3GPP TR 32.832 V10.0.0 (2011-03)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Study on Alarm Correlation and Alarm Root Cause Analysis (Release 10)

Keywords
Alarm, OAM

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Background and Objective

In a network, such as a convergent network, a single network fault (e.g. an entity under management is not performing at service level as expected by network operator) may result in the generation of multiple alarms from affected entities over times and spread over a wide geographical area. It is imperative that the network operator, the receiver of all the generated alarms, be able to evaluate the received alarms to identify the entity having the network fault.

Rapid and accurate determination of faulty entity will shorten the time to repair, and thus have direct positive impact in OPEX reduction and indirectly, facilitate the support of service contracts, between operators (providers of service) and service consumers.

It is noted that alarm correlation and alarm root cause are considered as important features of convergent network management, see [6].

The objectives of this study are:

1. Identify and define the management services offered by alarm correlation (AC) process and alarm root cause analysis (ARCA) process;
2. Identify the benefits of the AC process and ARCA process from views of network operators.
3. Identify the possible locations of the AC and ARCA processes within the IRP framework.
4. Identify possible IRP standard solutions, including enhancement of existing IRP standard solutions, that can offered the services identified in bullet 1.

1 Scope

The present document:

- defines the management services offered by Alarm Correlation (AC) process and alarm root cause analysis (ARCA) process;
- Identifies the benefits of the AC process and ARCA process from views of network operators;
- Identifies the possible locations of the AC and ARCA processes within the IRP framework.
- Identifies possible IRP standard solutions, including enhancement of existing IRP standard solutions.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP Work Item Description "WID Study on Alarm Correlation and Alarm Root Cause Analysis" UID_480045

[3] 3GPP TS 32.111-2 Alarm IRP: IS

[4] ISO 7498-1 Information Technology – Open Systems Interconnection – Basic Reference Model: the Basic Model

[5] 3GPP TS 32.122 Advanced Alarm Management (AAM): IS

[6] S5-101174 "Operator Common NGMN TOP 10 Requirements" [7]3GPP TS 32.302 Notification IRP: IS

[8] 3GPP TS 32.40x Performance measurements series

[9] 3GPP TS 32.342 Notification Log IRP: iS

[10] 3GPP TR 32.829: "Alignment of 3GPP Alarm IRP and TMF TIP FM".

[11] 3GPP TS 32.101 Principles and high level requirements

[12] 3GPP TS 32.752 Evolved Packet Core (EPC) NRM IRP; IS

[13] 3GPP TS 32.300 Name convention for Managed Objects

[14] 3GPP TS 32.362 Entry Point IRP: IS

[15] 3GPP TS 32.622 Generic network resources IRP; NRM

[16] 3GPP TS 32.662 Kernel Configuration Management IRP: IS

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

AlarmList: A record of active alarms (i.e. alarms that are not yet cleared) and non-active alarms (i.e. alarms that are cleared but not yet acknowledged by operator) (see 5.3.2 of [3]).

NotificationLog: A record (see 3.5.2 of [9]) of notifications that were emitted by NotificationIRP (see [7]).

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AAM	Advanced Alarming Management
AC	Alarm correlation
CM	Configuration Management
DN	Distinguished Name
FMC	Fixed Mobile Convergence
IRP	Integration Reference Point
IS	Information Service
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector
NE	Network Element
OPEX	Operating Expenditures
OSI	Open Systems Interconnection
MIB	Management Information Base
NRM	Network Resource Model
PM	Performance Management
RC	Root Cause
RCA	RC Analysis
SOA	Service Oriented Architecture
SS	Solution Set
TTR	Time To Repair

4 Context

3GPP currently have published two specifications that deal with alarm management [3, 5]. The former [3] specifies a capability that focuses on the collection (in the `AlarmList`), distribution and management of the alarms reported by various network elements (NEs). The latter [5] specifies a capability whereby the reported alarms can be categorized, based on IRPManager's rules. The goal for categorization is that IRPManager can decide which categories of alarms should be in the `AlarmList`, and which ones should not.

It is not atypical, using Alarm IRP [3], that the `AlarmList` would have recorded some 20,000 alarms per day in 2G network and 40,000 alarms per day for a 3G network. Using AAM IRP [5] should reduce those numbers but there is no field experience of AAM IRP that can confirm the reduction numbers yet.

