# Using Alarms as a Layer of Protection

**White Paper**
**exida**
**80 N. Main St.**
**Sellersville, PA**
**www.exida.com**

**April 2012**

exida White Paper Library
http://www.exida.com/Resources/Whitepapers

**Keywords:** Alarm Management, ISA-18.2, Independent Protection Layers, Alarm Rationalization, EEMUA 191, Safety IPL Alarms, Operator PFD, Operator response to alarms

## Abstract

Alarms and operator response to them are one of the first layers of protection in preventing a plant upset from escalating into a hazardous event. This paper discusses how to evaluate and maximize the risk reduction (or minimize the probability of failure on demand) of this layer when it is considered as part of a layer of protection analysis (LOPA).

The characteristics of a valid layer of protection (Specific, Auditable, Independent and Dependable) will be reviewed to examine how each applies to alarms and operator response. Considerations for how to assign probability of failure on demand (PFD) will be discussed, including the key factors that contribute to it (e.g., operator's time to respond, training, human factors, and the reliability of the alarm annunciation / system response). The effect of alarm system performance issues (such as nuisance alarms and alarm floods) on operator dependability (and probability of failure on demand) will be reviewed. Key recommendations will be drawn from the ISA-18.2 standard "Management of Alarm Systems for the Process Industries".

## Conclusion

Operator response to alarms (safety IPL alarms) can be used to reduce risk as part of a layer of protection analysis. In order to accurately estimate their risk reduction credit, it is important to understand the design of the system, the operator's environment and the alarm management practices and procedures that will be used during operation.

This paper has shown that reliability of the hardware (sensor, logic solver, HMI, final element) provides a lower limit for the probability of failure on demand for a safety IPL alarm. The example calculations yielded a hardware contribution of .045 and .024 for BPCS and SIL-rated hardware respectively. This means that it is impossible for a safety IPL alarm to achieve a PFD of 0.01 (SIL 2) even with perfect operator reliability. It also means that it is important to validate the reliability of the hardware that is being used as part of a safety IPL alarm. The selection of SIL-rated hardware can improve performance, but in general the PFD for a safety IPL alarm is dominated by the operator's ability to detect, diagnose and respond to the alarm correctly and within the required time.

As discussed, a primary factor in the operator's reliability is the performance of the alarm system itself. Consequently additional criteria have been proposed for evaluating whether an alarm is a valid IPL. In addition to being Specific, Auditable, Independent and Dependable, the following criteria address the performance of the alarm system and help ensure a well-functioning alarm system is provided for the operator.

- The alarm must be proven to be valid when it is first proposed / identified.
- The alarm system must be rationalized.
- Alarm system performance must be measured and proven to be adequate

If the alarm system has not gone through rationalization and / or its performance has not been proven to be acceptable based on comparison to metrics established in ISA-18.2, then it is recommended that a PFD of no less than 0.5 be used for a Safety IPL alarm. Certainly it would be inappropriate to claim a PFD of 0.1 in a LOPA (risk reduction factor of 10) if the operator is subjected to nuisance alarms, alarm floods and is not provided with alarm response procedures. In some cases it may be more appropriate to eliminate any credit altogether unless the above criteria have been met.

## Introduction

The purpose of an alarm is to notify the operator of an equipment malfunction, process deviation or abnormal condition that requires a response.  Alarms help the operator keep the process within normal operating conditions. They also play a significant role in maintaining plant safety, providing a means of risk reduction (layer of protection) to prevent the occurrence of harm from a process hazard as shown in Figure 1.

