ALARMS CONFIGURATION MANAGEMENT

P. Sollander, R. Martini, K.Sigerud, N. Stapley, A. Suwalska, CERN, Geneva, Switzerland.

Abstract

The LHC alarm service, LASER, is the alarm tool used by the operators for the accelerators and the technical services at CERN. To ensure that the alarms displayed are known and understood by the operators, each alarm should go through a well-defined procedure from its definition to being accepted in operation. In this paper we describe the workflow to define alarms for the technical services at CERN. We describe the different stages of the workflow like equipment definition, alarm information specification, control system configuration, test, and final acceptance in operation. We also describe the tools available to support each stage and the actors involved. Although the use of a strict workflow will limit the number of alarms that arrive to LASER and ensure that they are useful for operations, for a large complex like CERN there are still potentially many alarms displayed at one time. Therefore the LASER tool provides facilities for the operators to manage and reduce the list of alarms displayed. The most important of these facilities are described, together with other important services like automatic GSM and/or e-mail notification and alarm system monitoring.

INTRODUCTION

CERN's technical infrastructure is monitored from the CERN Control Centre (CCC). The CCC is manned 24 hours a day and 365 days per year. The control room is divided by activity in four islands. One of the islands is staffed by the technical infrastructure (TI) operators. Their mandate is to minimize the impact of technical breakdowns on accelerators and other important installations at CERN, to manage corrective maintenance activities and to co-ordinate interventions during breakdowns.

The systems supervised by the Technical Infrastructure operators range from electricity distribution, cooling, ventilation, safety systems and vacuum to control system components cryogenic equipment, lifts and heavy handling equipment. In all there are several thousands of pieces of equipment spread over the various surface and underground sites around CERN.

A failure on a piece of equipment is signalled to the operator either by a user over the phone or by the control system on an alarm screen. It is the job of the operator to analyse the information he receives and to take the appropriate actions. In 2006, the TI operators received more than 20'000 telephone calls and more than 500'000 alarms and generated over 8'000 work orders for corrective maintenance.

The operators use three main computer tools to manage their task:

- A LASER alarm screen (or in fact several screens), to get alerted of an event.
- Synoptic views, to diagnose a problem and, if possible, to repair remotely
- A Computerized Maintenance Management System (CAMMS) to create and follow-up work orders.

It is of the utmost importance that an event is consistent among these tools; a fault signalled on the alarm list must also be visible on the synoptic views and the state of a work order must be visible from the alarm list to give the operator a possibility to follow-up an event.

The following sections will concentrate on alarms and explain the system architecture, the alarm configuration workflow, how the alarms are managed in a way to make them comprehensible to operators, how the alarm system is made robust and also how they are used in operation and what services are connected to alarms. Although LASER is the common alarm tool for the CERN Control Centre (CCC), this paper will concentrate on the use made for technical infrastructure. First however, it is necessary to define what is meant by an alarm in this context.

DEFINITION OF AN ALARM

The notion of alarm differs in different organizations and in different tools and applications. At CERN and in the context of control room monitoring, an alarm is defined as <u>an event that needs operator attention and action</u>. An alarm is directed towards an operator who must have a fundamental understanding of layout, processes and systems. An alarm cannot carry all information necessary for the appropriate response [1]. If an event does not need operator attention, it should not be displayed on the alarm list but rather stored where it can be found on request, for example on a separate event list. An alarm is displayed as a single line on an alarm list and carries the following information:

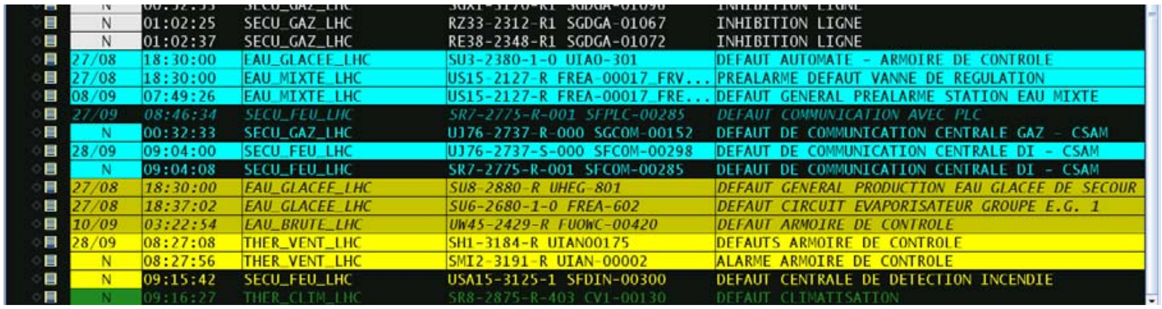

Figure 1: LASER alarms

- Information directly visible on the alarm list (see Figure 1):
  - Date and time of the event.
  - System/subsystem/functionality; a short text describing what system is concerned. Examples are “EAU_BRUTE_LHC” for LHC raw water or “ELEC_18kV_BA2” for 18kV supply for the SPS BA2.
  - Detailed location information; building, floor, room.
  - Equipment name/code; a name used by the equipment owner and if possible by the maintenance management system that uniquely identifies a piece of equipment.
  - Problem description; a text describing the event
  - Priority; displayed by text colour from the highest priority, 3 in red, through level 2 in yellow and level 1 in blue down to the lowest priority, 0 in white
  - State; an active alarm is displayed in a colour corresponding to its priority level (3 red, 2 yellow, 1 blue and 0 white [2]) and is displayed in green when terminated.
- Configuration information
  - Data source, address, responsible, etc.
- Additional operator help information
  - Cause, consequence, action, maintenance management codes, alarm instructions

Understanding the alarm information relies on organization wide common conventions for elements such as equipment identity and location.

ARCHITECTURE OF THE ALARM SYSTEM

The alarm system known as LASER (LHC Alarm SERVice) is made from 5 main components on 3 tiers as shown in Figure 2. These being: sources, the middle tier servers, the database, message oriented middleware (MOM) brokers and operator consoles.

The MOM brokers, running as a highly available cluster, provide a communication service between all the tiers. The database also has redundant instances for storing alarm definition data as explained above.

Sources send alarm events to the middle tier and these contain an alarm identity, timestamp and state (active or terminate). Sources are software processes, created and maintained by alarm providing clients, which monitor their infrastructure or accelerator subsystems. Each one is monitored by LASER, and if any fail, then an internal alarm is raised to notify operations of this problem.

The middle tier processes incoming alarm events, does some verification such as checking that the identities are valid, then stores the event, and delivers any necessary alarm change to the consoles along with its corresponding definition.

Finally, consoles subscribe to categories of alarms, which are descriptive subsets of the total set focused on users. Consoles show alarms as they occur, and also provide access to the archive, and other alarm information. Other external software clients can also subscribe to alarm output, for example the accelerator post-mortem system.

LASER handles the alarm tools and event delivery, however, the quality of alarm data depends primarily on the definition process.

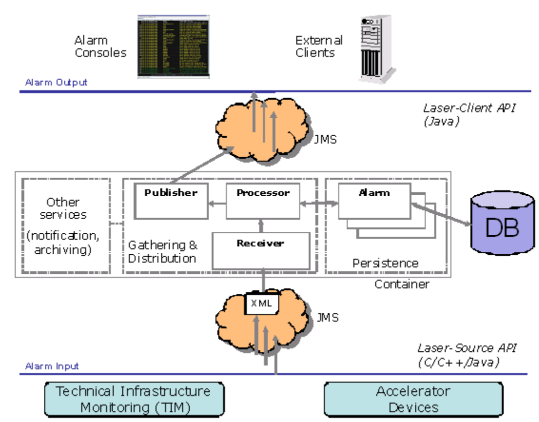

Figure 2: Architecture of the LASER system

ALARM CONFIGURATION WORKFLOW

The Technical Infrastructure Monitoring (TIM) system [3] handles the acquisition, processing and distribution of alarms, measurements and states essential to ensure the smooth running of the accelerator complexes and their related support activities.

MoDESTI Requests

The Alarm definition process requires several services to work in a specific sequence starting with equipment specialists, involving TI operators and ending with TIM support. Alarm integration includes cabling to monitoring units, declaration and validation of data in a reference database, configuration of the monitoring system, definition of the actions to be taken by the operators as well as the testing and acceptance of the alarm (see Figure 3). To work efficiently and to deal with the growing number of new alarms and frequent update requests, this complex process requires coordination.

