PROCESS SAFETY AND ENVIRONMENT PROTECTION 87 (2009) 3–13

Contents lists available at ScienceDirect

Process Safety and Environment Protection

journal homepage: www.elsevier.com/locate/psep

Hazards equal trips or alarms or both

Clive Timms

Strathayr, Rhu-Na-Haven Road, Aboyne, Aberdeenshire AB34 5JB, United Kingdom

ABSTRACT

Anyone who has been involved in the application of IEC 61508 and IEC 61511 by undertaking the Safety Integrity Level (SIL) determination for Safety Instrumented Systems (SIS) will appreciate the amount of effort and tenacity that is required to undertake the task. SIL determination of Safety Instrumented Systems requires considerable commitment and tenacity to get the job done, but it is like climbing to the top of a hill only to be faced with a mountain when we come to consider what is involved in reviewing or configuring a typical alarm system.

A medium sized process facility may have a few hundred or so primary Safety Instrumented Functions (SIF) or trips configured into a Safety Instrumented System, but the number of alarms configured into a process control system (PCS), that need to be assessed and prioritised, can often run into the thousands.

There is synergy between safety instrumented functions and alarms because they both make a contribution to reduce the risk of having unwanted events, and both need an assigned appropriate criticality.

This paper details various methods of criticality assessment which have been successfully applied to set the appropriate priority, identify the critical alarms that need to be upgraded to trips and to rationalise those of no value. It will also cover the use of software tools which can significantly reduce the effort involved in this process.

Keywords: Alarms; Trips; Prioritisation; Rationalisation; SIF; SIL; Risk

1. Introduction

Anyone who has been involved in the application of IEC 61508 (IEC, 1998–2000) and IEC 61511 (IEC, 2003) and the Safety Integrity Level (SIL) determination for Safety Instrumented Systems (SIS) will appreciate the amount of effort and tenacity that is required to undertake the task. SIL determination of Safety Instrumented Systems, or shut down systems as they are traditionally called, requires considerable commitment and tenacity to get the job done, but it is like climbing to the top of a hill only to be faced with a mountain when we come to consider what is involved in reviewing or configuring a typical alarm system.

A medium sized process facility may have a few hundred or so primary Safety Instrumented Functions (SIF) or trips configured into a Safety Instrumented System. These need to be assessed and assigned an appropriate SIL, but the number of alarms configured into a process control system (PCS) that need to be assessed and prioritised can often run into the thousands. The requirements for alarms usually involve different disciplines such as instruments, process, maintenance and the operators themselves. The latter often have the misconception that their life will be easier if they have alarms on everything. Thus the demand for more alarms, along with the ease of configuration afforded by PCS's, regularly leads to a proliferation of alarms. In other words, alarm configuration can all too easily get out of hand.

There is synergy between safety instrumented functions and alarms because they both make a contribution to reducing the risk of having unwanted events, and both need an assigned criticality. It is also important to be able to determine when an alarm should be upgraded to a trip to provide automatic protection, and conversely, when a trip can be downgraded to alarm status.

A SIF is engineered to provide protection against a hazard caused by some kind of failure, and has a concise and automatic role to play when a process moves out of its normal operating envelope. Using good practice to comply with the IEC 61508/61511 standards, a risk assessment can be undertaken to determine its criticality or SIL.

This risk assessment is related to the consequences that would occur if the SIF were to fail on demand and the frequency of a demand on the SIF. The consequences can be any combination of safety, societal, financial and environmental impact.

E-mail address: c.timms@ifb.co.uk.
Received 2 March 2008; Received in revised form 18 July 2008; Accepted 26 July 2008

doi:10.1016/j.psep.2008.07.003

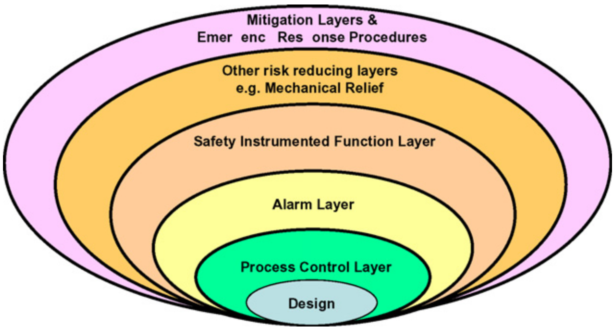

Fig. 1 – Typical risk reduction layers.

