The Cost / Benefit of Alarm Management

An Economic Justification for Alarm System Re-engineering

© 2000 Plant Automation Services
The Cost/Benefit of Alarm Management

An Economic Justification for Alarm System Re-engineering

Introduction

All modern industrial control systems provide alarm management to assist process operators in managing abnormal situations. The integrity and effectiveness of alarm management can either provide assistance or hindrance to the process operator in responding to these situations. Through the efforts of the Abnormal Situation Management Consortium, EEMUA, and other such professional groups, a large amount of best practice information exists to aid the control system engineer in designing effective alarm systems. However, legacy systems must generally be re-engineered in order to take advantage of these newer system capabilities and best practices. The re-engineering of alarm management in these legacy systems is a responsible first step in responding to the increasing frequency of industrial incidents and to begin to address the billions of dollars these incidents cost manufacturers annually. By any comparison, the re-engineering efforts are well worth the investment. Nevertheless, today’s business climate virtually forces managers to justify these investments on a financial return basis. This white paper presents a model for justifying an alarm system re-engineering project, and provides two case studies showing the application of the model.

The Alarm Problem

The basic purpose of an alarm system is to indicate the presence of an abnormal situation so that the operator can intervene to prevent escalation of the event. A properly designed alarm system assists the operator by indicating abnormal situations quickly and simply, while an improperly designed alarm system distracts, confuses, or fails to notify the operator of abnormal situations. When the alarm system plays an adverse role, the result can be production disruption, environmental violations, and/or equipment damage.

Serious industrial accidents can also occur. The near-meltdown at Three Mile Island, the most publicized industrial accident in the history of US industry, is a case in point. As documented (1, 2, 3) the incident was closely related to the poor design of the operator interface. A saturation of 110 alarms hindered operators for 2.5 hours before they were able to understand the problem. Poor layout, visibility of process indicators, and over-instrumentation of the process leads Perrow (2) to a comment that can be applied to any control system: “Operators err, it seems, in not being able to fully surmount the inadequacies and complexities of the equipment they must use.”

A second accident where poor alarm management was implicated occurred in 1994 at a UK refinery. The accident resulted in plant damage that cost £48 million (~US$70M) to repair, plus more than £200,000 (~US$300,000) in fines by the government safety regulator (4).

Admittedly, alarm systems are not the only contributing cause to abnormal situations. Inherently safe process design, training, and proper maintenance practices never lose their importance. The question then follows: How often are alarm systems improperly designed? According to D. Campbell Brown, studies show that the potential benefit of re-designing alarm systems is 5 to 8 percent of process throughput (up to $8 million for a typical refinery). “Evidence, including the official enquiry reports from several industrial accidents, has shown that poorly performing alarm systems can be implicated in abnormal situations, which altogether represent a huge cost to the U.S. petrochemical industry.” Also, “A recent study by the ASM Joint Research & Development Consortium estimated the cost of preventable abnormal situations in the U.S. petrochemical industry at $20 billion annually (4).”

Such events as those cited above have led to standards such as the ISA S84.01, IEC 61508 and IEC 61511 for the design and implementation of safety instrumented systems. OSHA has now adopted S84.01 along with other Process Safety Management (PSM) requirements as necessary for regulatory compliance in 29 CFR 1910.119. A plant must be able to demonstrate compliance to OSHA to continue operating. Section E of the regulation states: “The employer shall perform an initial process hazard analysis (hazard evaluation) on processes covered by this standard. The process hazard analysis shall be appropriate to the complexity of the process..."
and shall identify, evaluate, and control the hazards involved in the process.” Process alarms are part of the strategy to control hazards involved in the process and are subject to all PSM requirements (5).

In summary, a substantial portion of abnormal situations which result in significant loss can be attributed to improperly designed alarm systems. Therefore, it is important to evaluate the alarm system to ensure that it is configured to prevent the escalation of abnormal events. To make this evaluation and provide a financial justification for making the necessary improvements, a model will be required.

### Model for Assessing Control System Re-Engineering Benefit

The alarm system is a component of the protection layers in an industrial process. As described by Mostia (6), the layers are:

1. Process Design
2. Basic Process Control System
3. Critical Alarms
4. Safety Instrumented Systems
5. Mechanical protection means
6. Mitigation means
7. Plant emergency response

Each protection layer becomes active later in the chain of events resulting from an incident. Starting with layer 6, the intent is not to prevent an accident, but to minimize the severity.