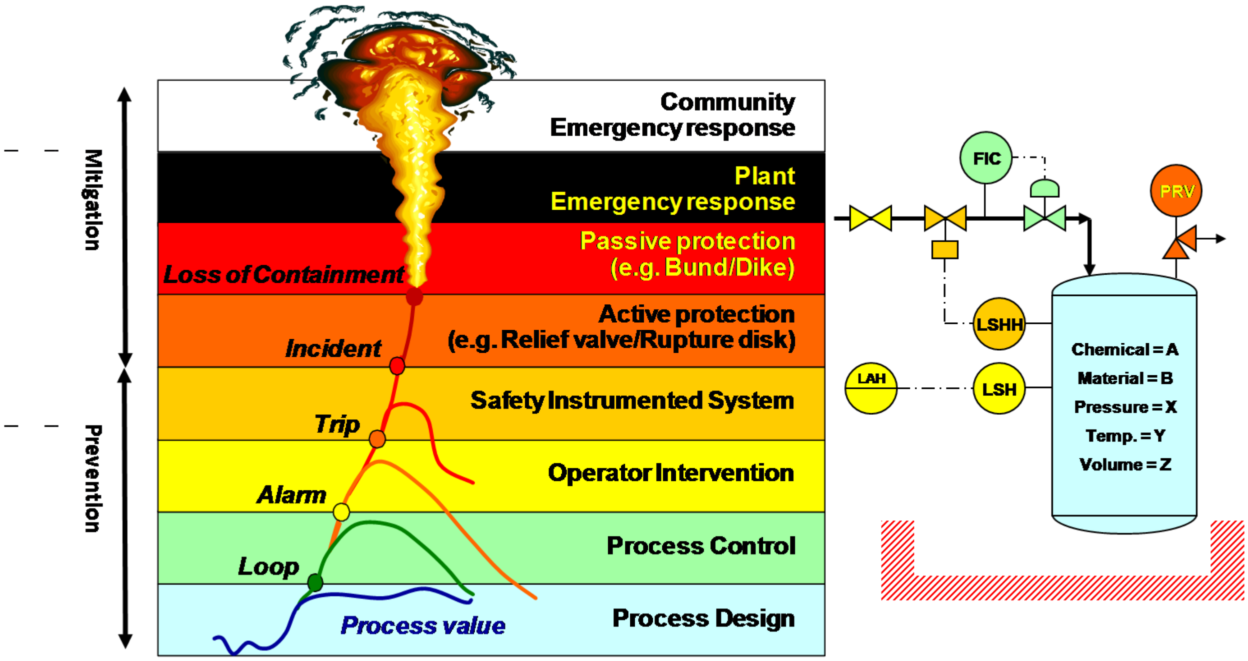


Figure 1. Layers of Protection and Their Impact on the Process

Unlike other layers of protection, such as a relief valve or safety instrumented system (SIS), the operator’s response to an alarm is not an automatic action but instead is a manual action which is subject to human error. Because of the inherent unreliability of human behavior, many safety practitioners struggle when determining the credit that can be taken for the alarm in a layer of protection analysis (LOPA). Some practitioners are very conservative taking no credit (a risk reduction factor =1.0), while others are very optimistic taking risk reduction > 10 (SIL 1 or greater). Since the operator response to an alarm should never be the last line of defense in preventing significant harm, it is often used in conjunction with a safety instrumented function (SIF).  In this scenario the credit taken for the alarm layer has a direct impact on the required safety integrity level (SIL) for the SIF.

When alarms fail as a layer of protection, catastrophic accidents, such as Milford Haven (UK), Texas City (USA), and Buncefield (UK) can be the result. At the Buncefield Oil Depot, a failure of a tank level sensor prevented its associated high level alarm from being annunciated to the operator. As the level in the tank reached its 'ultimate' high level, a second protection layer, an independent safety switch, failed to trigger an alarm to notify the operator and failed to initiate a trip which would have automatically shut off the incoming flow. The tank overflow and ensuing fire resulted in a £1 billion (1.6 billion USD) loss [1].

This paper provides considerations for how to determine the risk reduction (and probability of failure on demand) provided by an operator response to alarm when it is identified in a LOPA. These alarms will be referred to in this paper as safety IPL alarms. The paper also provides recommendations on how to ensure that the targeted or expected risk reduction is delivered in practice for alarms identified as IPLs or as safeguards from a HAZOP.