As discussed in [6], the sheer alarm volume (not referring to the case of alarm storms) and the low quality (in terms of readily useful information conveyed in alarm records) would require longer operator's alarm processing time. This would result in longer Time to Repair (TTR) and consequently, would increase OPEX and could lead to loss of customers' satisfaction.

To improve the situation, [6] asks for a) higher quality of information carried in alarms and b) use of alarm correlation and root cause analysis techniques.

The WID [2] scope, and thus this Study, specifically focuses on b).

This Study would expand the intended scope and examine if it is useful and feasible to correlate, in addition of alarms, network configuration changes data.

5 Concepts

5.1 Definitions

5.1.1 Alarm Correlation (AC)

There are two concepts/definitions of Alarm Correlation (AC) used in this study.

5.1.1.1 AC1

A single network fault may result in the generation of multiple alarms from affected entities over times and spread over a wide geographical area. The corresponding definition of AC is as follows.

> *Alarms are correlated and partitioned, in view of certain rules such as alarm propagation path, specific geographical area or equipments, repeated alarms from same source into sets where alarms within one set have a high probability of being caused by the same network fault.*
>
> *The correlation is relations between network events (e.g. current alarms as those captured in AlarmList, historical alarms as those captured in NotificationLog, network configuration changes, etc. However, at least one member of the correlated set is an alarm.) In this study, we label this correlation usage, AC1.*

5.1.1.2 AC2

Not all alarms are equal in terms of their impact to (operator's) delivered services and revenue. (Note that the alarm severity parameter of alarm record (see `AlarmInformation` of [3]) does not indicate such impact.) The corresponding definition of AC is as follows.

> *Alarms are prioritised in relation to its impact to delivered services and/or revenue. The rules to prioritize alarms can be based on, but not limited to, the following: Number of affected subscribers, Number of affected sites, Importance of affected subscribers (e.g. Gold) and Importance of affected site (e.g. holding special event).*
>
> *The correlation is a relation between an alarm and the "delivered services and/or revenue". In this study, we label this correlation usage, AC2*

Note: The term 'rule' used here has the same meaning as that used in [5] where three specific Rules were defined, i.e. threshold rule, transient rule and toggle rule.

Note: The term correlation in this document does not refer to the act of relating an alarm raising event with its corresponding ceasing event.

5.1.2 Root Cause Analysis (RCA)

There is one concepts/definition of Root Cause Analysis (RCA) used in this study.

> *RCA is a process that can determine and identify the network condition (e.g. fault, misconfiguration) causing the alarms. The determination can be based on the following:*
>
> - *Information carried in alarm(s);*
> - *Information carried in correlated alarm sets (see AC1);*
> - *Information carried in network notifications;*
> - *Network configuration information;*
> - *Operators' network management experience;*
> - *etc...*

5.2 Alarm propagation path

Communication protocols operate in stacks, see e.g. the generic seven-layered model of network architecture defined by ISO [4]. According to such protocol stack architecture, a protocol operates along a layer, where protocol end-points are terminated at designated network nodes. End point of a protocol layer provides the protocol specific communication service (e.g. a reliable sequenced transfer of packet of information) to its higher layer inside the same node. The higher layer, using the provided service, operates another protocol via its end-point with other nodes of the same layer.

An alarm (say Alarm#1 of the figure below) may occur in any of the nodes (say A1) and in any of the protocol layers. An alarm in one protocol layer at a given node will result in disturbance of the services provided to the layer above (say A2), that in turn reports an alarm (say Alarm#2). We call this the "vertical propagation of alarm" (or propagation inside the node).

Due to the disturbance of the lower layer services there will be disturbance in the protocol operation of the upper layer of the same node. That disturbance will impact its peer node (say Z2) where the other end of the upper layer protocol is terminated. The peer node would report an alarm (say Alarm#3). We call this the "horizontal propagation of alarm" (or propagation between nodes).

The following figure uses a two-layered protocol architecture to illustrate the idea of "propagation of alarm".

