3GPP TR 32.859 V2.0.0 (2013-09)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Telecommunication management;
Study on Alarm Management
(Release 12)

Keywords
Alarm management, OAM, Alarm definition

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 Report 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.

Introduction

The massive number and variety of network elements in a mobile system creates a huge amount of alarms, saturating the alarm management systems. In parallel the numbers of different types of alarms have increased to overwhelming proportions.

The network administrators are flooded with alarms and alarms often of poor quality. The consequences of bad quality alarms are severe, affecting many areas. Determining the service impacts of faults in the networks is an increasingly complex challenge for operators and requires good quality alarms.

The fault management area is well established in the telecom business; this technical report will explore the alarm information itself, target users, usage of information, mechanisms and processes to enhance usability of the alarm information.

The telecom alarm management experience described is shared in basically all areas of alarm management. Standardization bodies in the production and engineering fields (e.g. EEMUA [7], ANSI [6]) have addressed the problem and undertaken substantial work under last decade to come up with solutions.

The objective of this study is to analyse and secure applicability and impacts of the concept of alarm management in Telecom management. It is proposed to benefit from work in the production and engineering field, since the task of alarm management to a very high degree is independent of different businesses. It is a human-machine interaction.

This study also makes a shift in direction for Telecom management alarm standards, which historically have been focused on protocols and syntax for alarm parameters. In order to address the real problems, standards also need to focus on alarm quality and alarm semantics.

1 Scope

The scope of the present document is to improve the quality of alarms and enhance usability of alarm systems.

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 TS 32.101: "Principles and high level requirements".

[3] 3GPP TS 32.111-1: "Telecommunication management, Fault Management; Part 1: 3G fault management requirements".

[4] 3GPP TS 32.111-2: "Telecommunication management, Fault Management; Part 2: Alarm Integration Reference Point (IRP): Information Service (IS)".

[5] ITU-T M.3050.x series (2004): "Enhanced Telecom Operations Map (eTOM)".

[6] ANSI/ISA standard 18.2 -2009: "Management of Alarm Systems for the Process Industries ".

[7] EEMUA No 191 Edition 2 (2007): "Alarm Systems: A Guide to Design, Management and Procurement".

[8] ITU-T Recommendation X.733: "Information technology - Open Systems Interconnection - Systems Management: Alarm reporting function".

[9] Journal of Network and System Management (2009): "Chasing a Definition of "Alarm"", 17:457–481, Stefan Wallin.

[10] 12th IFIP/IEEE International Conference on Management of Multimedia and Mobile Networks and Services (2009), Stefan Wallin and Viktor Leijon, Telecom Network and Service Management: an Operator Survey.

[11] IEC 62682 Ed. 1: "Management of Alarm Systems for the Process Industries".

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].

alarm: TBD.

The following definitions are given in ANSI/ISA 18.2 [6]:

alarm management: The processes and practices for determining, documenting, designing, operating, monitoring and maintaining alarm systems.

alarm philosophy: A document that establishes the basic definitions, principles and processes to design, implement, and maintain an alarm system.

alarm system: The collection of hardware and software that detects an alarm state, communicates the indication of that state to the operator and records changes in the alarm state.

chattering alarm: An alarm that repeatedly transitions between the alarm state and the normal state in a short period of time.

eclipsing: Integrating repeated alarm in a single line

highly managed alarm: An alarm belonging to a class with more requirements than general alarms (e.g. a safety alarm).

nuisance alarm: An alarm that annunciates excessively, unnecessarily, or does not return to normal after the correct response is taken (e.g. chattering, fleeting, or stale alarms).

out-of-service: The state of an alarm during which the alarm indication is suppressed, typically manually, for reasons such as maintenance.

shedding: Activating predefined filter automatically in case of alarm flooding

shelve: A mechanism, typically initiated by the operator, to temporarily suppress an alarm.

suppress: Any mechanism to prevent the indication of the alarm to the operator when the base alarm condition is present (i.e., shelving, suppressed by design, out-of-service).

suppressed by design: A mechanism implemented within the alarm system that prevents the transmission of the alarm indication to the operator based on plant state or other conditions

stale alarm: An alarm that remains in the alarm state for an extended period of time (e.g. 24 hours).

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].

ADAC	Automatically Detected and Automatically Cleared
ADMC	Automatically Detected and Manually Cleared
AM	Alarm Management
ANSI	American National Standards Institute
CAPEX	Capital Expenditures
CPU	Central Processing Unit
EEMUA	Engineering Equipment and Materials Users's Association
eTOM	Enhanced Telecom Operations Map
FM	Fault Management
HMA	Highly Managed Alarms
HMI	Human-Machine Interface
IRP	Integration Reference Point
IS	Information Service
ISA	International Society of Automation
ITU	International Telecommunication Union
OPEX	Operating Expenditures
OS	Operations System
QOS	Quality Of Service
SNMP	Simple Network Management Protocol
TR	Technical Report

4 Rationale for the Study on Alarm Management

The massive amount of network elements in a mobile system and the variety of network elements and infrastructure equipment creates huge amount of alarms saturating operators alarm management systems. In parallel the numbers of types of alarms have increased to overwhelming proportions.

Major mobility network incident management centre can count alarms in the hundreds of thousands a day, with thousands of different types of alarms.. Findings from independent researchers [9] are frightening:

- > 80 % of all alarm types results in a trouble ticket less than once every 1 000 alarms
- > 90 % of all tickets are from the < 30 most common alarm types
- The alarm severity levels have no correlation to the real priority as judged by the network administrators

The majority of the alarms should never have been presented for the network administrators.

The fundamental problem is that the network administrators are flooded with alarms and alarms often with poor quality.

In many cases general events and log messages go into the alarm system.

Poor quality in this context can include:

- Nuisance alarms (repeating and fleeting alarms, redundant and cascading alarms)
- Stale alarms
- Alarm floods
- Alarms without response
- Alarms with the wrong priority
- Out-of-Service alarms
- Redundant alarms
- Events and log messages that should not have been alarms

Status of the alarm management environment

- Too many alarms occurring. Vastly over alarmed systems producing far more alarms to the operator than needed
- Too high proportion of them is nuisance alarms of little operational relevance
- The majority of the alarms should never have been presented for the network administrators!

