Alarm system guidelines

Alessandro Caproni[*]

October 23, 2010

[*] European Southern Observatory

Contents

1 Foreword

In the rush of developing complex distributed control systems, the figure of the operator is often overlooked. The operator is in the front line of real time operations making decisions that directly impact the efficiency, profitability, reliability and safety of the telescope. Operators have a large amount of information as input into their work process: analyze information, diagnose situations, predict outcomes and take actions to deliver value.

The severity of consequences of abnormal situations is directly impacted by the operator's ability to recognize the initial abnormality, his ability to assess and diagnose the situation, and finally, the timeliness and the accuracy of the action he takes. Many of the accidents during the past twenty years may have been prevented, or they consequences minimized paying more attention to the role of the operator and the factors that surround him and in particular

- the operator interface,
- the alarm management system
- control room factors like lightning and position of the consoles
- operator training

In recent years, an effective alarm system has been recognized as an immediate aid in improving operator situational awareness and effectiveness. A poorly functioning alarm system is often noted as a contributing factor to the seriusness of upsets and incidents.

The purpose of this guidelines is to avoid the so called “Alarm Problem” when the alarm system is continuously acivated creating far more alarm events than can understood and acted upon by the operator.

2 What is an alarm

The alarm is an intentional interruption to the operator. An alarm is a mechanism for informing an operator of an abnormal process condition for which an operator action is required to mitigate or prevent process upsets and disturbances. The most important criteria to decide if an event is an alarm is to answer to the following question:

> “Does the event require an action?”.

The alarm system must be reserved for events that require operator action. Other events like for example those that are aimed to “operator information” not involving action should be presented by other tools.

What can be an operator action in the context of the alarm system:

- making process changes by manipulating the control system
- ask others to make changes to the system (for example manually operate an antenna)
- beginning troubleshooting/analysing a situation
- increasing the monitoring of a section of the process
- contact other people regarding the situation
- logging conditions for a later examination of the problem
- changing operating mode for example from automatic to manual

Alarms must exist as a tool for the operator and must not be configured as a tool for control engineers or other staff.

Alarms should be configured in such a way that a single process does not produce multiple alarms signifying the same thing. That is alarms should be configured on the best indicator of the root cause of a problem.

Alarms should always been activated as a consequence of an abnormal situation and never for expected cases of operations. For example, in the case of a device an alarm should be activated only if the device is not working *when it is supposed to work*.

Usually engineers that publish the alarms think on the device they are developing: if the device does not work then send an alarm; if the device is working then clear the alarm. However, in a distributed control system it is possible to do something more then that. It is for example possible to write a component that checks if the device works but that sends an alarm only if that device should work.

In a distributed control system is possible to write components that check part of the sytem and send alarms depending on its operational state.

The operator sometime plays a role in the alarm system. For example it is possible to add a graphic component with a button that the operator has to press while switching the state of the system to suppress the sending of noisy alarms.

And finally, when deciding if an event generates an alarm we have to think if that event is useful to the operator. Definitely alarms must be produced only when things go wrong.

3 Priority

Alarm priority is a means to convey the seriousness of a specific process condition to the operator and drives the operator's response.

Best practice principles of alarm management require that every individual alarm be assigned a priority using a logical and consisten approach. It is important that the distributed control system presents alarm to the operator with a priority that has a consistent meaning.

ALMA alarm service offers 4 priority levels: Critical, Emergency, High and Low. Best practices suggest that alarm priorites should be distributed as shown in table. Regardless of priority, all alarms require an action.

Priority	*Distribution*
Critical	rare
Emergency	5%
High	15%
Low	80%

4 Documentation

The alarms are part of the DCS database configuration. Since the documentation of alarms is dynamic and subject to change, it requires ongoing maintenance to ensure accuracy, operability and compliance with the standards.

For each point on the system, the following must be done:

- configure each possible alarm for that point
- check that all the configured alarms should exist
- check for duplicates and choose one that best describe the root cause of the problem
- set the priority of each alarm
  - verify the severity of the consequences if no action is taken when the alarm appear
  - determine the time available for the operator to respond to the alarm
- write the documentation: the cause, response of the operator to the alarm, other points involved by the alarm...
- determine the trip point of the alarm by checking the history of the alarm, the equipment and so on.

The team to discuss the documentation should ideally be composed at least of

- two operators (one for each shift)
- engineers familiar with the working of the system and the distributed control system

- engineers with the deep knowledge of the equipments

To classify each alarm, three grids need to be filled. The third and last one puts together the informations of the first two and determines the most appropriate priority for the alarm.