## Using Alarms to Provide Risk Reduction

When an operator's response to an alarm is included in a layer of protection analysis, it is being counted on to provide a specific level of risk reduction in conjunction with other independent protection layers (IPL), such as a safety instrumented function (SIF). To evaluate its risk reduction, it is important to consider the behavior of the alarm system as a whole, in terms of its effectiveness in guiding the operator to take the correct action.  If the design and management of the alarm system or its actual performance are not satisfactory, then the level of actual risk reduction delivered will be less than expected because the operator's dependability will be compromised. This is particularly critical during abnormal situations such as might accompany a tank high level event.  If operators are flooded with alarms during the upset, or nuisance alarms are already present, then they might miss a critical high level safety IPL alarm, respond incorrectly, or not in time.

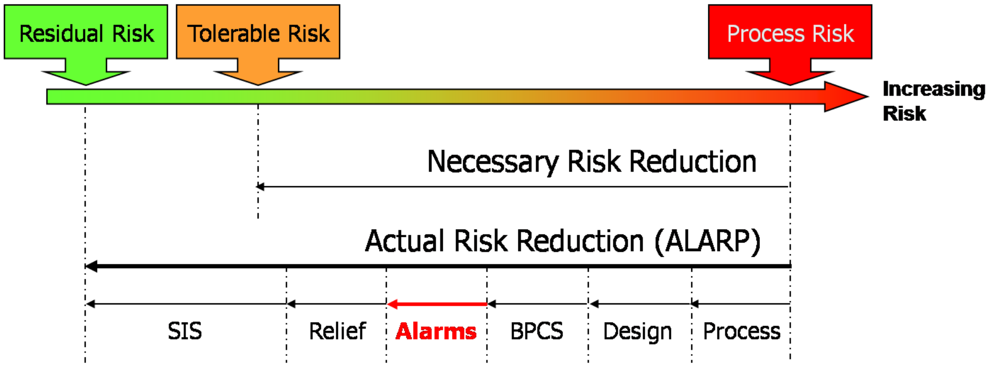


Figure 2. Risk Reduction through the use of multiple protection layers [2]

Thus, poor alarm management could reduce the protective capability of this layer or eliminate it altogether, which could mean that that the actual risk reduction no longer meets or exceeds the company-defined tolerable risk level. This could have a ripple effect on the Safety Integrity Level (SIL) requirements for numerous SIFs throughout the plant.  The higher the SIL level, the more complicated and expensive is the Safety Instrumented System (SIS). A higher SIL may also require more frequent and elaborate proof testing, which adds cost and can be burdensome in many plants.

## The Role of Alarm Management

The standard ANSI/ISA-18.2, *"Management of Alarm Systems for the Process Industries"* (ISA-18.2) provides guidance that can help users design, implement and maintain an alarm system that delivers acceptable performance and maximizes operator dependability [3]. Following the requirements and recommendations of ISA-18.2 is critical for safety practitioners that want to use alarms as a layer of protection.

Similar to the activities in the IEC 61511 / ISA 84 functional safety standard, alarm management activities are structured to follow a lifecycle approach wherein the key activities are executed in the different stages of the lifecycle. The products of each stage are the inputs for the activities of the next stage. A detailed comparison of similarities and differences between the functional safety and alarm management lifecycles is the subject of another paper, as is a discussion of the activities where the two lifecycles intersect [4, 5].

The first stage of the alarm management lifecycle involves the creation of an alarm philosophy document (APD). The APD establishes the basic definitions, principles, and processes for the design, implementation, maintenance, and management of alarm system(s). It contains the alarm system performance goals and describes the key work practices, roles and responsibilities. This document provides guidance for a consistent approach to alarm management and is critical to creating and maintaining an effective alarm system over time.

One of the most important and relevant activities is called alarm rationalization. Rationalization involves reviewing and justifying potential alarms to ensure that they meet the criteria for being an alarm as defined in the alarm philosophy document. It includes defining the attributes of each alarm (such as limit, priority, classification, and type) as well as documenting the cause, consequence, response time and operator action (response). The rationalization process is performed by a multifunctional team which typically includes the process engineer, controls engineer, lead operator(s), and safety / risk management engineer (as required).