The consequences of bad quality alarms are severe, affecting many areas. A few examples

- Too much time and resources are spent to define alarms as irrelevant – most of the alarms are now irrelevant!
- Alarm flooding add complexity in fault resolution activities and thereby delays
- Contributing factor to the seriousness of major incidents caused by delayed service impacts analysis
- Current quality of alarm severities, as set by equipment, are misleading and have a negative effect on the network service
- Operators may neglect important alarms caused by not understandable alarm information to respond to the alarm
- Significantly overstaffed network management centre and increased human resources allocated in the assurance processes
- General bad engineering – OS systems& staff have to cope with poor quality data
- Poor alarm management is a major barrier to reaching operational excellence, a business risk

- Unnecessarily complex and costly OSS solutions that have not supported a service and customer oriented approach at desired degree (CAPEX driver)

- Contributing factor to low success rate of alarm correlation tools in telecom. None will cure fundamental faults in the basic alarm system as poor quality alarms

- Bad alarm data quality is a significant, every day, cost driver (OPEX driver).

The telecom alarm management experience is shared in basically all areas of alarm management. The incitements to resolve the alarm management problems have been more obviously in other areas as in the production and engineering field.

The very same issues presented above are often cited as contributing factors in industrial major incidents as Milford Haven, Three Mile Island, Chernobyl, BP explosion, major power grid failures - to name a few. The alarm management systems have recorded alarm for hours but the fault resolution was delayed and understanding of the basic problem was drowned in the amount of alarms.

Standardization bodies in the production and engineering fields (e.g. EEMUA, ANSI) have addressed the problem and undertaken substantial work under last decade to come up with solutions. Solutions are reported to be adopted by industry, insurance and regulatory bodies.

Alarm management in telecom is obviously an overlooked and immature area that needs to change.

3GPP has a unique opportunity to address these problems, since 3GPP has all experts available in the definition of a mobile system including Telecom Management. This TR will elaborate and analyse this escalating and severe problem, propose solutions to share guidelines and mandatory requirements with the network element specifying groups.

5 Fault Management

The standardisation objectives for 3GPP Fault management are defined in 3GPP TS 32.101 [3]. In the context of this technical report the following identified purpose is in focus:

The purpose of FM is to detect failures as soon as they occur and to limit their effects on the network Quality of Service (QOS) as far as possible.

The standardisation objectives:

- Detect failures in the network as soon as they occur and alert the operating personnel as fast as possible.

The detailed 3GPP specifications in the area of Fault Management are found in the TS32.111-* series.

For fault detection the following information is presented in TS32.111-1 [5]:

For each fault, the fault detection process shall supply the following information:

- the device/resource/file/functionality/smallest replaceable unit as follows:

- for hardware faults, the smallest replaceable unit that is faulty;

- for software faults, the affected software component, e.g. corrupted file(s) or databases or software code;

- for functional faults, the affected functionality;

- for faults caused by overload, information on the reason for the overload;

- for all the above faults, wherever applicable, an indication of the physical and logical resources that are affected by the fault if applicable, a description of the loss of capability of the affected resource.

- the type of the fault (communication, environmental, equipment, processing error, QoS) according to ITU T Recommendation X.733 [8];

- the severity of the fault (indeterminate, warning, minor, major, critical), as defined in ITU T Recommendation X.733 [8];

- the probable cause of the fault;

- the time at which the fault was detected in the faulty network entity;
- the nature of the fault, e.g. ADAC or ADMC;
- any other information that helps understanding the cause and the location of the abnormal situation (system/implementation specific).

For some faults, additional means, such as test and diagnosis features, may be necessary in order to obtain the required level of detail.

The term "alarm" is defined as "abnormal network entity condition, which categorizes an event as a fault".

6 Alarm surveillance

6.1 Introduction

Alarm management and alarm systems have been a basic necessity for managing mobile telecom networks from its very start. Alarm surveillance is the prime alerting functionality for the assurance processes. Network operators need to act prompt on service impact failures in their networks. 3GPP has adopted the TM Forum eTOM processes for a common understanding of operator's way of working. The figure below is presented in TS 32.101 [2]. The terms "Detect fault" can be treated as equivalent to the concept of alarm surveillance.

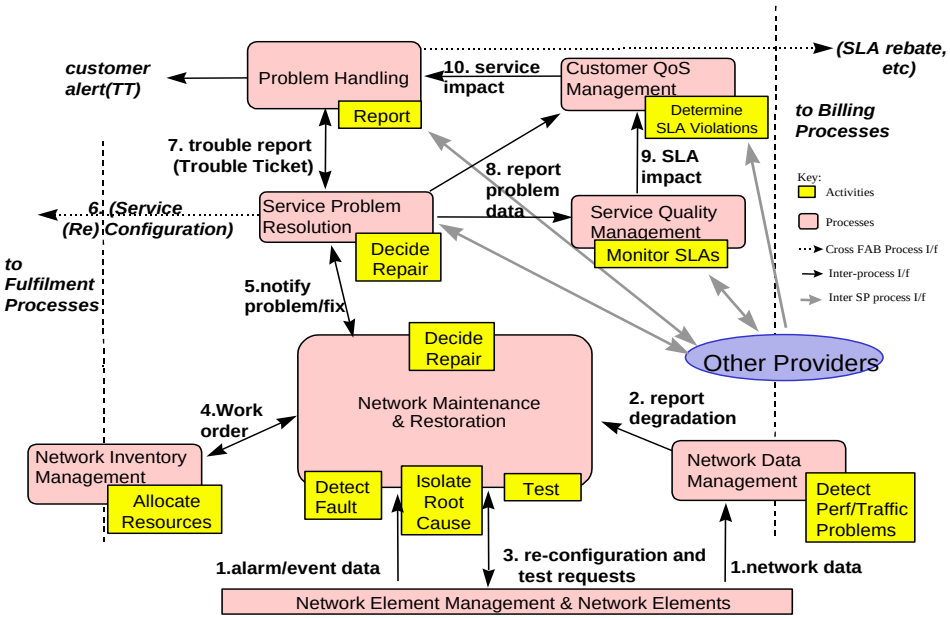


Figure 1

Implemented processes are the choice of operators and not target for 3GPP standardisation.

