ISC Safety Lore

June 2020

Issue 10

Key lessons from incidents related to alarm management

Introduction

Alarm systems are important in monitoring the condition of the plant. Alarms assist personnel to maintain a system or process within a safe operating envelope. The objective of alarm management is to provide operators with a consistent and reliable action event notification interface that supports their efforts to operate the process while ensuring they are not overwhelmed safely and efficiently with unnecessary information.

Case 1 – Gas plant

A major explosion and subsequent fire occurred in a gas plant. Two people died and eight were injured in the incident. The plant had been suffering from operational upsets following pigging of the upstream gas pipelines. A warm liquid ("lean oil") system failed, allowing a metal heat exchanger to become intensely cold and therefore brittle. When operators tried to reintroduce warm lean oil, the vessel fractured and released a large quantity of gas which found an ignition source and exploded.

Key learning points

The direct cause of the incident seemed to be loss of lean oil flow leading to a significant reduction in temperature of a heat exchanger. On the day, the lean oil recovery system which extracts Liquified Petroleum Gas from the condensate stream had tripped and the plant operators were struggling to restart production. It was common that many process alarms were active at one time, many of them considered to be nuisance alarms. There was lack of identification of safety critical alarms. That resulted in slow response to the loss of oil flow. Operators were expected to deal with at least three or four hundred alarms a day. A past incident occurred in the plant where investigators revealed that for a 12-hour shift, 8500 alarms went off, which means 12 alarms every 60 seconds. Operators followed a practice to silence the audible alarms and switching the visual ones from flashing to steady state. In addition to that, the display could only contain a certain number of alarm signals. Once that number was exceeded, existing alarms would be hidden by a new page of alarms, making it impossible for operators to follow-up on the current situation.

Case 2 – Oil refinery

A lightning strike started a fire on the crude distillation unit. The ensuing plant disturbances and power interruptions affected the vacuum distillation, alkylation units as well as the fluidised catalytic cracking unit (FCCU) where the explosion occurred, resulting in the release of 20 tonnes of flammable hydrocarbons from the outlet pipe of the flare knock-out drum of the FCCU. Twenty-six people were injured in the incident, and the explosion caused significant production loss.

Key learning points

In terms of alarm management, the large number of control room alarms during the process upset conditions made it difficult to operators to assess and reflect on what was happening. As the investigation revealed, too many poorly categorised alarms overwhelmed the operators as the process upset developed. Observations from the distributed control system alarm records indicated that during the incident, alarms were being presented to operators at the rate of one every two to three seconds. In the last ten minutes before the explosion the two operators had to recognise, acknowledge, and take appropriate action on 275 alarms. Alarms going off this frequently resulted in operators cancelling them because of their nuisance value without necessarily recognising what they meant. As most alarms were assigned the same high priority, virtually all were presented on the area alarm summary and the operators were unable to tell which alarms were critical to safety and which were not. There was no philosophy for determining what priority an alarm should have and no control was exercised over the number of alarms in the system. The use and configuration of alarms should be such that safety critical alarms, including those for flare systems, are distinguishable from other operational alarms; alarms are limited to the number that an operator can effectively monitor; and ultimate plant safety should not rely on operator response to a control system.

Each alarm should have a clearly defined purpose, such as safety, equipment failure, abnormal process conditions or product quality. The correct number of alarms should be determined by operability criteria. Preferably, there should be as few safety critical alarms as possible. These should be limited to those situations where a wider knowledge of the process conditions is required than can be provided by any automatic protection system.

The ISC believes that leadership across six key functional elements is vital to achieve good process safety outcomes. These elements are:

- systems & procedures
- engineering & design
- assurance
- knowledge & competence
- human factors
- culture

In the *What can I do* section below you can see how each of these elements plays a part.

Figure 1: The ISC Framework

What can I do?	
Management	
	• The use and configuration of alarms should be such that: safety critical alarms are distinguishable from other operational alarms; alarms are limited to the number that an operator can effectively monitor; ultimate plant safety should not rely on operator response to a control system alarm; and alarms must have a specific action required.
	• Make sure that the company has an alarm philosophy in place and keep it up-to-date.
	• Make sure to implement lead process safety metrics to measure the performance of the alarm system together with regular audits taken place.
	• Display systems should be designed to provide an overview of the condition of the process including, where appropriate, mass, and volumetric balance summaries.
	• Make sure that alarms are prioritised and there is adequate time for the operator to respond with defined prioritisation rules (based on the potential consequences if the operator fails to respond in the correct time). It is best to prioritise proportionately, e.g. 5% high priority, 15% medium, and 80% low.
	• Improving alarm management has to continue through the life-cycle of the plant via the Management of Change and the plant Safety Management System to maintain control and ownership.
	• Investigate all incidents or near misses where operators missed alarms or initiated an incorrect response.
	• Ensure new alarms or modification of existing systems are covered in Management of Change.
	• Make sure that there enough operators and supervisors to manage upsets properly, and that they are there when needed.
	• Set up clear roles and responsibilities for normal and abnormal conditions and have a thorough training system in place to ensure that supervisors and operators have the adequate level of competency.
Process Engineer/Supervisor	
	• Check if operators experienced being overwhelmed by alarm 'floods'; if there are nuisance alarms, eg are large numbers of alarms acknowledged in quick succession, or if audible alarms regularly turned off.
	• Make sure that the operator training covers topic of how to handle alarm floods and if operators know what to do with each alarm.
	• Ensure that operators report all upsets in the process and that those events are investigated.
	• Make sure that operators understand and follow the alarm prioritisation and action rules.
	• Make sure that there are enough operators to manage upsets properly, and that they are available when needed.
	• Track alarm data and metrics, and review to see where alarms can be rationalized.
Operator	
	• Make sure that you know what to do with each alarm and have a clear understanding of alarm prioritisation.
	• Check if the control room displays are well laid out and easy to understand; support is available, written or on-screen.
	• Make sure that you can easily 'navigate' around the alarm pages and that all terms used on screen are understood and clear. If unsure, ask the supervisor.
	• Make sure that your roles and responsibilities are communicated clearly both for normal and abnormal conditions and that you are trained what to do in such circumstances.