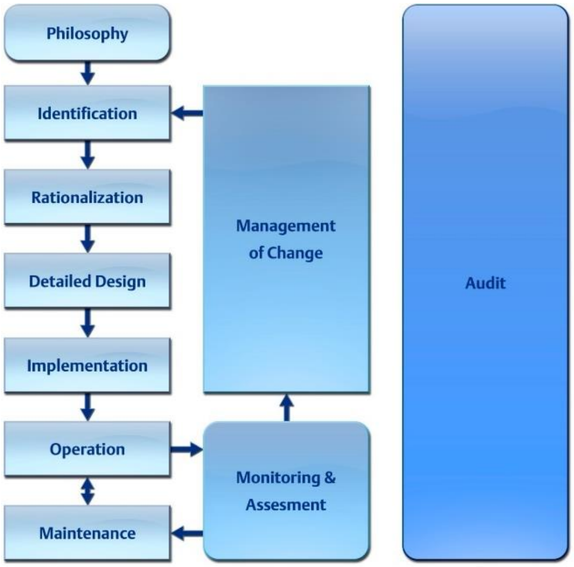


Figure 3. ISA-18.2 Alarm Management Lifecycle [3]

ISA-18.2 is expected to be considered "recognized and generally accepted good engineering practice" (RAGAGEP) by both insurance companies and regulatory agencies as ISA-84 / IEC 61511 is today.

## Similarities and Difference between Alarms and SIFs

A safety instrumented function (SIF) is an action that a safety instrumented system (SIS) takes to take the process to a safe state when specific conditions are violated. A SIF is commonly thought of as the equipment (sensor, logic solver, and final element) within an SIS that carries out a single set of actions in response to a single hazard, along with the associated application software.

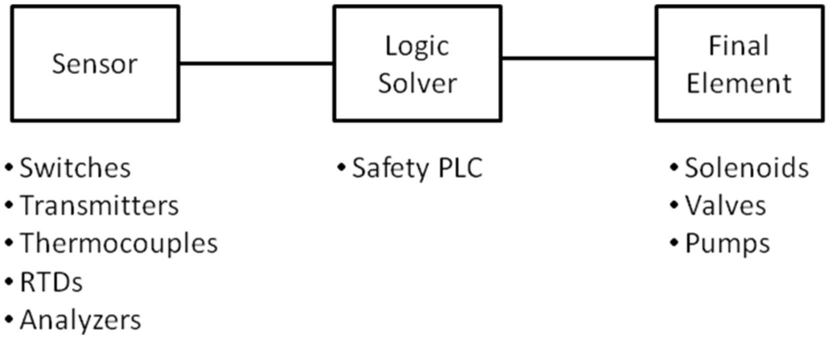


Figure 4. Typical Safety Instrumented Function [6]

An alarm is "an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition ***requiring a response*** [3]". An important principle of ISA-18.2 is that an alarm requires a response, which is an action taken to correct the abnormal situation (or otherwise prevent harm). Examples of valid responses include closing a valve or starting a backup pump. Acknowledging an alarm is not considered a valid operator response as it does not affect the abnormal situation.

There are many similarities between a SIF and a Safety IPL alarm. They share a common purpose of helping to reduce the risk of unwanted events. They are both assigned a criticality – priority for alarms, and safety integrity level for SIFs. A typical chemical plant has a small number of safety instrumented functions, but may have hundreds or thousands of alarms in the Basic Process Control System (BPCS). Each safety instrumented function is evaluated individually and is designed and verified to address a specific hazard. An alarm is also evaluated individually, but because all alarms are processed by the operator before the associated action is taken, the alarm system must also be evaluated as a whole. The alarm load on the operator, the presence of nuisance alarms and the relative distribution of alarm priorities, have been shown to have a significant impact on the probability that an operator will take the correct action when an alarm is annunciated.

## Analyzing Operator Response to Alarms

For consistency with the techniques used to perform SIL calculations, alarms will be treated and analyzed as if they were a SIF consisting of a "sensor", "logic solver" and "final element". As shown in Figure 4, Alarm annunciation is analogous to the "Sensor" block in a SIF. It is comprised of the sensor, logic solver and HMI. The role of "Logic Solver" is now performed by the operator and the "Final Element" consists of the HMI, logic solver and final element. In other cases the response requires a manual operator action in the field.