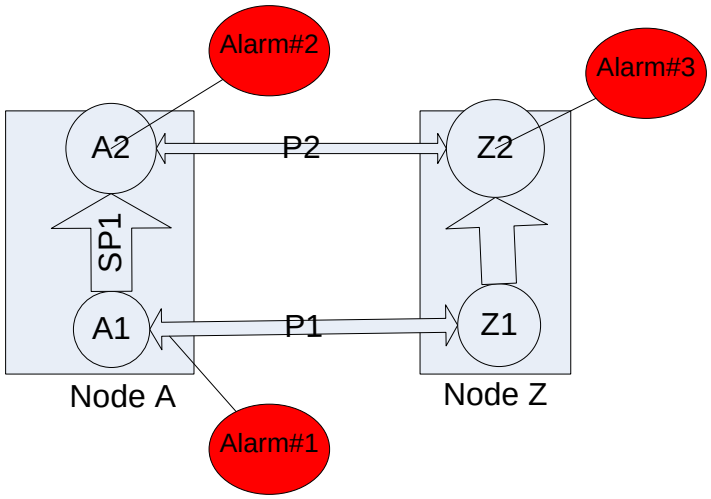

Figure 1: Alarm propagation

There are 2 nodes in the above figure. The circles represent various protocol end-points. Two protocols (P1, P2) are being operated by the 4 end-points of the two nodes.

The P1 specific communication service provided by endpoints of protocol P1 is denoted with SP1. Using that service, the upper layer endpoints A2 (and Z2) operate their own protocol P2 and provide the P2 specific communication service (not shown in the diagram) to their higher layers.

The A1 endpoint operates P1 to provide its services SP1. Suppose there is a failure in P1. Then the A1 endpoint reports the alarm (say, Alarm#1). A P1 failure would result in disturbance (failure) of service SP1. Endpoint A2 will notice the disturbance of SP1 and may report an alarm (alarm#2). This is an example of vertical propagation of failure.

The endpoints A2 (and Z2), while consuming the service SP1, operate protocol P2. A disturbance of service SP1 would impact the ability of A2 to operate and maintain P2 in normal mode of operation. Z2 would notice the abnormal mode of operation of P2 and may report an alarm (Alarm#3). This is an example of horizontal propagation of failure.

In the above figure, Z1 can also notice (and report a corresponding alarm) the failure of P1, which will subsequently disturb its service provided to Z2. In the above configuration, there are two alarm propagation paths to Z2, i.e. A1 to A2 to Z2 and A1 to Z1 to Z2.

In the figure below, where one or more intermediate nodes such as Node X, are involved, there may be some differences in the alarm propagation path. For example, Z1 may neither notice nor experience any failure of its P1 protocol connection when a failure occurs at endpoint A1. (Note that whether a local endpoint can detect failures at a

remote link is dependent on the particular protocol in question.) Therefore, in this example there may be only one alarm propagation path to Z2, i.e. A1 to A2 to Z2.

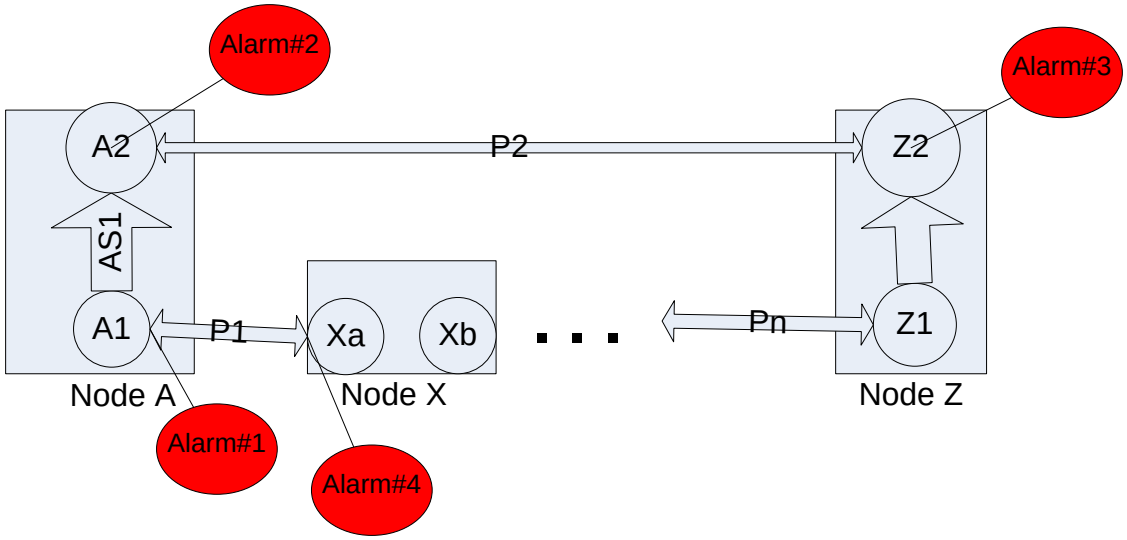

Figure 2: Example alarm propagation when transit node is involved

5.3 Use of CM data

The alarm propagation paths (such as the ones shown in subclause 5.2) are determined by the configuration of the network. If function-a has no relation with function-b (e.g., one is not serving the other, one is not exchanging messages with the other), then alarms in function-a would not be propagated to function-b.