Alarm systems are integral to protection layers 2-4. In order to justify the effort to re-engineer the alarm system, a model will be used to quantify the contribution of protection layers 2-4 to abnormal situation management. In order to comply with the ISA S84.01 standard and OSHA, there are 5 steps involved in analyzing the contribution of these layers. The steps are:

1. Establish Process Safety Management practices. These must be in place to have a consistent design approach for an alarm system and to meet OSHA regulations.
2. Conduct a Process Hazard Analysis. This analysis identifies potential hazards (HAZID) and analyzes the impact of a hazard (HAZOP/HAZAN). Estimates can be made to quantify the predicted cost of the four categories of loss in an industrial accident:
   - Production loss (tons/units) = Duration of outage * Production Rate
   - Impact of regulatory violation (mandated shutdown) = Cost of forced outage plus fines
   - Replacement cost of property/equipment
   - Injury/Loss of life. Site medical records are typically filled out when an injury is treated, and can be tabulated to yield accident frequency by severity (minor, serious, disabling, death). There is evidence that supports this approach. A 13 year study in a major chemical plant shows that for every fatality, there are 29 disabling injuries, 877 serious (SOHIO serious injury index method), and 8,618 total injuries. Furthermore, studies show that there is better than 99% confidence that serious injury frequency is strongly related to total injuries, as well as disabling injuries. Heinrich’s formula (300 minor injuries – 29 serious injuries – 1 major injury) was supported by the Monsanto, Texas City study from 1952-1966 (6).
3. Determine the target time between incidents. Commonly, a figure such as 10,000 years between incidents has been used (6, 12). This is determined by each company or industrial facility, and depends upon the nature of the hazard or loss.
4. Use a Fault Tree Analysis (FTA) (6, 7) to determine the effectiveness of the existing safety systems to meet the target time between incidents. The objective is to build a logic diagram that shows the probable causes and existing safety checks for undesirable events. Each of the elements is assigned a frequency (# incidents/time) or probability of occurrence. Some are assigned objectively (from experience), and others are assigned based on hard data.

   There are 3 types of logic blocks used to calculate the frequency of failure:
   - For probability inputs (failures/attempt) as opposed to frequency (failures/time). Calculated as the multiplication of the inputs.
   - Summation of the input frequencies
Calculate using the following formula, as documented by Goodner (11):

\[
\text{Failure Rate} = \frac{\text{Failures}}{t} = \ln\left(1 - \sum_{n=1}^{\#\text{inputs}} \prod_{t}(1 - e^{(-\lambda/\text{time})})\right)
\]

where:

\( \lambda \) = failure frequency of the component, failures/time

\( t \) = period of evaluation, same time units as frequency

\( \prod \) = multiply a series of terms

5. If the existing system is inadequate (predicted time between incidents < desired time between incidents), engineering and administrative controls can be used to reduce the likelihood of an event. Engineering and administrative controls include process control, alarms, and safety systems.

Note that certified professionals in risk assessment should conduct the FTA. These professionals are often found on staff from the industrial manufacturer, or are available as outside resources.

As an example of the use of the model, in a semiconductor facility it is desired that a shutdown be avoided for 2 years. Facility data indicates that the cost of a shutdown is $500,000 per day. In Figure 1, the root causes of the shutdown are specified as the number of events/year, as noted at the bottom of the FTA. The auto bottle switch control is expressed as a probability rather than a frequency.

The FTA indicates the frequency of a line shutdown is 4.88 times per year, thus the annual cost of shutdowns is over $2,000,000. With this data, the cost of re-engineering the alarm system can be justified. After the re-engineering project, the FTA is repeated with the results shown in Figure 2. The re-engineering achieved the goal of 2 years between incidents.

Case Study #1: Hydrocarbon Processing

This simplified case study from the hydrocarbon processing industry demonstrates how the model can be used to detect and correct an alarm system that contributes to operator error.

An oxidation reactor takes hot hydrocarbon feed and mixes it with air. The heat of the hydrocarbon feed and the heat of the exothermic oxidation is removed by cooling water coils in the reactor. Insufficient cooling from the cooling water increases the reactor
temperature and decomposes the unstable product (oxidized hydrocarbon). This decomposition reaction is exothermic and will generate more heat, which can lead to loss of containment and explosion.

The reactor is protected by a safety instrument system. When the safety system activates it costs the company approximately $750,000 in business interruption, so the goal of the operator is to prevent the safety system from activating.

The reactor cooling coils are supplied with water by an electrical pump and a steam driven pump. The failure rate of the electrical feed to the pump is 1 failure every 5 years, or 0.20 failure/year, while the steam source supplied to the steam driven pump is very reliable. If the electrical feed fails, shutting down the electric driven pump, the outside operator must start the steam driven pump. However, the cooling water flow provided by the single steam driven pump is not sufficient to remove heat from the reactor. Thus, the operator must reduce air feed to the reactor to prevent a complete reactor shutdown.

A study by the company indicates that an operator can successfully prevent a shutdown 60 percent of the time. However, an improper (or no) response will occur 4 out of 10 times (40 percent probability). This poor response rate is due to confusion caused by a flood of alarms (cooling water low flow, pump off normal state, reactor temperature rate of change, exit oxidized hydrocarbon temperature and rate of change). The confusion results in a delay in cutting air supply to the reactor, and thus the reactor shuts down.

Therefore, failure of electric power to the cooling water pump (0.20/year) will result in one shutdown in every 12.5 years (0.08/year, see Figure 3). This shutdown rate corresponds to a cost of $60,000 per year. With an appropriately designed alarm system, the alarm flood is minimized or eliminated, allowing the operator to properly respond 90 percent of the time. This will reduce the shutdown frequency to once every 50 years (see Figure 4).