6.2 The surveillance vision

The very essence of the surveillance functionality is to alert the operator when incidents appear in out networks. This is a human-machine interface and a common expectation is that operators should never overlook important alarms. To be able to fulfil such request the goal must be to monitor only necessary alarms at the right time by extracting the ones needed. The vision is:

- Few alarms.
- Clearly prioritized and presented to the operator.
- Each with a needed action.

- Each action is taken.
- Alarms aid the operator in an upset.
- The system is monitored so performance is maintained.

The reality in our complex networks with the variety of network elements and infrastructure equipment is nearly the reverse. Huge amount of alarms are saturating the alarm management systems. In parallel the numbers of types of alarm have increased to overwhelming proportions. The quality of the alarm information is too often of poor quality.

7 Alarms

7.1 Alarm definition

The definition of alarm is not consistent between different telecom bodies and we have conflicting definitions of events in 3GPP e.g.

X.733 alarm[8]:	A notification, of the form defined by this function, of a specific event. An alarm may or may not represent an error.
X.733 alarm report[8]:	A specific type of event report used to convey alarm information.
3GPP alarm [3]:	Abnormal network entity condition, which categorizes an event as a fault.
3GPP alarm notification [3]:	Notification used to inform the recipient about the occurrence of an alarm.
3GPP 32.111-1[3]: event:	This is a generic term for any type of occurrence within a network entity.

NOTE: A notification or event report may be used to inform one or more OS(s) about the occurrence of the event.

3GPP 32.111-2 [4]: event:	Occurrence that is of significance to network operators, the NEs under surveillance and Network Management applications. Events do not have state.

The problem in telecom obviously starts with retaining a definition like X.733 [8] "An alarm may or may not represent an error".

EEMUA No 191 [7] /ANSI IS 18.2 [6] clearly emphasizes the philosophy of alarm management and if the following most important criteria for alarms isn't agreed, the severe problems with "alarms" will persists:

- Does the event require an operator response? If the answer is "No" it shall not be defined as an alarm!

The accepted key criterion is that alarms must require an operator response – that is, an action.

To be effective, the alarm system must be reserved for the implementation of items complying with this definition – things requiring operator action to avoid a consequence. Items that do not comply must be removed from the alarm system. Alarms everywhere are configured without meeting this criterion, which is one of the main reasons the alarm problem exists.

Basic principles of the EEMUA approach and its guidelines for alarm systems are:

- Each alarm should alert, inform and guide.
- Every alarm presented to the operator should be useful and relevant to the operator.
- Every alarm should have a defined response.
- The alarm rate should not exceed that which the operator is capable of handling.
- The alarm system should be explicitly designed to take account of human limitations.

ANSI/ISA 18.2 [6] defines:

> Alarm: An audible or visible means of indicating to the operator an equipment or process malfunction or abnormal condition requiring an action.

Alarm management: The processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems.

ANSI/ISA 18.2and EEMUA very strongly address the need to redefine the term "alarm". The fundamental usage must be reclaimed and communicated.

7.2 Good Alarms

EEMUA No 191 [7] emphasizes that alarms must exist solely as a tool for the benefit of the operator. They are not to be configured as a miscellaneous recording tool or for the benefit of the control engineer or other staff.

To let operators monitor only necessary alarms at the right time by extracting the ones they need, is the key to solve the problem identified. If any secondary logs are provided it must be possible to easily separate those from other events.

Some of the characteristics that an alarm should have are summarised in the list below:

CHARACTERISTICS OF A GOOD ALARM	
• Relevant	i.e. not spurious or of low operational value
• Unique	i.e. not duplicating another alarm
• Timely	i.e. not long before any response is needed or too late to do anything
• Prioritised	i.e. indicating the importance that the operator deals with the problem
• Understandable	i.e. having a message which is clear and easy to understand
• Diagnostic	i.e. identifying the problem that has occurred
• Advisory	i.e. indicative of the action to be taken
• Focusing	i.e. drawing attention to the most important issues

A more detailed list of characteristics of a "good alarm" should be explored focused on the Telecom arena. Such a list should be the prime source to support other 3GPP groups involved in network element standardization, with guidelines to enhance the readability, accuracy and relevance of alarm information.

A major challenge for a coherent management of the mobile system is the continued involvement of more and more IP based solutions based on other management paradigms such as SNMP. This is potentially a major opportunity to work with IETF on an alarm standard for devices.

Proposal: Elaborate on a requirements list for "good alarms" that could be shared between standard organizations and interfaces.

7.3 New alarm definition requirements

The new definition should address solutions to the following requirements:

1. Drastically decrease the amount of alarms.
2. Increase the information quality in the alarms in order to support the operational processes and enable automation.
3. Decrease the integration efforts and costs of alarm interfaces and network elements.

7.3.1 Decrease the amount of alarms

The output of EEMUA, ANSI work is clear on the need of a fundamental shift in philosophy on how vendors generate alarms. Vendors lack a solid definition of what should constitute an alarm.

Important requirements that need to be part of the definition:

- Alarms represent an undesired state.
- Alarms require manual action from an operator.
- The fewer the better.

It is important to realize what the above means. First of all, many alarms sent today are generated from a state change such as link going down. But is that an alarm? Not if it is configured down, not if it is test equipment, not if it is not carrying any service. But most devices anyhow blindly send a link down alarm.

If a remedial action that is required by an operator cannot be described, it is not an alarm.

We need a proper definition of alarm that is adopted by vendors so a clear distinction is made between e.g.

- Alarms
- Events (not in the alarm system)
- Log messages (not in the alarm system)
- Data for later analysis (not in the alarm system)

A definition that includes the above criteria's is an important output of this work. It must be written in such a way that vendors can use it in order to reduce the number of alarms sent. A side effect of this is probably that we will recognize the need for another "channel" for events or log messages that do not qualify as alarms. This is still useful for reporting, post-analysis, debugging etc., but it is not alarms. These kinds of messages pollute current alarm systems

Proposal: Revisit the 3GPP TS 32.111-2 Alarm IRP IS for alarm definition and make it much stricter and add requirements for alarms.

Proposal: Consider solutions for efficient transfer/separation of events or log messages.

7.3.2 Increase the information quality

The alarm information quality must be addressed by proper information design when generating alarms. Vendors must understand that operators *and* software do analyse the alarms and therefore information quality is of vital importance.