To determine if two alarms are correlated by alarm propagation paths, one must know the relation, if any, between the two alarmed resources. Alarm (alarm record) carries the identity of the alarmed resource plus other information but it does not carry the identities of related resources.

To find the 'relation', one must rely on the configuration data of the network. In the IRP framework, this means one needs to have access to the MIB (see [15] for definition of MIB] of the network under management.

Alarm propagation paths are determined by the configuration of the network. A MIB is the representation of the configured network. The success of alarm correlation algorithm, using alarm propagation paths, would therefore, depend on the accuracy and details on the information in the MIB.

5.4 Use of PM data

Often, the root cause of a set of alarms can be traced back to NE drop of performance. In the IRP framework, performance data are carried in PM files [8].

Network performance drop can generate alarms. To assist correlation of alarms of such type, the alarm records should carry the causation, i.e. the 'bad' performance measurement or data.

In this document, the candidates that are subject for correlation are not restricted to alarm information, but also include PM data.

5.5 Use of notification data

Often, the root cause of a set of alarms can be traced back to NE configuration changes, e.g. wrong data entered into a routing table, wrong patches applied, planned outage, etc. In the IRP framework, configuration change information is carried by notifications such as notifyObjectCreation, notifyObjectDeletion and notifyAttributeValueChange [16].

In this document, the candidates that are subject for correlation are not restricted to alarm information, but also include notification data.

6 Benefits

6.1 AC1

This clause lists the benefits of AC1.

AC1 allows operator to view alarms in groups (called AC1 groupings) where alarms of the same group would have been caused, most probably, by the same fault. The benefits of using this type of grouping, as opposed to other types (grouped by network regions; by alarm raised times; by `perceivedSeverity` level), for viewing alarms are:

a) Viewing alarms in one AC1 group (instead of viewing alarms individually) can provide operator hints that can result in faster and accurate courses of action to verify and confirm the NE fault (so repair action can be initiated).

b) When operators are assigned to work on alarms that are not grouped or grouped by non-AC1 method, there is a risk of assigning operators to work on alarms that lead to the same NE fault, thus wasting effort. For example, operator-A is assigned to work on alarm-A and operator-B is assigned to work on alarm-B and it may turn out that both alarm-A and alarm-B are caused by the same NE fault. One operator's effort is wasted. This type of assignment (and therefore, wasting effort) would not occur if AC1 process place alarm-A and alarm-B in the same group.

c) When viewing large volume of alarms in AC1 groups, the operator can easily spot the small groups (or alarms not belonging to any group) that might be just important, in terms of impact to network operations, for example.

d) TTR has two components – a) the duration between reception of alarms and identification of the NE fault causing the alarm and b) the duration of a repair action. The latter component is fixed. The AC1 can reduce the former component (see a), thus shortening TTR. Short TTR decreases OPEX. Short TTR increases customer's satisfaction.

6.2 AC2

This clause lists the benefits of AC2.

a) The `perceivedSeverity` of an alarm record is decided by the NE reporting the alarm. This signals the NE's relative (in) ability to function as planned. It does not signal the relative impact to operator's service offerings (to paying customers, for example). Prioritization of repair actions, based on `perceivedSeverity`, can be detrimental such as in this case: to repair an NE that has a critical `perceivedSeverity` but carrying no customer traffic, at the expense of repairing another NE who has a major `perceivedSeverity` but carrying traffic of a customer that has a large penalty clause in the service contract. AC2 is best for prioritization of repair actions when achieving customer's satisfaction is the goal.

Example 1: NE-1 has a (main) power unit and a battery back up power unit. NE-2 has a power unit and no back up power unit. NE-1 main power unit has an alarm-1. NE-2 power unit has an alarm-2. Alarm-2 would indicate a higher priority level because it potentially can disrupt (if not already disrupting) users' traffic.

Example 2: An E1 circuit is in operational state and has an alarm. An E3 circuit (a higher capacity circuit but is not related to or supporting the alarmed E1 circuit) is not in operational state and has an alarm. The E1 circuit alarm would indicate a higher priority level because it can carry (if not already carrying) user's traffic.