Analysis of the remainder of the unit will likely show other opportunities for improvement. When taken in total, financial justification for the re-engineering should be apparent.

**Case Study #2: Pulp and Paper**

This more complex case pertains to a recovery boiler, an area of great concern for a pulp mill. The Black Liquor Recovery Boiler Advisory Committee (BLRBAC) has documented 156 explosions and 450 near-miss incidents in the last 35 years. The nature of these incidents is summarized by Lefebvre and Santyr as follows: “In addition to equipment damage, some of the more severe explosions have resulted in injury or even death of operating personnel. There have also been several hundred emergency shutdowns where the fear of an explosion has led to a forced outage. The frequency of explosions has remained relatively constant over the years, and the problem cannot be considered solved (8).”

Many of these incidents have occurred due to leaks in boiler tubes resulting in contact between boiler water and the liquid smelt. Fortunately, there are leak detection methods used in the industry (9) to alarm operators before an accident occurs. Another cause of boiler explosions is adding fuel and air to the boiler during a blackout (no flame) condition. Thus it is important to alarm low O2 in the firebox. These are not the only alarms applicable to a recovery boiler. The BLRBAC checklist for instruments and control systems of
recovery boilers includes 103 different conditions for which alarms are recommended on a recovery boiler. Considering the importance of the alarm system in this type of unit, it is important to make sure that the alarm system is properly designed.

Having stated the importance of the alarm system for safe operation of a recovery boiler, the task remains to quantify the benefit of alarm system re-engineering for this type of unit consistent with the practices established by BLRBAC. An FTA will be used for this purpose. To begin, the HAZAN/HAZOP is conducted. In this case, the outcome of a recovery boiler explosion is:

- **Production loss** – The outage from a boiler explosion is 3 months. There are 2 recovery units on site, so losing one unit curtails production 50%. For an operation producing 1000 tons/day, this is a loss of 45,000 tons of product.

- **Property loss** – To re-build a recovery boiler following an explosion is a cost of $50 million.

- **Safety** – For a severe explosion, the likely outcome is 3 fatalities, 4 disabling injuries, 12 serious injuries, and 20 minor injuries.

![Figure 5: Predicted Incidents Before Re-engineering](image)

The company has determined that the desired time between incidents is 10,000 years. In Figure 5, the effectiveness of the existing safety system is examined for a blackout.

The FTA indicates that the probability of an explosion resulting from a blackout is 935 years (over ten times more likely than desired). This statistic means that during an operator’s 15-year career there is a 1 out of 62 chance he will see an explosion. If the operator does see the explosion, there is a 1 out of 21 chance he will be killed, and a 1 out 5 probability that he will have an injury that will effect his or her lifestyle. With the high incident and annual cost, and the safety concerns, the FTA provides the required financial justification for the re-engineering effort.

The many nuisance alarms in the system leads operators to a low regard for alarms, hence the rate of alarm response failure is 50 percent. In addition, the high-combustibles alarm does not provide any protection because by the time the alarm activates there is not adequate time for mitigation. Also, many alarms do not have a specified response action so real alarms lose their importance (e.g., the operators hide the fan alarms by placing black electrical tape over the keyboard alarm LED). This situation makes the operators less responsive to the relatively rare low oxygen alarm (14/year based on operating history).
After addressing the alarm issues, the alarm system provides a significant protection layer against blackout, and reduces the probability of an explosion. Figure 6 shows the fault tree analysis with improved operator response.

By eliminating nuisance alarms and consolidating simultaneous alarms into a single indicator, the operator has an increased ability to respond to incidents. The demonstrated responsiveness changed from a 50 percent failure rate to a 10 to 20 percent failure rate. This leads to a lower incidence of explosion (9.72E-5/year). Thus, the calculated time between incidents (10,300 years) meets the goal and the probability of an accident and economic loss is minimized.

### Conclusion

The contribution of alarm systems to industrial loss cannot be ignored. As documented, improperly configured alarm systems contribute to accidents at a non-trivial rate. Although alarm systems are intended to minimize incidents, too often they amplify the consequences of these incidents. Duplicate alarms, nuisance alarms, and improperly prioritized alarms all contribute to operator confusion, and thus increase accident frequency.

Alarm system deficiencies can be corrected through alarm re-engineering. The re-engineering process restores the alarm system to a useful state by eliminating duplicate and nuisance alarms, and ensuring that the necessary alarms are properly prioritized and documented.

But in order to attain the required funds for a re-engineering effort, data must be available that demonstrates a financial return for the project. As demonstrated by the case studies, the required data can be attained using the FTA model. The model provides a methodology for determining the cost (environmental, property, and human loss) due to accidents, and for determining the probable frequency of incidents. This data can then be used to justify an alarm re-engineering project, resulting in an alarm system which assists the operator in detecting and responding to incidents in a timely manner.

### End Notes