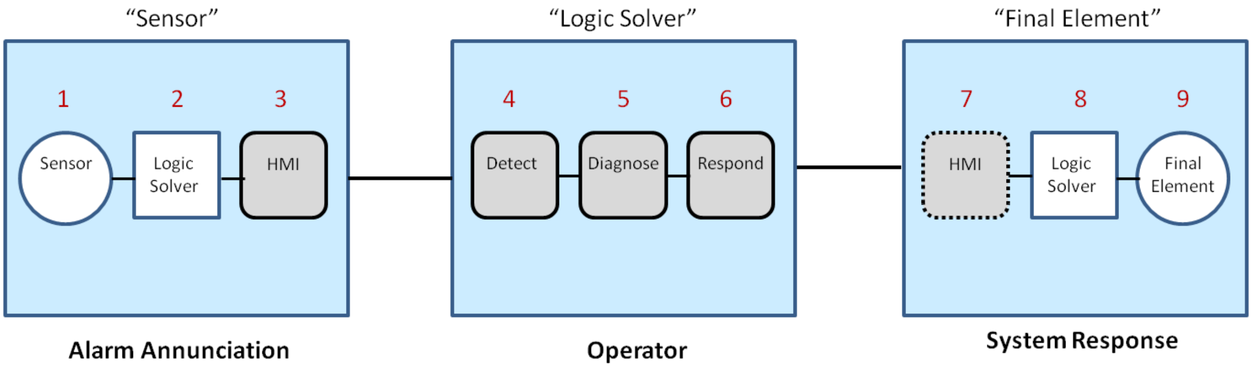


Figure 5. Modeling the Operator Response to Alarm

To analyze the probability of failure on demand (PFD) of the operator response to an alarm layer it is necessary to examine the sequence of events which would make for a successful operator response. The first step after the initiating event occurs is the triggering / annunciation of the alarm. If a failure were to occur in the hardware or software associated with the alarm (the sensor, the control logic for triggering the alarm, or the Human Machine Interface) then the alarm would never be annunciated. This represents the probability of failure on demand that the alarm is annunciated. The complete series of events is described below.

1) The physical sensor must provide an accurate and reliable process measurement to the logic solver.

   *If the sensor fails (like at Buncefield) the alarm will never be generated.*

2) The logic solver / controller must compare the process measurement to its defined limit and generate an alarm if the alarm threshold has been reached or exceeded.

   *If the logic solver fails the alarm will never be generated. If the alarm has been disabled, then the logic solver will not generate the alarm. If the alarm limit is set incorrectly or has been modified inappropriately, the alarm will not be triggered at the appropriate time.*

3) The alarm event must be annunciated / displayed in the Human Machine Interface (HMI) for the operator to see.

   *If communication between the logic solver and the HMI fails or the HMI computer itself fails, then the alarm will not be annunciated or displayed to the operator. If the alarm has been suppressed (either manually by the operator or programmatically by the control system), then the alarm event will not be presented through the HMI.*

   *In the aftermath of the Deepwater Horizon explosion it was determined that one of the contributors to the loss of life was the suppression of the alarms that indicate the presence of fire, explosive gas or toxic gas. It was reported that the audible (horn) and visual (flashing lights)* *annunciation of these alarms was inhibited to prevent a false alarm from waking people at night.* [7]

4) The operator must **Detect** the presence of the alarm (via the HMI).

   *If the HMI is poorly designed (information is not presented in proper context to provide situation awareness) then the operator may fail to notice the alarm. If the alarm system is experiencing performance issues such as nuisance alarms (stale alarms, chattering alarms), alarm overload, or alarm floods, then the operator may notice it after it is too late or miss the alarm altogether. Cyber security incidents such as Stuxnet have shown how a "man-in-the-middle" attack can present false information to the operator through the HMI.*

   *During the Milford Haven refinery explosion, the operators were inundated with 275 alarms in an 11 minute time span causing them to fail to recognize and act upon the flare high level alarm. The control room HMI displays did not help the operator understand what was going on and presented misleading information (a control valve that was actually closed was indicated as open).*[8]

5) The operator must **Diagnose** the problem (what is the likely cause), assess the potential consequences, and determine the necessary corrective action.