Example 3: HNB-1 is configured to support a "Gold Tier Configuration" while HNB-2 is supporting an "Entry level Tier Configuration". The two HNBs reported alarms of the same type. The HNB-1 alarm would indicate a higher priority level because it is supporting a "more value" customer.

6.3 RCA

This clause lists the benefits of RCA.

a) Operator can focus the repair actions at root causes (sometimes, referred to as primary alarms) as opposed to addressing the 'symptoms' (secondary alarms).

b) Short TTR depends on accurate identification of root causes of problems.

7 AC-RCA management services

7.1 Requirements

Reference [6] clause 1 describes the benefits and Requirements of "Quality and quantity of Alarms". Its expectation is summarized by the following quoted text:

"Well designed alarm concepts for the overall product minimize the number of service outages and in case of failure the time back to service. Network operator's loss of market image and a loss in revenue can be minimized extensively. The alarm concept needs to be provided as part of the product and should not be project specific.

Good alarm quality and a minimum quantity of alarms reduce operational costs significantly. Without appropriate correlation and meaningful alarms, complex networks are no longer manageable in centralized network operations centers."

7.2 Current IRP support

This clause examines the capability provided by the various IRPs today and identifies areas where improvements are needed to satisfy the reference [6] expectations (7.1).

7.2.1 Functional architecture

Reference [11] clause 5.1 lays out the Management reference model against which various IRP specifications were positioned (deployed). See Annex A for the reference model.

One specific IRP specification, namely the Notification IRP, is of particular interest for the subject study in that it carries alarms and configuration changes in near real-time. For example, multiple NEs can report alarms and configuration changes to one DM. Multiple DMs can relay the reported alarms and configuration changes to NM etc. This hierarchical information relay architecture is suitable (and is used for years in industry) to support relatively rapid information transfer from NE to NM via DM and at the same time, offering DM opportunity to perform some information filtering and/or correlation.

We do not see changes necessary for this architecture.

7.2.2 To express/capture alarm service impact and repair urgency/priority

Reference [6] Requirements make clear that it is important for readers (operators) of alarms to rapidly identify service affecting alarms (e.g. having significant service impact for customers). This allows operator to prioritize their repair actions given limited resources at any given time.

An NE knows if its resources are being used but it cannot know if it is being used by customers. Even if it knows that the failed resource is being used by a customer, it would not know if the failure is affecting a significant or insignificant portion of the total customer's expected service. Also, it would not know if the affected customer is of Gold-type. One technical standard solution is for IRPManager to provide such information after NE is on-line with the OAM network. For small devices such as Home NodeB, this is a technical viable solution. For a small device, in many situations, IRPManager can know that it is exclusively used by a Gold-type customer and therefore, can configure the device on-line that its alarms would carry a higher severity level indication. See example 3 of clause 6.2.

This technical solution would not be suitable for 'larger' device that can support multiple services for large number of subscribers at the same time. Note that we make a distinction between

a) knowing if the alarmed resource can potentially support lots of customers' traffic and

b) knowing if the alarmed resource is currently affecting Gold-type customers' traffic.

The `AlarmInformation` attribute supports the operator on bullet-a above since it carries the alarmed resource identity and `specificProblem`.

The AlarmInformation attribute does not support the operator on bullet-b.

To provide a solution to support bullet-b above, we don't recommend adding new attributes or changing semantics of attributes in AlarmInformation (e.g., not adding a new attribute carrying service-affecting-critical, service-affecting-minor type of values).

We recommend the use of AC2 (7.3.2) function service to satisfy this Requirement (bullet-b).

7.2.3 The correlatedNotification attribute

In principle, each layer (of the hierarchy of Management reference model of Annex A) can do filtering and correlation. In practice, their filtering and correlation work (usefulness) are restricted by their view/knowledge (e.g., a NE might not know its alarm-6 is related to configuration changes of its neighbor NE) and the requirement that it should emit notification rapidly (and therefore, not much time to do thorough correlation analysis).

The alarm notification, reported by a lower layer to a higher layer carries an AlarmInformation [3] structure. One attribute of AlarmInformation is the correlatedNotification attribute. This attribute allows NE and DM to embed/insert their individual alarm correlation result (called partial-correlation-result in this document), based on their knowledge of their local environment.

This partial-correlation-result, captured in a notification, is seen as an assistant (useful information) to its higher-layer correlation processes

The current definition of correlatedNotification serves its purpose, i.e. it carries the partial-correlation-result and serves as an assistant (useful information) to higher layer correlation process.