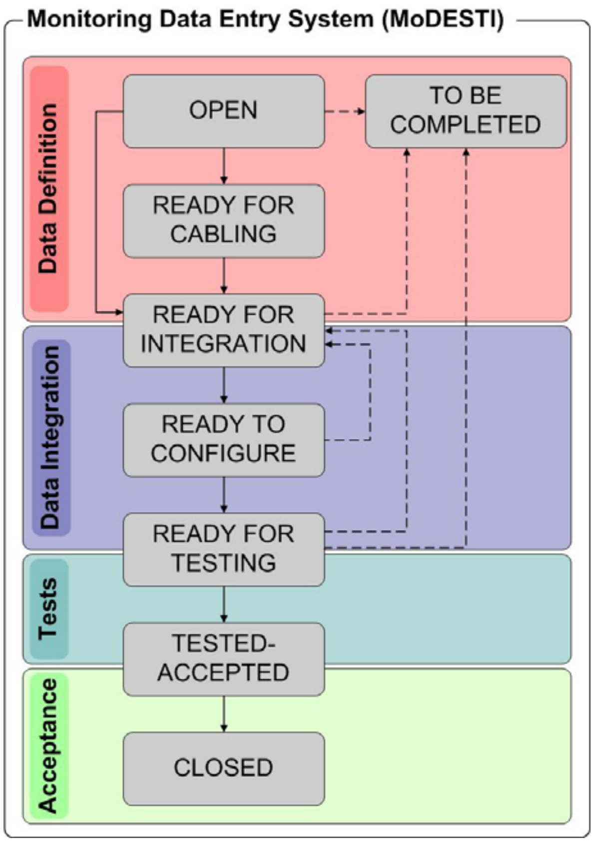

Figure 3: The data integration workflow

To manage this process CERN devised the Monitoring Data Entry System for Technical Infrastructure (MoDESTI). The data defining the alarm(s) is first entered on a standardised Excel sheet and then submitted to the workflow tool based on CERN's Electronic Data Management System (EDMS) [4],[5]. This tool allows the different people involved in alarm definition to act in the pre-defined order. The system generates e-mail informing the appropriate specialists about the next steps and actions to be performed or problems to be solved. Moreover, at any moment, the alarm requestor can check the status of his/her request.

Before the alarms are integrated into the system, they are both manually checked by the TI operators and submitted to automatic consistency checks. Only fully verified data is entered into the reference database. Once alarm definitions are validated and stored in the reference database, they can be safely configured in the TIM and LASER systems. The configuration of the two systems is synchronised and covers new alarms, deleted alarms, as well as changes to alarm descriptive data. All new technical infrastructure alarms are initially declared in 'test' mode. These alarms will appear on the LASER alarm screen in a distinctive way so that TI operators do not treat them as real alarms. Once the new alarms are tested and conform to the requestor's needs, they are configured in 'operational' mode. At this point the MoDESTI request can be closed.

Data Updates

Several web applications are available allowing authorized equipment specialists and TI operators to consult and edit the alarm data. Newly developed administration interfaces ensure that alarm definitions can be easily and safely modified. Data validation is performed at two levels: first at the user interface level, and then within the update APIs which detect any incoherencies in the alarm definition. If the data modified affects the configuration of the alarm, it is flagged for reconfiguration.

A number of recently deployed automatic background processes carry out data checks as certain alarm parameters may become obsolete during the lifecycle of the alarm. A good example is an alarm responsible person affiliation. This information must be updated if the person is finishing his/her contract at CERN. To avoid having invalid data, an automatic e-mail notification with the data update request is sent a month before end of contract to the concerned person, their supervisor as well to TIM support.

Learning from the past; improving the workflow, issue management

CERN has chosen to define many detailed alarms rather than few general alarms. Currently, the Laser system hosts 140'000 different alarms and the number is expected to grow to approximately 400'000 when all alarms for the LHC have been defined. The advantage of having many detailed alarms is that single faults are described in detail and can be handled more quickly and easily, giving better maintenance management. The disadvantages are: first that the alarm system must handle a high average throughput of alarms, second that each individual alarm must be described and configured, and finally operators must handle a large number of alarms simultaneously. For instance when a general power outage occurs, alarms are generated from many different systems [6].

To solve these issues, CERN has put in place a scalable architecture for the alarm system, an automated process for alarm definition and a set of different means to handle the flow of incoming alarms on the console level.

In the past few years, CERN has completely renovated its alarm system; a new data integration procedure MoDESTI based on EDMS has replaced an older system and given a more rigorous integration mechanism; the TIM control system has replaced a previous generation of infrastructure monitoring tools, improving availability, robustness and correctness issues; finally, LASER rationalized and updated the long-standing previous generation of the alarm system.

ALARM MANAGEMENT TO AVOID FLOODING SCREENS

The alarm console, combined with the server and using alarm definition parameters has several mechanisms for limiting the number of alarms on screen to a usable maximum and organising them. This is especially useful when there is a major incident such as large electrical failure.