   *The operator could mis-diagnose the problem resulting in actions that make the situation worse or do not correct it. During the incident at Three Mile Island operators initially turned off the high pressure water injection pumps (part of the emergency cooling system) when they were needed to cool the reactor believing that the presence of too much coolant was the cause of the steam pressure release.* [9]

6) The operator must complete the actions that comprise the **Response** within the allowable time. These actions could include starting / stopping or opening / closing devices through the HMI, calling a field operator, or performing manual actions in the field (manually closing a shutoff valve).

   *Under the stress of the situation, the operator could mistakenly perform an incorrect action (close the wrong valve)or not complete the actions in time before the consequences are inevitable.*

7) The operator response must be communicated through the (HMI).

   *If the HMI (computer) fails then the operator will not be able to complete the action.*

8) The logic solver must receive and interpret the operator's HMI command and send the appropriate signal to the field (final element).

   *If communication between the logic solver and the HMI fails then the command will not be sent from the logic solver. In a "man-in-the-middle" cyber attack, commands sent by the HMI may be prevented from reaching the logic solver.*

9) The final element must receive the command from the logic solver and perform the desired action (open / close, start / stop).

   *The final element could fail to perform the required action. If the final element must be energized to perform its desired action, then a loss of utilities (power, instrument air, etc.) will prevent the response from occurring. If a manual response is required, the operator may not physically be able to perform actions such as climbing to the top of a column or opening a manual valve that has been painted shut.*

## Operator Time to Respond

The operator allowable time to respond represents the time from the activation of the alarm to the last moment that the operator action will prevent the consequence (the completion of Step 6). For a conventional process control application using a DCS, the time it takes to complete steps 1-3 and steps 7-9 can be assumed to be negligible compared to the time it takes the operator to complete steps  4-6.