It is noted that this correlatedNotification captures notification ID, not alarm ID. Use of notification ID supports the use of configuration changed information, and not just alarm information, as candidates for correlation.

We see one change necessary for this definition of correlatedNotification. We need to clarify in the specification that the items identified as correlated by this attribute indicates the AC1 type of correlation, i.e. all items are highly probably caused by the same network fault. (Note: Current Alarm IRP IS [3] has such hint of usage/interpretation in clause 6.8.3.2 for notifyClearedAlarm.)

We do not need to change the syntax definition of this attribute.

7.2.4 The perceivedSeverity attribute

The perceivedSeverity of an alarm record (i.e., AlarmInformation) is decided by the NE reporting the alarm, most probably a design time decision. The level of perceivedSeverity used is to indicate the NE's relative (in)ability to function as planned. Its level does not indicate the relative impact to operator's service offerings (to paying customers, for example).

It is technically possible to standardize a mechanism for IRPManager at run time to configure alarms of certain class, or even of certain instances, to carry a certain perceivedSeverity level, to indicate "the relative impact to operator's service offerings (to paying customers, for example)". We think such scheme is not manageable given the size of the FMC network, the large capacity of a node (supporting many customers traffic) and the dynamic nature of the connections (at time-1, the link is supporting a Gold-type customer and at time-2, it is not). See more details in 7.2.2.

We understood the need, expressed as Requirement in [6], to capture the urgency level (say, level critical) indicating "significant service impact for customers". We recommend the use of AC2 (7.3.2) function service to satisfy this Requirement.

We recommend not modifying the usage and definition of perceivedSeverity attribute. We also recommend not standardizing an interface allowing IRPManager to configure perceivedSeverity levels at run time.

7.2.5 Unique identification of notification

In a large scale network, as in the case of FMC network, there will be tens of thousands of alarms originating entities and multiple alarm reporting/management systems (e.g. Alarm IRPAgent).

To apply AC1 or AC2 type of correlation in a high layer (in the context of the Management reference architecture of Annex A), it is necessary that the alarms would carry unique identifications, i.e. no one ID can refer to more than one alarm, e.g. one ID leads to identification of a NE-1 alarm and a NE-2 alarm.

To guarantee uniqueness, Alarm IRP [3] does not recommend the use of alarm ID for alarm identification. The alarm ID uniqueness scope is that of a particular AlarmList instance. Its scope does not cover all possible AlarmList instances in the network. In other words, there could exist an alarm in AlarmList-1 with alarm ID=6 while another alarm record in AlarmList-678 with alarm ID=6 as well.

Alarm IRP [3] uses a combination of 'source' and "notification ID" to guarantee network-wide uniqueness (see `correlatedNotification` of Annex B). The source carries the DN [13] of the NE originating the alarm notification. NE, when notifying the occurrence of an alarm, would capture its DN plus a notification ID in the alarm notification. NE is responsible for not reusing notification ID value.

Therefore, as long as the entities originating the alarm notifications never reuse the ID values and that all entities have a DN, the combination will guarantee uniqueness, i.e., the combination will always refer to one and never multiple notifications.

It is noted that a notification can carry alarm or configuration change information. So, using the `correlatedNotification` means that the correlated items are not necessarily alarms but can be configuration change information as well. This is an important and necessary feature since many alarms are caused not by another alarm, but possibly by some configuration changes (e.g. wrong version of software is activated). A correlation function needs to use notification ID to express such causation (i.e. an alarm is correlated with a configuration change). It is technically impossible for the correlation function to express such causation using alarm ID.

We recommend to continue using notification ID (and not alarm ID) for correlation purpose.

In the FMC network management context, we recommend to use the same `correlatedNotification` concept to

- Guarantee uniqueness (see Note) of notification identity and
- Allow correlation of notifications that are not just carrying alarm but also configuration changes.

NOTE: This guarantee has a pre-condition that the entity originating the alarms has a DN. In the FMC context, that would imply the name space for mobile resource and name space for mobile backhaul / backbone resources do not clash/overlap.

7.2.6 Precision of alarm reporting

Current alarm record carries an attribute called `objectInstance`. This is the DN of the alarmed resource and the class of resource is defined in one of the NRM IRP such as EPC NRM IRP [12]. Take MME as an example. The MME contains multiple components. Each component can generate alarms. But the components are not modeled in EPC NRM IRP [12] (only `MMEFunction` is modeled). When component-K or component-Y originates an alarm, the alarm would carry the MMEFunction DN and not that of component-K or component-Y. Receivers of this alarm cannot tell if component-K or component-Y is in alarm state. Lack of modeling of these components (of MME in this case) result in lack of precision in alarm reporting.