Priority – Each alarm has a defined priority, higher priority alarms require an immediate action, lower priority alarms can wait until the following working day if necessary.

Categories – Alarms can appear in one or more categories thereby creating subsets of alarms. Consoles are configured to show alarms in categories that a particular operator is interested in.

Filters – Alarms can be filtered out based on their definition and identity. Console users can create a more focused set within a category.

Masking – Some active alarms can be masked, they will return on the main list if they are re-activated again. This is used to temporarily remove alarms that are being treated by the maintenance teams.

Inhibiting – Some alarms are waiting to be removed as their underlying hardware, or sensors have been removed. They are inhibited so they will never appear on the main list again. Some alarms exhibit annoying behaviour such as oscillation between states. They are inhibited until a specialist can solve the issue.

Reduction – Alarms can be grouped into similar problems, and often represented as a tree with a parent alarm representing a set of problems. The parent is seen on the main console list, with the ability to see the children associated with it if necessary. There are 2 main types. “Multiplicity reduction” is triggered if a more than a defined number of children are active. The alarm server generates a pseudo alarm to represent the problem associated with the children. For example, if there are more than 2 vacuum valves failed in a sector, then they are reduced by a sector alarm. “Node reduction” is triggered when children are linked as part of their definition to a different alarm event. If that alarm event arrives, the children are associated with it and reduced. For example, if there is no computer network for a building because there is no electricity. Network alarms can be reduced in favour of the electrical alarms.

Oscillation control – Some alarms repeatedly change state due to underlying hardware or surveillance problems. Often this is triggered by dead-band tuning errors, or poorly configured analogue to digital converters. If an alarm repeatedly changes state, this is shown as a continuous alarm in an oscillation state.

Grouping – a future enhancement will be to provide dynamic grouping by definition criteria. As the number of alarms will increase significantly for LHC, this will be an important mechanism for operators to focus on certain classes of problem.

ALARM SYSTEM AVAILABILITY, CORRECTNESS

Alarm systems in general, and LASER specifically, should work “correctly” and always be “available”. We consider what this means here.

In terms of “continuous availability”, LASER relies on a set of other physical services such as its server machines, as well as a set of infrastructure services such as networks, and databases. It also itself is composed of components, such as the MOM brokers and sources. It is virtually impossible to guarantee that all of these can provide a continuous service under all circumstances. Having acknowledged that some of this can fail it is important to make the failure and the consequences obvious so it can not only be fixed, but also so it can be understood that unaffected parts of the system can still be used and will behave correctly. For example, it is possible that the archiving in LASER can fail (perhaps due to a database problem), but alarm event delivery from sources to consoles will continue unaffected. LASER was designed to be failsafe such that alarms are generated and displayed if there is any doubt. If at any time a failure could cause misunderstood behaviour, it is better for the system not to be available. It is important that operators, providers, and developers, all have a correct mental model of how the alarm system functions, in terms of expectations and behaviour, or the system cannot be exploited to its full value.

The alarm consoles provide supervision of the LASER system itself, for example by showing different icons according to the availability of the alarm server.

Another aspect of correctness is that of the alarms themselves. The alarm is only as true as its input, for example, a sensor. A common problem is alarms coming from hardware with analogue input converted to binary decisions. Without proper tuning, it can sometimes be unclear to the surveillance system whether the alarm should be active. As such alarm “truth” is approximate and at finer granularity, indeterminate. Time is another aspect of this problem. Adding a timestamp to an alarm event requires an understanding of the accuracy and precision of the time source.

At some point in the life of an alarm system, a serious situation *will* occur. It is very important to focus on learning from the outcome to improve the system to reduce a reoccurrence. It would be unfortunate that only when a serious or costly failure (sometimes involving insurance, safety, or legal issues) occurs, is any lack of resources closely examined.

OTHER LASER SERVICES

LASER also provides some additional services available in the console.

History – Any alarm may have a history of events associated with it, the console can request and show the previous times the alarm was activated or terminated, up to the last 6 months. It is useful for operators to know if that alarm had occurred before, when and how often.

On-screen search – For when there are many alarms, a quick search facility highlights alarms on the console with the requested text.

Archive – the alarm system stores all events for 2 years. This archive can be searched for sets of alarm events. This is for discovering patterns of problems, investigations and auditing. For example some computer equipment had been stolen a few months previously, and it was possible to discover exactly when from the alarm archive, by examining the network alarm events around the time. General statistics are gathered for reports as well.