Do we have relevant alarm types for 3G and 4G networks? We have an outdated TMN probable cause list with values like "Out of CPU cycles".

Proposal: Work on a relevant and updates list of alarms rather than copying the outdated TMN probable cause list.

It is important for an operator to know if a potential cleared alarm notification will be sent, (ADAC or ADMC in 3GPP terminology), however there is nothing in the alarm that indicates this. ADAC/ADMC indication should be added to the information model. Rather the standard has a confusing manual clearing state and operation. Can an operator manually clear an ADAC alarm? We should not mix state changes from operators and state changes from the devices. Alarms can potentially be cleared from the devices. Operators can acknowledge alarms, consider the alarms to be fixed and comment alarms. The three latter are examples of operator states, which should be handled by the standard including a textual comment to these kinds of state changes. They must allow for several operators, so a list with operator-state and comment, rather than a single attribute for "ack".

Proposal: Revisit the 3GPP TS 32.111-2 Alarm IRP IS and make the information model more strict.

Which data belongs to the alarm type?

If we look at current alarm interfaces they do not distinguish between data that belongs to all instances of an alarm types and which are unique for an alarm instance. Examples of data that belongs to the alarm type:

- Operator instruction.
- Does the alarm have a corresponding cleared alarm notification (ADAC/ADMC)? It is very important for the operator to know if the device will report a cleared alarm or not.
- We could put mapping to the X.733 type identifiers here: [event type, probable cause, specific problem].

Note that alarm-type data need not be sent in the notifications. It is enough with the alarm-type identity.

Which data belongs to the alarm instance?

- Severity: the severity of the alarm. Much more focus must be spent on this. Studies show that the severity sent by the vendor has no correlation with the priority set by operators.
- Clear/Active: it is important to separate the clear state from the severity as such. This is not well handled in standards. We must be able to talk about a cleared minor alarm for example.
- Clear separation of state-changes from devices versus actions from operators. For example the notion of "manual clear" is sometimes used, the operator view is one thing the device view is another, these should not be mixed.

Proposal: Separate the severity of the alarm versus it if is cleared or not.

The classical alarm type identification is [event type, probable cause, specific problem]. This has some problems in that probable cause is a flat enumerated and specific problem is in most cases a free form text string. This has led to probable cause being an old not manageable enumerated and vendors escape to the free form text string. It is time to improve on this. We could learn from other systems like DNS, a hierarchical naming scheme is much more manageable. We could use a similar pattern for alarm types and define standardized alarm types and let vendors specialize those with "sub-types". The standardized alarm types must be worked upon by 3GPP and not left to vendors. Note that since specific problem is a string, vendors can add alarm types "randomly". This makes it hard to produce a good alarm management system since there might be alarm types without a corresponding well defined action.

Proposal: Allow for a hierarchical alarm type definition so that vendors can subtype standardized alarm types rather than escaping to an unmanaged free form string.

Proposal: The definition shall be inspired by work done by EEMUA and ANSI.

7.3.3 Decrease the integration cost

Although we have alarm interface standards, the cost of integrating alarm interfaces to the OSS systems are still surprisingly high. The cost comes from two major layers:

- The Syntactical Layer: protocols and data-models for the integration interface. (3GPP Solution Sets).
- The Semantical Layer: making something useful out of the alarms to the operators. This includes automatic look-up of proposed repair actions, alarm texts etc. (Not really addressed today).

The first item should be studied, why do we still need costly integration projects for integrating alarm interfaces? There are a couple of issues in the current solution set around how alarm instances are identified that certainly adds to the integration complexity. AlarmId is an overlapping identification mechanism in parallel with the X.733 triplet. It actually adds inconsistencies to the model. This is one example that should be cleaned up.

The second item is not covered in today's standards. There is a need to address a way of expressing a semantic alarm model which defines all alarm types and what they mean, so they can be automatically integrated into the alarm system. Today this is a manual intensive process reading documentation, looking at specific problem strings, asking the vendor etc.

When it comes to protocols and data models for alarm interfaces, 3GPP should look at IETF liaison for several reasons:

1. Great value if we can have a common alarm interface across 3GPP and IETF.
2. IETF are good at concrete protocols and data models, they have a bad history when it comes to alarms. IETF skills in defining concrete interfaces could help 3GPP improve.

We could get feedback from 3GPP Solution Set integration projects. What takes time? What is costly? Why is it complex to do the alarm interface integration? Based on that we can improve the syntactical interface definition. Study how the semantic information can be defined, which alarm types do we have? What do they mean? What is the Operator Action? This should be expressed in a way so that the alarm interface integration could be done automatic.

7.4 New Alarm definition proposal

The EEMUA and ANSI/ISA18.2 papers [7], [6] emphasize the need of a redefinition of the term “alarm”. This is to communicate to “producers” and “users” of alarm the very most important basic thing - alarms must exist solely as a tool for the benefit of the operator and requiring operator action to avoid a consequence.

The paper "Chasing a Definition of "Alarm" "[9] is an important walkthrough of the complexity of alarm definitions, related concepts and includes also comparisons between different standardization bodies in Telecom as (X.733, IETF, 3GPP, DMTF and ITIL). The analysis in the document is clear, the telecom business shares the very similar issues with an unprecise definition of "Alarm" as the production&engineering businesses. The paper argues for the need to focus on the definition of the alarm concept and on the alarm information itself.

ANSI/ISA 18.2 [6] defines:

Alarm: An audible or visible means of indicating to the operator an equipment or process malfunction or abnormal condition requiring an action.

Analysis of the EEMUA anad ANSI/ISA work states:

> Alarm response is really not a function of the specific process being controlled. It is a human-machine interaction. There is little difference between different businesses. While many industries feel "We're different!"- that is simply not the case when it comes to alarm response.

The understanding of the definition may be easily mapped to the telecom environment, primarily the focus "indicating to the operator" and "condition requiring an action". "Audible" and "process malfunction" may be terms that are not fully applicable/used in the telecom business.

The usage of the term "Alarm" is spread in a telecom organization into many different processes, with very different level of detailed knowledge. It would thereby be beneficial to try to set a definition that can easily be shared and give a common understanding of what is meant with an "alarm".

In paper [9] a similar definition is proposed:

Alarm: An alarm signifies an abnormal state in a resource for which an operator action is required.