An alarm function works through the human interface – 'A Methodology for Alarm Classification and Prioritisation' – (Timms, 1999) to provide an early warning that the process has moved away from the normal operating envelope in order to:

- Alert the operator to disturbed plant conditions.
- Provide indication of further developments that may need attention.
- Trigger a trained operator response.

Alarms normally contribute to the overall risk reduction as they represent one of the many typical independent risk reduction layers as shown in Fig. 1. The criticality of the alarm should also be assessed in order to set an appropriate priority. It therefore makes sense to assess the criticality of an alarm in a similar way to a SIF, but based on the consequences that would follow if the alarm fails or is missed by the operator.

However, the contribution that an alarm makes to risk reduction can become clouded if the operator cannot identify the important alerts against a background of alarm problems. The three main problem areas that can potentially compromise safety, production and the environment are:

- Nuisance alarms.
- Standing alarms.
- Alarm avalanches or floods.

Nuisance alarms and standing alarms are usually caused by instrument faults, out-of-service equipment or inappropriate limit and/or dead-band settings. They can be relatively easily identified and rectified by maintenance or adjusting the configuration parameters. However, alarm avalanches or floods are usually the result of consequential or secondary events following a primary event, and the more alarms that are configured; the more there are to appear before an operator in a plant upset condition. The problem for the operator is how to distinguish between the primary initiating event and the secondary consequence events.

The primary objective must therefore be to rationalise the alarm system to a configuration which alerts the operator to alarms in order of importance, so as to give him/her the best chance to take corrective action. Inability to take corrective action can have significant safety, economic and environmental consequences. We must also eradicate those alarms that serve no purpose as this will significantly reduce the alarm overload. This can be achieved by a well-defined methodology, and the effort can be significantly reduced by engaging specialist software tools as discussed later.

1.1. *The UK HSE position*

The UK HSE often uses the Texaco Refinery explosion in 1994 as the prime example of how the poor application alarms and human factors can result in serious incidents—HSE, 1997. This paper is not going to regenerate the UK HSE findings, but their position on alarm handling has been made very clear. They have produced an UK HSE information sheet 'Better Alarm Handling' (UK HSE, 2000) to provide some basic guidance, and the Hazardous Installations Directorate (HID) have outlined their strategy with respect to inspection and enforcement, and their expectations with respect to users and designers, in an article entitled 'Better alarm handling—a practical application of human factors' (Wilkinson and Lucas, 2002).

In both publications the UK HSE guidance provides a simple three-stage approach:

- Find out if you have a problem.
- Decide what to do and take action.
- Manage and check what has been done.

The HSE also reference the Engineering Equipment and Materials Users Association (EEMUA) publication 191, 'A Guide to Design Management and Procurement' (EEMUA, 1999) as 'the nearest thing to a standard currently available'.

2. Undertaking an alarm rationalisation exercise

2.1. *Avoid the common pitfalls*

The initial reaction when faced with alarm problems can often be to look for ways of using technology to suppress unwanted alarms. PCS vendors are eager to demonstrate how sophisticated their technology can be and commit their customers to using these techniques. There may be possible scenarios where suppression of alarms is simple (e.g. main and standby equipment with auto changeover) but as a rule, the more complex the plant then the more complex the suppression scenarios, leading to very time consuming and complicated solutions. It is also all too easy to loose the focus due to the complexity, and this could result in flawed logic for the scenarios and hence compromise the alarm integrity.

An alarm flood reduction will almost certainly require a rationalisation exercise to challenge each alarm and reduce the number of configured alarms. In essence, an alarm review following the methodology outlined below, in conjunction with software tools to aid the process, will achieve the most significant benefits. Channelling efforts into this type of activity should be the first priority.

2.2. *Software tools will help*

The quantity of data to be manipulated, sorted and rationalised will often be considerable, and can amount to thousands of alarms on a modest size process facility. It makes little sense to undertake an alarm review as a paper exercise, since dealing with large numbers of alarms will simply overwhelm those involved in the process, and the final paper report will be hard to manage and update as it will only represent a snapshot in time. It can be tempting to use spreadsheets to manipulate the data, but they are not the most appropriate solution since they do not have the integrity or sorting power afforded by database-based approaches.