:**

It should be possible for SPM to retrieve alarms which are cleared.

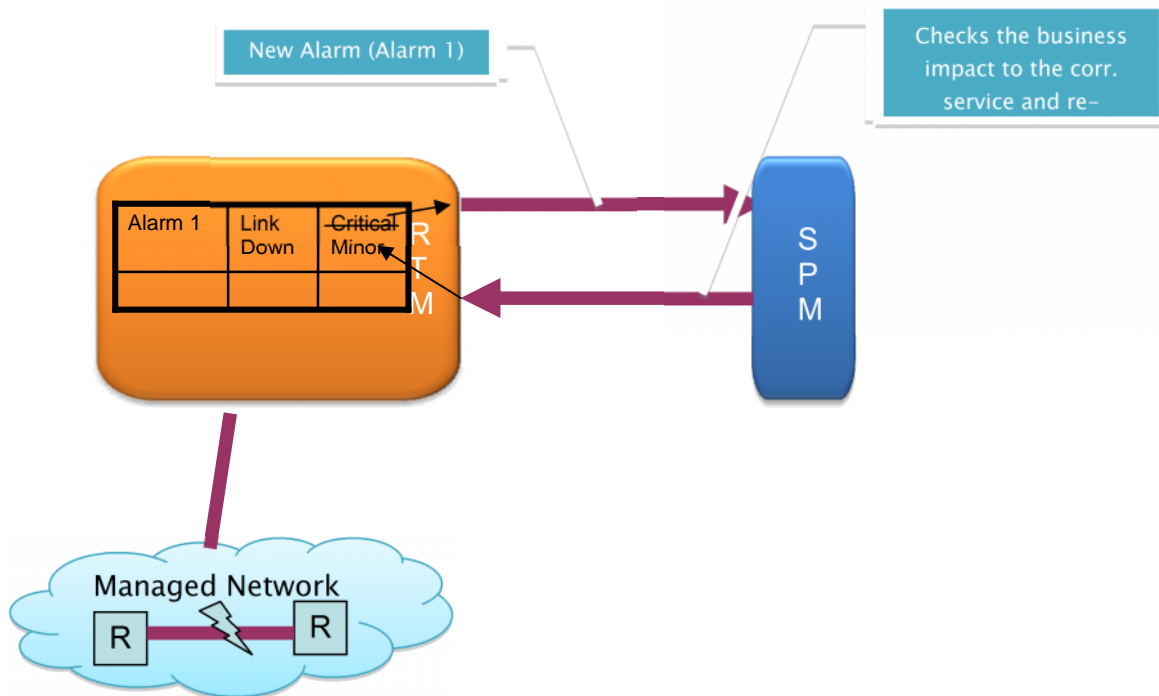
In today's networks SPM need to correlate alarms from multiple RTMs to find the root cause of a certain service fault. It is possible that some of the resource faults that effect the service fault might be cleared in the RTM. However the SPM might require information about such cleared faults also to perform root cause

analysis of the actual service fault. So the RTMs should facilitate retrieval of cleared alarms also to the SPM.

**Requirement FM\_FN\_010:**

It should be possible for SPM to re-classify the alarm severity.

Since SPMs have a service & business perspective of the managed network, using the information available at the Service Assurance function, SPM should be able to re-classify the severity of an alarm and inform the same to the RTM.