We recommend an investigation of using <<SupportIOC>> (see Note) to model these components, thus allowing more precision of standardized alarm reporting.

NOTE: <<SupportIOC>> is like <<InformationObjectClass>> except that its instances are not visible by Basic or Bulk CM IRPManager. Each <<SupportIOC>> instance has its own DN.

7.3 New services

7.3.1 AC1 function

The benefits of AC1 type of correlation is listed in 6.1. AC1 correlation result does not identify the alarm root cause but can provide strong hints of the identity of the alarm root cause.

We recommend the use of `correlatedNotification` attribute to capture this AC1 type correlation result (called partial-correlation-result). See 7.2.3 for more information.

To support a network wide AC1 type correlation, we recommend the use of a function, called AC1 Function. It can be modeled as AC1IRP, like other IRPs such as AlarmIRP [3], EPIRP [14]. Its inputs are active alarms in all AlarmList (that contains all active alarms), network configuration data (that provides information about alarm propagation paths) and notifications logged in all NotificationLog [9] (that contains all past notifications that carry alarms and notification changes). Its outputs are AC1 groups (see 6.1).

7.3.2 AC2 function

The benefits of AC2 type of correlation is listed in 6.2. AC2 correlation result does not provide hints of the identity of the alarm root cause. AC2 correlation result is used by operators to prioritize their repair actions.

Given a set of alarms, AC2 partitions the alarms into groups. Members of a group would share the same property. Operator specifies the property. Examples of property are:

- Number of affected sites over a certain number;
- Number of affected subscribers over a certain number;
- Affected site is designated as important (e.g. holding special event).

There is no pre-defined (standardized) priority level designation for groups. For example, standard would not define the first bullet above as most urgent group (i.e. alarms in that group needs to be resolved urgently) and the last bullet above as least urgent.

Operator defines (and knows the meaning of) the properties of various groups and therefore knows the relative repair action priority/urgency among groups.

To support a network wide AC2 type correlation, we recommend the use of a function, called AC2 Function. It can be modeled as AC2IRP. Its inputs are AlarmList and a list of property. Its outputs are AC2 groups where members of one group share the same property.

7.3.3 RCA function

RCA identifies the cause of a number of alarms. AC1 correlation result can provide hints of the cause of alarms (see 5.1.1.1).

It is noted that root cause may not be singular in that alarms can be caused by multiple causes. Furthermore, root cause may not be an alarm itself. It can be a configuration change gone wrong (e.g. wrong version of software is loaded into NE, wrong NE attribute values are configured).

We question the feasibility of using standardized pre-programmed rules for RCA function.

This document recommends:

- The use of experienced operator, knowledgeable of network configurations, network activities and NE peculiar behaviours, with hints from AC1 function outputs, to identify root cause of alarms.
- The use of AC1 function (see 7.3.1) to report the root cause of an AC1 Group (see 6.1), in case it identifies the root cause of the AC1 Group.

7.3.4 Location of functions

In current IRP framework, all IRPs, e.g. AlarmIRP, are name-contained by IRPAgent. This implies the IRPs are located below the Itf-N.

We would suggest the AC1IRP and AC2IRP not be name-contained by IRPAgent. This implies it does not have the restriction that they be operated below the Itf-N. For example, an AC1IRP can be operated above the Itf-N, in the NMS space.

8 Recommendations

Start a Release 10 Work Item (WI) on Alarm correlation and root cause analysis. This WI would produce Change Requests (CRs) to Alarm IRP series recommendations to include the following:

a) The Requirements, benefits, context and use cases of AC and RCA;

b) Clarification ofy the semantics of the `correlatedNotification` attributes. See 7.2.3.

c) The `AlarmInformation` attributes that can report the result of AC and/or RCA or can assist the tasks of AC and/or RCA. Note that the `AlarmInformation` class is defined in TS 32.111-2, Alarm IRP IS.

d) Operations and/or notifications via which operator can receive the results of AC and RCA;

e) The context, such as location within the IRP Framework, in which the AC and RCA can be deployed.

Annex A:
Management reference model

This is the Management reference model defined in [11]. It is included here for ease of reference.