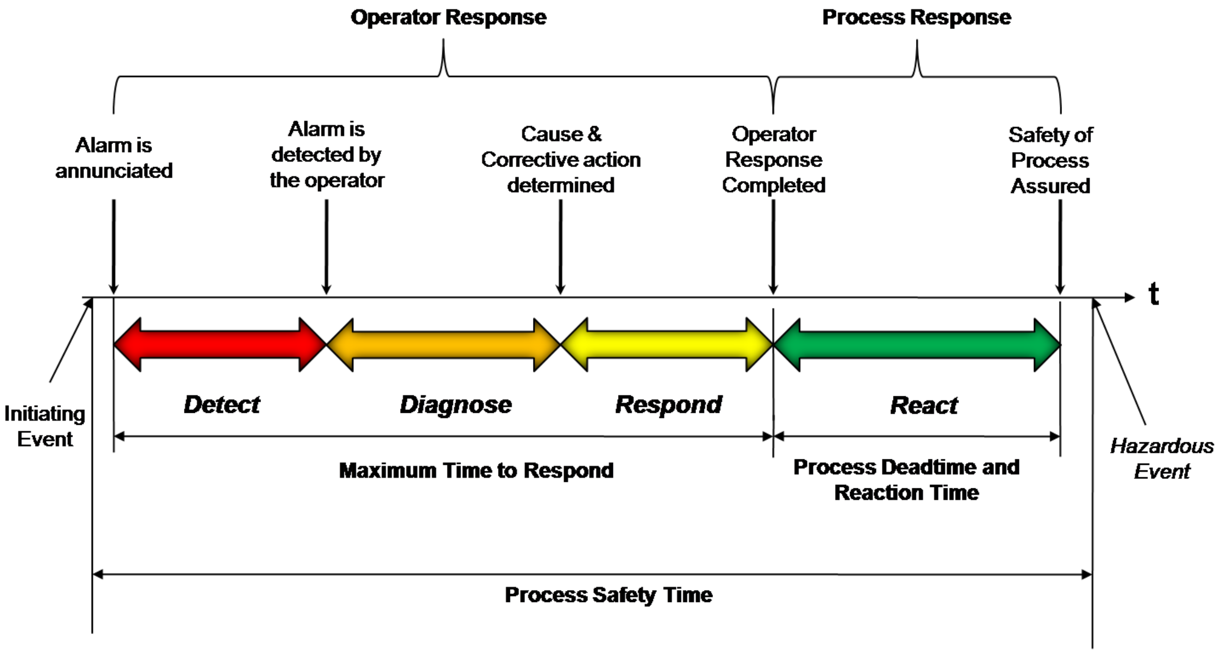

Operator Response
Process Response
Alarm is annunciated
Alarm is detected by the operator
Cause & Corrective action determined
Operator Response Completed
Safety of Process Assured
t
Initiating Event
Detect
Diagnose
Respond
React
Hazardous Event
Maximum Time to Respond
Process Deadtime and Reaction Time
Process Safety Time

Figure 6. Operator Response Timeline

Because of process deadtime, some processes will not react to the corrective action immediately; thus process reaction time and the process safety time (the time between the initiating event and occurrence of the hazardous event) must be factored into the determination of the allowable response time (how much time is available for the operator). If the actual time that it takes the operator to complete steps 4-6 is greater than the allowable response time, then the hazardous event is likely to occur and alarm plus operator action has failed as a layer of protection.

For Safety IPL alarms to be effective, it is important that operators be given sufficient time to respond. To this end many companies define a minimum allowable operator response time for Safety IPL alarms (typically on the order of 20 - 30 minutes). This means that if the available operator response time is less than this value, then the alarm cannot be claimed as a layer of protection (PFD = 1.0). Operator response time is estimated during the alarm rationalization stage of the lifecycle taking into account the alarm limit, consequence threshold and process dynamics such as rate of change.

There is occasionally the temptation to claim, during the rationalization, that the operator "must respond to alarm X within five minutes" even if the response time analysis indicates this is not feasible. In such cases, the rationalization team, and especially its facilitator (chairman), must be assertive in rejecting the alarm as a valid IPL and insist on re-engineering and re-evaluation of the risk.

## Determining Probability of Failure on Demand for LOPA

Assuming that the failure events are mutually exclusive, the PFD for the operator's response to an alarm can be determined by adding the three separate contributions representing the "sensor", "logic solver", and "final element" as if it was a safety instrumented function:

$$\text{PFD}_{\text{Safety IPL Alarm}} = \text{PFD}_{\text{Alarm}} + \text{PFD}_{\text{Operator}} + \text{PFD}_{\text{System Response}} \quad \text{[Eq. 1]}$$

$\text{PFD}_{\text{Alarm}}$: the probability that the alarm fails to annunciate (Steps 1 - 3)

$\text{PFD}_{\text{Operator}}$: the probability that the operator fails to successfully detect, diagnose, and respond to the alarm correctly and within the time available (Steps 4 - 6)

$\text{PFD}_{\text{System Response}}$: the probability that the operator acts, but the final element / response to the operator action fails (Steps 7 - 9).

A survey of the literature shows that significant variation exists in the recommended PFD to be used for the overall layer of protection ($\text{PFD}_{\text{Safety IPL Alarm}}$). As shown in Table 1, EEMUA 191 provides recommended $\text{PFD}_{\text{Safety IPL Alarm}}$ values as a function of quasi alarm system performance requirements. It recommends not using a $\text{PFD}_{\text{Safety IPL Alarm}}$ below 0.01 for any operator action. The IEC 61511 / ISA 84 standard allows the use of $\text{PFD}_{\text{Safety IPL Alarm}}$ equal to 0.1. [10]