In the telecom business we feel comportable with the introduction of the terms "state" and "resources". The very most important part "for which an operator action is required" is included.

The concept of "states" are important in telco and "resources" are widely used in e.g. TMForum eTOM.

The term "abnormal state" could be reworded to "undesired state". Its better aligned with the EEMUA & ANSI/ISA 18.2 work, focusing on "it requires an operator action to avoid a consequence".

Alarm: An alarm signifies an undesired state in a resource for which an operator action is required.

Proposal: Introduce the above definition as a new definition of "Alarm" in 3GPP.

7.4.1 Definition of Alarm Notification

In paper [9] the following figure is introduced to clarify some basics:

Beyond the imprecise definition of "alarm"we often refer the term "alarm" to the alarm *notifications* exchanged by systems. It may be difficult to fully change the usage of such dualism but in the context of standardisation we would have a definition available also clarifying "alarm notification".

Alarm notification: A message about an alarm state change such as raise or clear.

Proposal: Introduce the above definition of "Alarm notification" in 3GPP.

7.4.2 Definition of Managed alarm

ANSI/ISA18.2 has defined the concept of highly managed alarms but do not define the term "managed alarm" itself.

We propose the concept of managed alarm to include added states and other information that relate to the alarm management process, in the NM domain (above Itf-N). Here the operator can enrich the information for the purpose of the alarm management process. With "managed alarm" operators can e.g. transform severity of the alarm from resource focus to a full focus on service impacts, to prevent or mitigate network and service outage and degradation. The concept applies to any severity level.

Managed alarm: The management representation of the alarm in the NM domain.

Proposal: Introduce the above definition of "Managed alarm" in 3GPP.

8 Alarm Management

8.1 General

The ANSI ISA 18.2 standard postulates that a foundational part of alarm management is the definition of an alarm; an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response. The essential element of this definition is the response to the alarm. This definition is reinforced in the alarm management processes described in the standard.

Beyond the fundamental definition/redefinition of an alarm, alarm management is about work processes. The alarm response is a human-machine interaction. This takes place above the Itf-N. The Itf-N machine to machine interaction is required to facilitate these work processes and the human-machine interaction. Better performing alarm systems must be created based on the requirements on how they are used and the challenges we face in a continuously changing environment, as described in clause 4.

8.2 Operability

A higher level alarm design issue is the fundamental limitation of the human user. It is crucial that the operators are not overloaded with alarms and potentially loses the overview of the network and services.

The concept of alarm management, as elaborated by ANSI / EEMUA, emphasises two main parallel approaches to minimize the threat to operator effectiveness:

1. Eliminate the alarm overload. This is done in the design of alarms, ensuring that all alarms are justified and properly configured. This should be the first priority but is a cumbersome and prolonged effort and will not cover all potential overload scenarios.

2. Improve the management of alarm overload. The designers of any alarm system should recognise the fundamental human usability limitation and support functionality to cope with alarm overload. E.g. alarm lists displays should never be allowed to be unusable caused by repeating alarms. Many different systematic technics are available, see clause 11 "Alarm suppression methods".

It is noted that alarm overload is among other things, affected by the number of resources handling the alarms and the amount of alarms generated.

9 Alarm Management Lifecycle

9.1 Processes

ANSI/ISA18.2 [6] emphasizes the need to implement a lifecycle process to manage the alarm systems.

A basic planning is necessary and the first step is to develop an alarm philosophy that documents the objectives of the alarm system and the processes to meet those objectives.

The different processes can be grouped into an engineering part (A-E), operational part (F-H,I) and follow up part (J).

The figure below from ANSI/ISA 18.2 [6] presents the main processes in the Alarm Management Lifecycle. Details of this important concept are found in the ISA 18.2 standard.

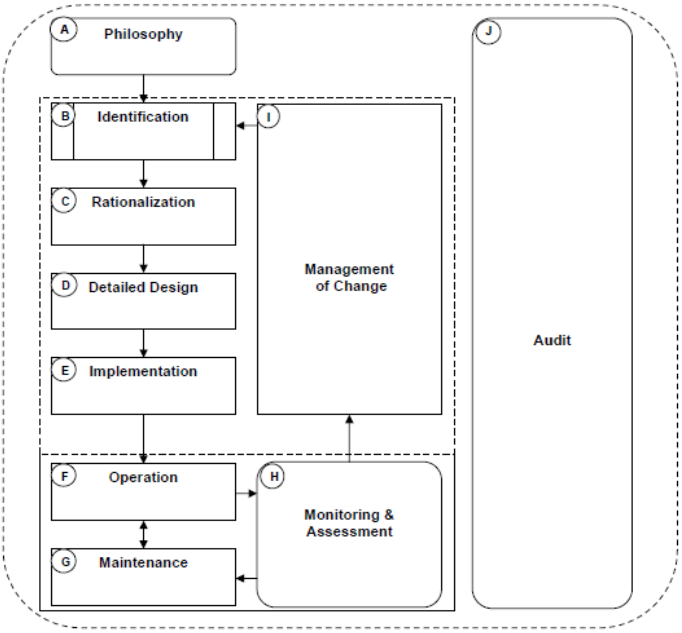


Figure 2

Of prime importance and of most complexity of the alarm management processes is probably the rationalization task that will analyse and prioritize many of the individual alarms. In telecom most of the classification of alarm severity is done by the equipment vendors and will need to be analysed and often reclassified dependent on the network environment, service offered etc.

The ANSI /ISA18.2 standard stresses the audit functionality, to regular follow the behaviour of the alarm systems with defined KPIs. Important part of alarm management will be alarm suppression methods presented in clause 11.

Obviously we find a similarity with inheriting eTOM [5] processes. It will be up to the individual operators to tailor its operations and will not be target for standardisation.

However, bad quality alarms, in contrast with "good alarms" will be complex or impossible to handle even in an advanced alarm management environment.

9.2 Highly Managed Alarms

The alarm severities defined in a mobile system are basically set out of criteria limiting the functionality the network equipment is supporting. Huge amount of alarms classified as Critical are sent to operator's management centers but are rarely critical from the overall business perspective. They may even not be critical from time to respond.

An operator view may obviously be very different from the alarm severity defined by the equipment vendor.