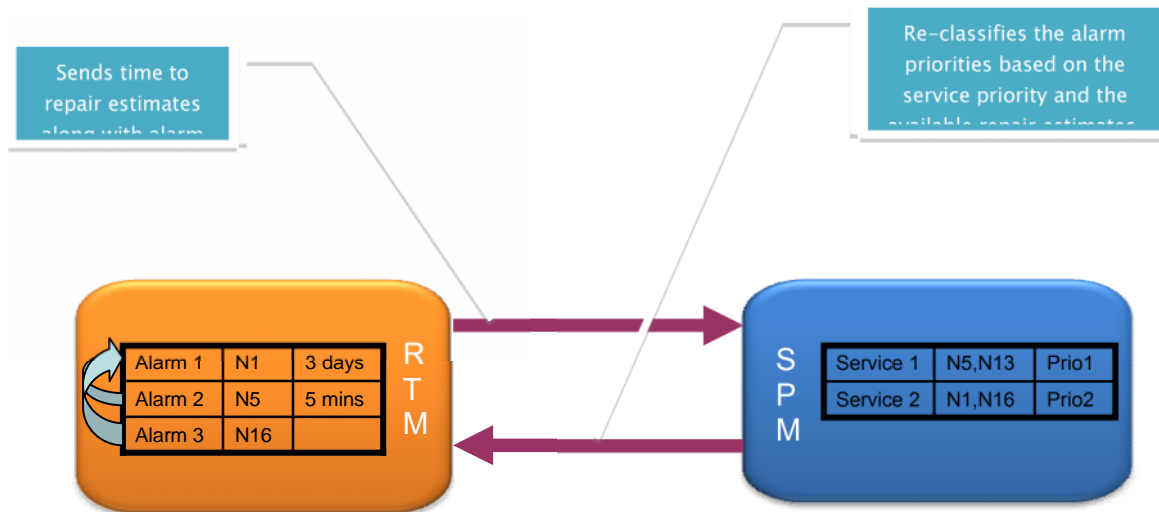
**Figure 8: SPM reclassifying the severity of an alarm.**

**Requirement FM\_FN\_010:**

It should be possible for RTM to inform SPM an estimate on the time needed to repair a fault whenever such information is available to RTM.

Let us consider the following example:





**Figure 9: SPM prioritizing the fault fixes based on the repair time estimates from RTM and the service priorities.**

Service 1 uses NEs N5,N7,N8,N10,N11,N13

Service 2 uses NEs N1,N9,N11,N17,N16,N13

Service 1 has priority over Service 2.

The RM&O has detected problem in NEs N5,N16

The RM&O RCA results in figuring out that N1 is actually root cause for N5 and N16 problem

Then what should actually happen is this

SM&O SLAM decides fixing N5 problem is higher priority than N1 and N16

It should get info from NMS/RM&O which says fixing N5 will not be sufficient N1 has to be fixed

SM&O decides to fix N1

(for the example we are assuming that all nodes can be switched some common backup node.)

There could be possibility that RM&O says that N1 is the root cause but fixing N1 will take 3 days, whereas N5 can have a temporary fix in 5 minutes and the fix will last for say 5 days. Then SM&O makes a decision to prioritize N5.

So the point is that not just alarms related to specific services should be available, but SM&O should let RM&O decide how to fix the problems. SM&O can not diagnose problems as effectively as RM&O (it has a technical point of view), but SM&O can decide (it has a commercial point of view), what is important and prioritize the fault fixes accordingly.

### Information Model

In future it is expected that there will be multiple sources supplying FM related information to the SM Layer entities. This is because the underlying networks can be multi-technology and multi-vendor networks. However the SM Layer should not have to make these distinctions. Hence the following requirements

#### Requirement FM\_IM\_001:

It should be possible to model the alarm as both an object on which conversation is possible (similar to the model adopted by MTOSI) as well as a simple notification mechanism (similar to the model used by 3GPP, X.733 etc)

Since the SPM can inter-work with multi-vendor RTM solutions such flexibility on the alarm model is required. This implies that the same SPM can work with a simple RTM solution that supports only

notification kind of mechanism and provides a get\_alarms kind of API; and also work with an RTM that allows viewing an alarm as an object and supports various operations on such object.

**Requirement FM\_IM\_002:**

It should be possible for the SPM to discover the RTM capabilities.

Since multiple alarm models are possible, the capabilities of RTMs could be different. So the RTMs should advertise their capabilities or provide such information when requested by the SPM. The SPM can then use the interface with the RTM accordingly.

**Requirement FM\_IM\_003:**

It should be possible for SPM to receive normalized probable cause details from RTM.

Probable cause provides further qualification to an alarm. It is very useful in understanding the reason for the alarm. However there are multiple standards existing currently that define different probable causes and hence different RTM solutions adopt different conventions. This makes it difficult for the SPM to identify the reason for a fault and thereby deduce the impact to a particular service. If the RTMs can provide normalized probable cause codes this will help the SPM can interpret the probable cause in a more consistent manner.

**Requirement FM\_IM\_004:**

The alarm model should have provision to accommodate attributes like the Trouble Ticket associated with the alarm etc.

Most of the Trouble/Problem Management systems are in-turn integrated with Trouble Ticketing systems. It is quite common that there is a trouble ticket created (manually or automatically) for each alarm or for a set of alarms. Having the trouble ticket association available in the fault management system (RTM & SPM) will enable the operators to easily check the actions being taken to recover from the fault using the trouble ticket association.