Alarm definition information – The global known set of definitions is available for consultation.

Diagnostics – The console can embed components that can request further information and display it directly from a subsystem.

Alarm list export – The alarm system allows exporting all lists (active, history and search lists), not only to a printer, but also as a comma separated values (CSV) file attached to an email.

Alarm Help – Although most alarm information is held within the alarms configuration database, there is a need to be able to link an alarm to additional information. This link enables LASER to show this additional information in a web browser. Technical infrastructure operation uses this link to what is known as the *Help Alarm* application. Furthermore, other visual components can be used, for example, one component for accelerator operators shows detailed equipment status with appropriate basic commands such as reset.

Help alarm related services

Help Alarm (HA) is a web based GUI to display additional information about an alarm:

- *Cause, consequence and actions for the alarm* – defined in collaboration with the alarm owner, and changeable directly on the HA interface, should it need to be.
- *Alarm instructions* – information from the equipment owner or intervening personnel concerning the alarm. For instance, that the alarm should be inhibited for a few days while a spare part is being ordered. A history of all instructions ever issued for a particular alarm is available as a link,
- *Past maintenance orders* – a list of the 4 last maintenance orders issued for the equipment at fault. The list shows dates and states of the maintenance orders and gives links to more detailed information directly from the maintenance management system. All work orders issued for the same alarm are easily accessible along with the comments about the work done. This is valuable information for quick interventions in case of repeated problems.
- *Contact information for the equipment responsible* – Name, telephone and email address.
- *Alarm configuration information* – such as monitoring equipment details, references to any existing MoDESTI requests. This section also contains a direct link to the TIM alarm information to allow visualisation of the alarm concerned, which is often used for trouble shooting.

Help Alarm currently only exists for technical infrastructure alarms from the TIM system, but it has shown to be so useful that it should be extended to other systems. By giving the possibility for *on-line* data modifications, Help Alarm aids in keeping the alarm information up to date; an operator can easily initiate a modification directly from the GUI.

Another service connected with alarms is the *Alarm Notification System* (ANS); equipment groups can define *call-out lists* which are lists of telephone numbers to be called on the arrival of an alarm. It is possible to configure the LASER alarm system with an ANS identifier so that, when an alarm is activated, the corresponding identifier is sent to the ANS. In this case, the console alarm will be prefixed with an [A] to let control room operators know that an automatic notification has been issued. The notification can take the form of a telephone call, an SMS, an email message or any combination of these. An acknowledgement of the reception of the automatic call is sent to the control room operator by email.

CONCLUSION

Alarm management in the heterogeneous environment of the CERN technical services is a complex and sensitive domain. Not only do the technical components such as data collection, transmission and display have to be robust and sophisticated, catering for a wide variety of situations and functions, but the definition and maintenance of the alarms has to be rigorously applied.

The renovation of the control system for LHC operation was the opportunity to implement an open architecture with the necessary improvements allowing the flexibility and scalability needed to adapt to future requirements. Alarm data quality is assured by implementing a strict workflow giving control of the alarm definition and integration process to each concerned unit and providing full traceability of modifications.

The system, in operation since 2005, has proved successful and is ready to take on the remaining data for LHC operation in 2008. However, as organizations are dynamic by nature and continuously change, there is, and will always be, room for improvement.

REFERENCES

[1] B. Hollifield and E. Habibi, “Alarm Management: Seven Effective Methods for Optimum Performance”, ISA 1st Edition, 2007

[2] CERN TIS/GS, “Safety Instruction 37, ‘Level-3’ Safety Alarms and Alarm Systems”, Revision 3, CERN, September 2003, p. 3, http://edms.cern.ch/file/335802/LAST_RELEASED/IS37_E.pdf

[3] J. Stowisek, A. Suwalska, T. Riesco, ” TECHNICAL INFRASTRUCTURE MONITORING AT CERN”, EPAC’06, Edinburgh, June 2006 https://edms.cern.ch/file/750284/2/TUPLS135.PDF

[4] T.Pettersson "Engineering and Equipment Data Management at CERN - paper presented at MICAD 2003" https://edms.cern.ch/file/370320/1/micado1.doc

[5] D.Widegren “PLM at CERN - A True Challenge” PDT Europe conference Geneva, 24-26 September 2007 https://edms.cern.ch/file/865862/1/PDTE-PLM-at-CERN.doc

[6] EEMUA 191, "Alarm Systems: A Guide to Design, Management and Procurement", EEMUA, 2nd Edition, 2007.