ANSI / ISA 18.2 have defined one class of alarms call "Highly Managed Alarms", HMAs. These alarms are the very most critical alarms, catastrophic from operations, security, business or any other top level reason. These alarms should receive special treatment particularly when it comes to viewing their status in the HMI. These are the alarms that must never be missed and must always be given the highest attention.

Considerable high levels of administrative requirements are applicable for the HMAs. For companies following this standard, detailed documentation and a multitude of special administrative requirements in a precise way need to be fulfilled.

These include:

- Specific shelving requirements, such as access control with audit trail
- Specific "Out of Service" alarm requirements, such as interim protection, access control, and audit trail
- Mandatory initial and refresher training with specific content and documentation
- Mandatory initial and periodic testing with specific documentation
- Mandatory training around maintenance requirements with specific documentation
- Mandatory audit requirements

The Highly Managed Alarm classes are also subject to special requirements for operator training, frequency of testing, and archiving of alarm records for proof of regulatory compliance.

In Telecom, we hardly have the physical catastrophic scenarios or human physical security aspects to handle. However, our services may be a part of a delivery chain that could be vital components in a HMA scene and as such the HMA or part of the HMA concept could apply also for the telco parts.

Millions of mobile customers are now and then affected by major failures in the infrastructure of mobile systems. Assurance management of the continuously increasing complexity of our mobile systems could benefit from concepts like Highly Managed Alarms. We would identify the very most critical equipment and secure that these types of alarms are treated in the most thoughtful way. The HMAs may never be hidden, delayed etc in e.g. alarm flooding.

Setup of HMA will include many of the processes identified in the Alarm Management Lifecycle. To implement HMA in the mobile system new requirements on the information services of the 3GPP IRP can be expected.

10 Alarm states

The 3GPP alarm states are limited to the operational state of the logical and/or physical resource(s). State information is also related to the life-cycle of the alarm from an operator's point of view. Separate operator states that indicates "the alarm is not of interest any more", "already seen" etc. would be valuable information for operators and the alarm systems. A state called Closed could be introduced. Operators view should not be mixed with the device view for e.g. clear.

Proposal: Consider extension of the alarm states to include operators alarm life-cycle view.

Proposal: Consider introduction of an alarm state called e.g. Closed.

ANSI/ISA 18.2 [6] has elaborated and extended alarm states for alarm systems with a set of states for alarm suppression. These should be of significant value also for the telecom business. The states are called Shelved, Suppressed by Design and Out of Service and can connect to any alarm state shown in the figure below.

ANSI [6] do define these states as:

Shelved state

The shelved state is used when an alarm is temporarily suppressed using a controlled methodology. An alarm in the shelved state is under the control of the operator. The shelving system may automatically unshelve alarms.

Suppressed by Design state

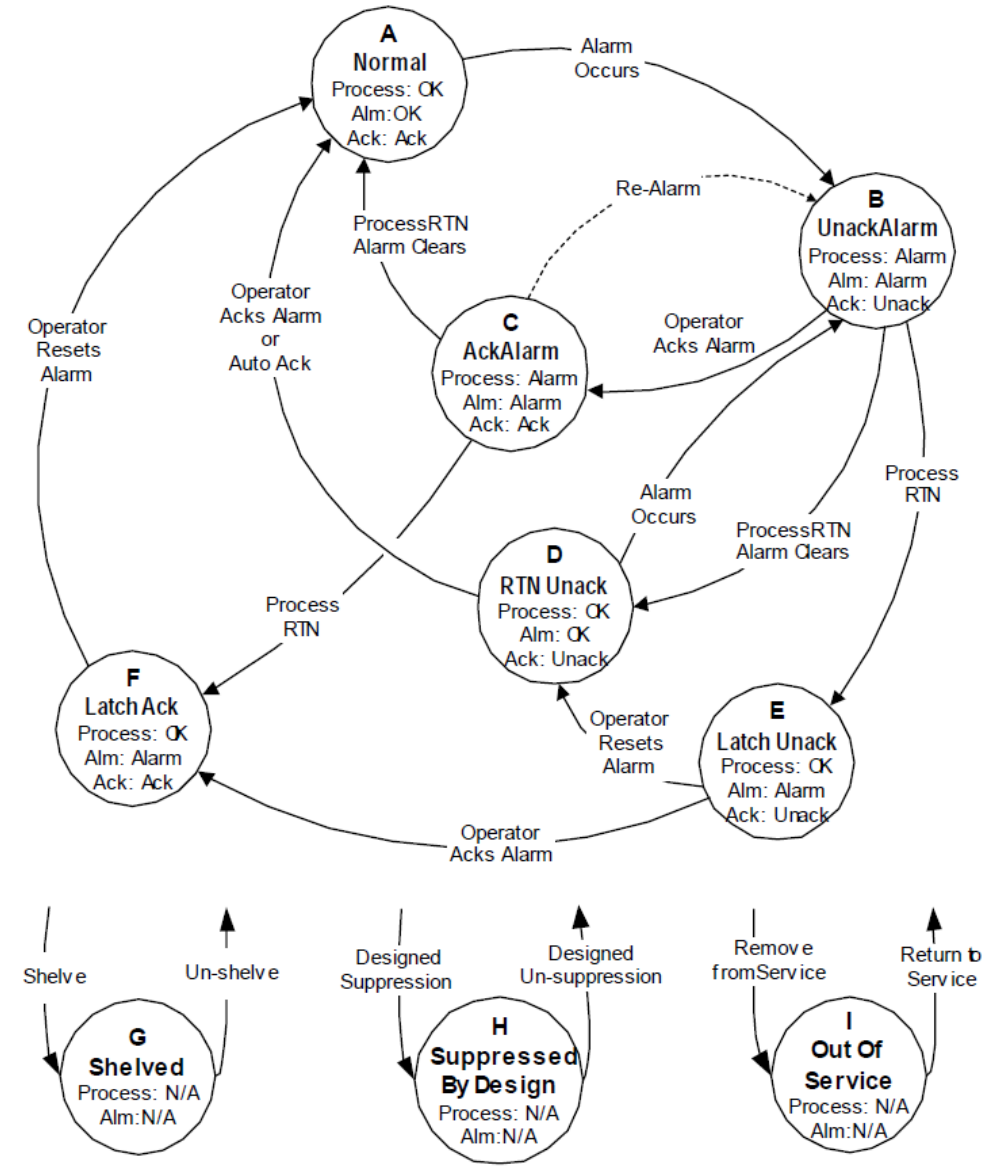
The suppressed by design state is used to suppress alarms based on operating conditions or plant states. An alarm in the suppressed by design state is under the control of logic that determines the relevance of the alarm.