One of the questions to ask while documenting an alarm is "*How severe are the consequences if an alarm occurs and no operator action is taken in response?*". The severity could be one from none[1], minor, major and severe. The consequences must be evaluated in respect of personnel safety, environmental impact and finally cost.

This means that for each alarm the team should fill a 3x3 grid: the columns are the three severities[2], the rows are safety, environmental impact and cost. Having safety, cost and environmental impact in the same grid does not mean that they have the same importance, of course. The following grid helps determining the consequences of an alarm.

Category	*Severity none*	*Severity minor*	*Severity major*	*Severity severe*
Personell safety	No injury	Slight injury (first aid).	Reversible health effect (such as skin irritation)	Severe injuries
Public / Environment	No effect	Local envirnmental effect	Non permanent damage	Limited or extensive damage
Costs / Downtime / Quality	No loss	Cost or damage less then min threashold	Cost or damage between min and max thresholds	Cost or damage gretaer then max threshold

While discussing alarms, the team should concentrate on each alarm and not to cascade of alarms. Each alarm must be considered as the only event when filling the grid. This grid must be filled quite verbosely.

Another parameter to consider is the maximum time within the operators can take actions to mitigate a problem i.e. it is how much time is available to take the effective action from when the alarm is emitted to when the consequences becomes unavoidable, regardless of the action. The consequence of an uncorrected alarm generally worsen with the passage of time therefore the shorter the time available to respond, the higher the priority of the alarm will be. It is usually a good practice to divide the alarms in three categories depending on the response time, and fill the following table.

Description	*Max response time*
No alarm	$>$ 30 minutes
Promptly	10 to 30 minutes
Rapidly	3 to 10 minutes
Immediately	$<$ 3 minutes

Alarms that need a response in less then 3 minutes (immediately) are the alarms the request an immediate action interrupting whatever else activity the operator is doing. If the reaction time is between 3 and 10 miutes (rapidly) then the action has to be executed in a short time. If the reaction has to be taken between 10 and 30 minutes then an action has to be taken but there is time to do something before. Finally, if the response must be taken in more then 30 minutes there there is no need to set an alarm.

It is inappropriate to fire a alarms for which no action must be taken for more then 30 minutes because for such a situations there are no quick action needed nor there is an urgency. However there are exceptions to this rule and an alarm can be justified, An example could be a maintenance needed because a detector found corrosion in an equipment: an action must be taken but it could be at the end of the shift.

The two set of properties we examined upon, severity of consequences and reaction time, can be used to determine the most appropriate priority of an alarm as described in the following table.

[1] If the consequences are classified as *none* then there is no need to have the alarm.

[2] Note that in ALMA there are 4 severities so in the grid there are 4 columns.

Max Time to react	*Consequence severity: minor*	*Consequence severity: major*	*Consequence severity: severe*
>30 min	No alarm	No alarm	No alarm
10-30 min	Low	Low	High
3-10 min	Low	High	High
<3 min	High	Emergency	Emergency

If the process described above has been correctly performed the distribution of the priorities should be as recommended in Section 3. If you decide to use the Critical priority, the first requirement is that such an alarm is a Emergency in the table and then promoted to Critical: the rules for promoting an alarm should be clearly stated in the alarm system documentation. The number of Critical alarms should be very low.

There are cases of alarms that do not fit in the table above for any reason. In this case it is better to set their priorities as required but clearly document the reason.

To be consistent all the process should be well documented and for each alarm should be documented (at least):

- the cause of the alarm
- corrective actions
- potential consequences
- time available to the operator to respond

Documenting alarms in this way has an impact in operating methodology for most operators:

- every alarm requires a response i.e. is unacceptable to ignore an alarm
- every alarm is documented and has an identified response
- alarm priority is used to distinguish the order of response

Even if we can take a great advantage because of the big number of replicated identical equipments in our environment, the documentation process usually lasts long and involve several persons so the cost is not trivial and has to be taken into account.

A Abbreviations

- *ALMA*: Atacama Large Millimiter Array
- *ACS*: ALMA Common Software
- *AS*: Alarm System or Alarm Service
- *DCS*: Distributed Control System

References

[1] Alarm systems a guide to design, management and procurement, 2007.

[2] Peter Bullemer, Dal Vernon Reising, Catherine Burns, John Hajdukiewicz, and Jakub Andrzejewski. *Effective operator display design.* ASM Consortium guidelines. Abnormal Situation Management Consortium, 2008.

[3] Alessandro Caproni et al. *Alarm system: software architecture and HowTo manual.*

[4] Bill R. Hollifield and Eddie Habibi. *Alarm Management: seven effective methods for optimum performance.* Instrumentation,Systems, and Automation Society, 2007.