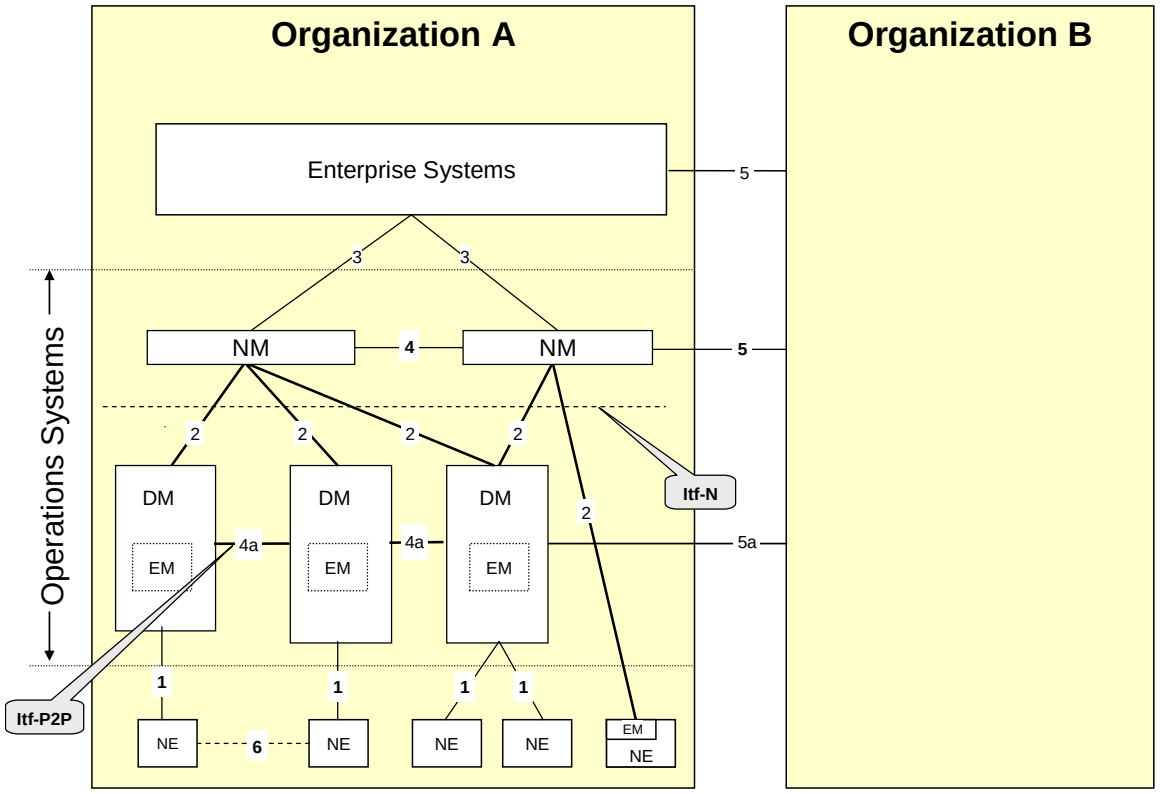

Figure 1: Management reference model

Annex B:
Parameter correlatedNotification

This attribute is defined in 3GPP TS 32.111-2 [3] and it is included here for ease of reference.

Quote:

5.3.5 CorrelatedNotification

5.3.5.1 Definition

It identifies one MonitoredEntity. For that MonitoredEntity identified, a set of notification identifiers is also identified. One or more CorrelatedNotification instances can be related to an AlarmInformation. In this case, the information of the AlarmInformation is said to be correlated to information carried in the notifications identified by the CorrelatedNotification instances. See further definition of correlated notification in ITU-T Recommendation X.733 [2], clause 8.1.2.9.

The meaning of correlation is dependent on the type of notification itself. See the comment column of the correlatedNotification input parameter for each type of notification, such as notifyNewAlarm.

Notification carries AlarmInformation. The AlarmInformation instances referred to by the correlatedNotification may or may not exist in the AlarmList. For example, the AlarmInformation carried by the identified notification may have been acknowledged and Cleared and therefore, no longer exist in the AlarmList.

5.3.5.2 Attribute

Attribute Name	Support Qualifier
source	M
notificationIdSet	M

Unquote.

Annex D:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2010-12	SP-50	SP-100771			Submitted to SA#50 for Information	0.3.0	1.0.0
2011-03	SP-51	SP-110124	--	--	Submitted to SA#51 for Approval	1.0.0	2.0.0
2011-03	--	--	--	--	Publication	2.0.0	10.0.0