Out-of-service alarm state

The out-of-service alarm state is used to manually suppress alarms, (e.g. use control system functionality to remove alarm from service), when they are removed from service, typically for maintenance. An alarm in the out-of-service state is under the control of maintenance.

In the telecom business, alarms generated under maintenance and/or change management contribute to a very high degree to the alarm floods in our alarm systems. A specific Out-of-service alarm state would together with appropriate OSS functionality enable limitation of these nuisance alarms.

Alarm State transition diagram from ANSI/ISA 18.2 [6].



Note 1: States G, H, and I can connect to any alarm state in the diagram.

Note 2: The dotted line indicates an infrequently implemented option.

Figure 3

11 Alarm suppression methods

11.1 Purpose

A key idea of EEMUA No 191 [7] is that the cognitive resources of operators are limited and therefore should not be overloaded with alarms. The alarm management solutions should support the operators with specific techniques to handle alarm flooding as grouping of alarms.

The common expectation is that operators should never overlook important alarms. However it's important to understand that human operators have a limitation to the extent to which they can operate effectively to a period of high level uploading. It emphasizes the usability of an alarm system from the operator's perspective. The conclusion is obvious: every alarm should be useful and relevant to the operator. There should be no alarm without a predefined operator response.

3GPP Telecom Management has not focus on standardization of NEM/NM OSS functionality. However the concept that EEMUA and ANSI has introduced and standardized in this area could be of significant potential in our telecom business. The systematic approach to handle suppression of alarm floods is impressive. We share the very same problems where the production and engineering field have come up with solutions.

Suppression methods have been elaborated for e g repeating alarms, alarm flooding, chattering and fleeting alarms, testing, shelving, eclipsing, load shedding and out-of-service handling. Such functionality are preferably introduced at lowest possible level in the TMN logical functional hierarchy.

The reference documents EEMUA[7] and ANSI[6] includes rich and detailed descriptions of a variety of alarm suppression methods and is recommended for further study of this topic.

Proposal: Secure that the 3GPP IRP concept will support/enable efficient alarm suppression methods at lowest possible level in the TMN logical functional hierarchy according to the systematic EEMUA/ANSI approach.

Below (11.2-11.4) is a presentation from ANSI/ISA 18.2-2009 [6] of three of the key suppressions methods and the approach taken in this area.

11.2 Alarm Shelving

The temporary shelving of alarms by the operator is a common practice to keep nuisance alarms and other alarms from interfering with the effectiveness of the alarm system. Shelving includes a set of functions to ensure the integrity of the alarm system is maintained. Where alarm shelving is provided, the requirements of this clause shall be met.

11.2.1 Alarm Shelving Functional Requirements

The alarm shelving function shall provide the following:

a) displays of shelved alarms or equivalent list capabilities, to indicate all alarm shelved,

b) a time limit for shelving,

c) access control for shelving of highly managed alarms, if allowed,

d) the ability to unshelve alarms,

e) a record of each alarm shelved.

11.2.2 Alarm Shelving Functional Recommendations

The alarm shelving function should be designed to prevent alarm floods when alarms are automatically un-shelved.

11.2.3 Shelved Alarm Displays

Shelved alarm displays, or equivalent list capabilities, for an alarm system with shelving functionality have several required and recommended functions.

11.2.3.1 Information Requirements

Shelved alarm displays shall provide the following information:

a) the tag name and description,

b) alarm type,

c) the unsuppressed alarm state,

d) the alarm priority,

e) the time and date the alarm was shelved or the shelved time remaining.

11.2.3.2 Functional Requirements

Shelved alarm displays shall provide the following functions:

a) sorting of alarms by chronological order of shelving or shelved time remaining,

b) sorting of alarms by priority,

c) individual unshelving of alarms.

11.2.3.3 Functional Recommendations

Shelved alarms displays should provide the following functions:

a) sorting of alarms by chronological order for active alarms,

b) operator entry of the reason the alarm was shelved,

c) filtering of alarms by priority,

d) filtering of alarms by alarm state,

e) filtering of alarms by process area,

f) navigational link to a process display,

g) navigational link to the tag display.

11.3 Out-of-service Alarms

The suppression of alarms by placing an alarm out of service is common practice to remove alarms from service to allow maintenance. There are several required and recommended HMI functions related to out-of-service alarms.

11.3.1 Out-of-service Alarm Functional Requirements

The out-of-service alarm function shall provide the following:

a) a method to individually remove each alarm from service,

b) a method to individually return each alarm to service,

c) displays of out-of-service alarms or equivalent list capabilities, to indicate all alarm out-of-service,

d) access control to place highly managed alarms out-of-service if allowed,

e) a record of each alarm placed out-of-service.

11.3.2 Out-of-service Alarm Displays

Out-of-service alarm display, or equivalent list capabilities, shall be provided for the alarm system. Out-of-service alarm displays have several required and recommended functions. The out-of-service alarm displays may be combined with the shelved alarm displays.

11.3.2.1 Information Requirements

Out-of-service alarm displays shall provide the following information:

a) the tag name and description,

b) alarm type,

c) the unsuppressed alarm state,

d) the alarm priority,

e) the time and date the alarm was placed out-of-service.

11.3.2.2 Information Recommendations

Out-of-service alarm displays should provide an indication of the suppression method (e.g. out-of-service).

11.3.2.3 Functional Recommendations

Out-of-service alarm displays should provide the following functions:

a) sorting of alarms by chronological order of suppression,

b) operator entry of the reason the alarm was suppressed,

c) sorting of alarms by priority,

d) sorting of alarms by alarm state,

e) sorting of alarms by process area,

f) individual return-to-service of alarms.

11.4 Alarms Suppressed by Design

The designed suppression of alarms is common practice to prevent alarms that are not needed due to intended or actual operating conditions. Where alarm designed suppression is provided, the requirements of this clause shall be met.