**Requirement FM\_IM\_005:**

It should be possible for SPM to receive notifications of maintenance mode state transitions of the alarming resources from the RTM.

Typically, the alarms raised when a resource is in maintenance mode are ignored. However, it is also important that the SPM is aware that a particular resource is in maintenance mode and hence no alarms are being notified during such period. This enables the SPM to understand the impacts to the associated services and act accordingly. Such transition of maintenance state can be indicated by a pre-defined notification/message format or a particular alarm can be agreed to indicate such a state transition.

**Requirement FM\_IM\_005:**

It should be possible to capture the perceived severity of the network as well as the severity from the service management perspective. Similarly the RTM should be able to provide an estimate of the repair time (whenever possible) along with the alarms. Such information will help SPM to determine the service/business impacts better.

The alarm data model usually contains only the perceived severity that represents the severity of the alarm as perceived by the originator of the alarm (say an EMS system that has detected a link loss with a resource). However, the Alarm data model should accommodate also the service/business severity of the alarm that is assigned by the SPM, this should be informed back to the RTM so that fault recovery is handled based on the service/business severity.

## Glossary

COTS – Commercial Off-the-Shelf

CM – Configuration Management

DM – Domain Manager is Sub-NMS which is aware of the presence of other sub-NMS and is geared up to support consolidated Network Management of the deployed Network.

FAB – Fulfillment, Assurance and Billing

FM – Fault Management

KPI – Key Performance Indicator

KQI – Key Quality Indicator

NE – Network Element

Frameworkx – New Generation OSS

PM- Performance Management.

PM MoM – Performance Management Manager of Managers

RM&O – Resource Management and Operations

SM – Service Management

SM&O – Service Management and Operations

Sub-NMS – Network manger which when deployed actually manages only part of the network (mostly because of mutli-vendor networks)

TMF – Telemanagement Forum

## References

[1]	3GPP TS 32.001: "Telecommunication management; Principles and high level requirements"
[2]	3GPP TS 32.111-2: "Alarm Integration Reference Point (IRP):Information Service (IS)"
[3]	3GPP TS 32.123: "Advanced Alarm Management (AAM) Integration Reference Point (IRP):Information Service (IS)"
[4]	3GPP TS 32.391: "Delta Synchronization Integration Reference Point (IRP): Information Service (IS)"
[5]	SLA Management Handbook, Volume 2, Concepts and Principles.
[6]	Telecom Interface Program - RESOURCE FM HARMONIZATION STUDY
[7]	TMF 518 : "Resource Trouble Management"

## About the Authors

**Raghavendra Tadepalli:**

Raghavendra Tadepalli is working as an Architect in Wipro Technologies Bangalore, India. He has OSS experience of over 7 years. The author can be contacted at: [raghav.rao@wipro.com](mailto:raghav.rao@wipro.com)

**Vinay Stephen Devadatta:**

Vinay Stephen Devadatta is working as a Principal Consultant in Wipro Technologies Bangalore, India. He has OSS experience of over 12 years. The author can be contacted at: [vinay.devadatta@wipro.com](mailto:vinay.devadatta@wipro.com)

## **About Wipro Technologies**

Wipro is the first PCMM Level 5 and SEI CMMi Level 5 certified IT Services Company globally. Wipro provides comprehensive IT solutions and services (including systems integration, IS outsourcing, package implementation, software application development and maintenance) and Research & Development services (hardware and software design, development and implementation) to corporations globally.

Wipro's unique value proposition is further delivered through our pioneering Offshore Outsourcing Model and stringent Quality Processes of SEI and Six Sigma.

## **Wipro in Telecom**

Wipro Technologies offers world class software and technology solutions for the telecom industry. Wipro has successfully executed several projects handling end-to-end program management for key telecom OSS/BSS products, provided new software modules and customizations as desired by the telecom vendors and service providers. Wipro's unique value proposition is delivered through our pioneering Offshore Development Model and stringent Quality Processes including ISO 9000, SEI CMM Level 5 and Six Sigma.

© Copyright 2009, Wipro Technologies, No part of the whitepaper may be reproduced in whole or in part without the written permission of the authors. All other trademarks mentioned herein are the property of their respective owners. Specifications are subject to change without notice.