11.4.1 Designed Suppression Functional Requirements

The designed suppression function shall provide the following:

a) displays of alarms suppressed by design or equivalent list capabilities, to indicate all alarms suppressed by design,

b) a record of each alarm suppressed by design.

11.4.2 Designed Suppression Displays

Designed suppression displays, or equivalent list capabilities, shall be provided for the alarm system. Designed suppression displays have several required and recommended functions. The designed suppression displays may be combined with the shelved alarm displays or outof-service alarm displays.

11.4.2.1 Information Requirements

Designed suppression displays shall provide the following information:

a) the tag name and description,

b) alarm type,

c) the unsuppressed alarm state,

d) the alarm priority,

e) the time and date the alarm was suppressed.

11.4.2.2 Information Recommendations

Designed suppression displays should provide an indication of the suppression method (e.g. designed suppression).

11.4.2.3 Functional Recommendations

Designed suppression displays should provide the following functions:

a) sorting of alarms by chronological order of suppression,

b) sorting of alarms by priority,

c) sorting of alarms by alarm state,

d) sorting of alarms by process area.

12 Conclusions

This work has been triggered by valuable work and solutions found in the production and engineering industry of an escalating major problematic area in management of a mobile system. Our network administrators are flooded with alarms and alarms with often poor quality, hindering efficiency and ability to adopt better OS support.

Standardization bodies in the production and engineering fields (e.g. EEMUA [7], ANSI [6]) have addressed the problem and undertaken substantial work under last decade to come up with solutions. The work with ANSI/ISA-18.2-2009 Alarm Management Standard started 2003. ISA-18.2 is a standard, not a guideline or a recommended practice, and is reported to be developed in accordance with stringent ANSI methodologies. As such, it will be regarded as a "recognized and generally accepted good engineering practice" (RAGAGEP) by regulatory agencies and insurance companies. ISA-18.2 is in the process of being adopted as an International IEC standard (IEC 62682 Ed. 1.0 [12]).

Management of a mobile system may not face the security and hazardous issues that triggered the ISA-18.2 work, but obviously we do share the very same problem in the alarm management field. Potential dependencies with security and hazardous impacts are usage of mobile services as transport mechanism for delivering alarm notifications from e g equipment in rural areas in power grid networks. It may be brought to focus by regulatory agencies. The expanding field of machine-machine communication and deployment of heterogeneous networks are other areas that will challenge the existing way of alarm management in a mobile system and call for efficient solutions.

We yet do not have any good technology to relieve operators of manual work, this is shared with the production and engineering field, main identified reason is the alarm quality issues. It is worth noting that after decades of research in telecom, alarm correlation is still the most prioritized research area. This can partially be interpreted as a failure, since no solution seems to be ready [10].

We have obviously many drivers to adopt and benefit from the work done by EEMUA and ANSI/ISA18.2.

The systematic approach on a specific process for alarm management and the set of alarm suppression methods are impressive. The significance of enhanced alarm quality and the most fundamental of all; a new alarm definition to reclaim the real use of alarms. The basic principle of proper alarm management is that alarms must require an operator response, items that do not comply must be removed from the alarm system. Alarms must exist solely as a tool for the benefit of the operator. The production and engineering fields argue that if this principle is followed, huge improvement in a system will be made, even if none of the other principles are followed – it is that powerful!

The outcomes of the EEMUA and ANSI/ISA-18.2 work is an important "eye-opener" in Telecom Management. Many of the solutions proposed cannot be target for standardization in 3GPP, e.g. the improvement of the work process on top of the Itf-N, the improvement of the human-machine interface. However the alarm management processes are proposed to be the focus and be supported by 3GPP Telecom Management solutions. A new alarm definition is obviously a fundamental approach to solve the issues identified. The alarm rationalization stage in the lifecycle of alarm management would in management of a mobile system need to handle tens of thousands different types of alarms. To

minimize operators need to analyse and transform every single alarm related to its usability should be at the essence of 3GPP Telecom Management standardization work. In order to address significant and real problems, our standards also need to focus on alarm quality and alarm semantics.

13 Recommendations

Be inspired by and adopt EEMUA No 191, ANSI/ISA 18.2 [7] and [6] as guides for alarm management of a 3GPP mobile system. This is impressive work that should be reused in Telecom Management.

Redefine the term "alarm" used in our specifications according to the ANSI/ISA 18.2 and EEMUA findings. The fundamental usage must be reclaimed and communicated.

Accept the proposed new definitions in clause 7.4 for “Alarm”, “Alarm notification” and “Managed alarm” as new definitions in 3GPP.

Items that do not comply to the new alarm definition must efficiently be transferred/separated from our alarm systems.

Elaborate on a requirements list for "good alarms" that could be shared between standard organizations and interfaces.

Work on a relevant and updates alarm probable cause lists for entities of a 3GPP compliant mobile system.

Revisit the 3GPP TS 32.111-2 Alarm IRP IS for alarm definition and make it much stricter and add requirements for alarms. We need to enhance the alarm quality and alarm semantics.

Separate the severity of the alarm versus it if is cleared or not. Consider extension of the alarm states to include operators alarm life-cycle view. Consider introduction of an alarm state called e.g. Closed.

Allow for a hierarchical alarm type definition so that vendors can subtype standardized alarm types rather than use an unmanaged free form string.

Annex A:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2012-11					First draft		0.1.0
2013-01					Post-SA5#87 Malta changes. Based on TR skeleton draft S5-122966 plus pCRs S5-130187, S5-130282 and S5-130045	0.1.0	0.2.0
2013-04					Post-SA5#88 Qingdao (China) changes. Based on pCRs S5-130748, S5-130749, S5-130750, S5-130751, S5-130799	0.2.0	0.3.0
2013-05					Post-SA5#89 Sophia Antipolis (France). Based on pCRs S5-130932, S5-130972,S5-131077, S5-131079	0.3.0	0.4.0
2013-06	SA#60	SP-130282			Presented to SA for information	0.4.0	1.0.0
2013-06					Several editorial changes from EditHelp	1.0.0	1.0.1
2013-08					Post-SA5#90 Valencia (Spain). Based on pCR S5-131425	1.0.1	1.1.0
2013-09	SA#61	SP-130455			Presented for approval	1.1.0	2.0.0