| **Claimed PFDavg** | **Alarm system integrity / reliability requirements** | **Human reliability requirements** |
|---|---|---|
| 1.0 - 0.1 (standard alarm) | Alarms may be integrated into the process control systems | No special requirements - however the alarm system should be operated, engineered and maintained to accepted good engineering standards |
| 0.1 - 0.01 (safety-related alarm) | Alarm system should be designated as safety related and categorized as SIL1 (as defined in IEC 61508) | The operator should be trained in the management of the specific plant failure that the alarm indicates;<br>The alarm presentation arrangement should make the claimed alarm very obvious to the operator and distinguishable from other alarms;<br>The alarm should be assigned to the highest priority in the system;<br>The alarm should remain on view to the operator for the whole of time it is active;<br>The operator should have a clear written alarm response procedure for the alarm;<br>The required operator response should be simple obvious and invariant;<br>The operator interface should be designed to make all information relevant to management of the specific plant failure easily accessible;<br>The claimed operator performance should have been audited |
| Below 0.01 | Alarm system would have to be designated as safety related and categorized as at least SIL2 | It is not recommended that claims for a PFDavg below 0.01 are made for any operator action even if it is multiple alarmed and very simple |

Table 1. Recommended PFD Values for Safety-related alarms per EEMUA 191 [11]

Using one of these values without understanding the basis for how they were determined and ensuring that the inherent assumptions are valid is likely to lead to risk reduction claims that are optimistic. A more rigorous and thorough approach can be taken by evaluating the individual components that contribute to the overall PFD $_{\text{Safety IPL Alarm}}$. The following sections provide information on how to estimate the PFD of components that contribute to PFD $_{\text{Safety IPL Alarm}}$.

## Estimating PFD of Hardware Components

Below are some common and representative values for the hardware components that contribute to the Alarm Annunciation and System Response. It should be noted that, unlike a safety instrumented function, the equipment used may be part of a Basic Process Control System (BPCS) and may not be SIL-rated. Also the PFD is a function of the proof test interval, which means that the hardware comprising this element must be tested at an appropriate frequency.

| Component | PFD | Comments |
|---|---|---|
| Typical Rosemount 3051 Pressure Sensor (not SIL Rated) | 1.11e-3 | Source exSILentia: Mission time 15 yrs, |
| Typical Rosemount 3051 Pressure Sensor Sensor (SIL 2 Rated) | 4.19e-4 | Source exSILentia: Mission time 15 yrs, |
| Typical Logic Solver (not SIL Rated) | 6.16e-3 | Source exSILentia: Mission time 15 yrs, |
| Typical Logic Solver (SIL Rated) | 6.85e-5 | Source exSILentia: Mission time 15 yrs, |
| Human Machine Interface (PC & Monitor) | 1.1e-2 | 2 HMIs in parallel, Operator always watching, 1 occurrence of the safety IPL alarm / year, 1% Beta (common cause) factor |
| Typical ASCO Solenoid Valve (not SIL Rated) | 2.71e-2 | Source exSILentia: Mission time 15 yrs, |
| Typical ASCO Solenoid Valve (SIL Rated) | 1.25e-2 | Source exSILentia: Mission time 15 yrs, |
| Typical ASCO Solenoid Valve (SIL Rated) with Partial Valve Stroke testing | 9.11e-3 | Source exSILentia: Mission time 15 yrs, monthly PVST |

Table 2. Representative Component PFDs

## Estimating PFD of the Operator

A key driver in the calculation of PFD $_{\text{Safety IPL Alarm}}$ is the reliability of the operator. A review of the top 100 plant accidents determined that operator failure was the second leading cause (after equipment mechanical fatigue). [12] For the operator to be successful they must detect the alarm, diagnose the problem, and complete the corrective action within the allowable time. The ability of the operator to execute a successful response is affected by workload, short term or working memory limitations, physical condition, fatigue, training, and motivation. Per Nimmo, "The bottom line of most studies into human error indicates that humans are more likely to make an error if they are:

- Required to make an important decision quickly under emergency conditions.
- Required to make multiple decisions in a short time span.

- Bored or complacent.
- Poorly trained in procedures.
- Physically or mentally incapable.
- Subjected to confusing or conflicting displays or data.
- Unqualified for their job.” [13]

Stress can also be a significant factor affecting the operator’s PFD. As shown in Table 3 it can vary by several orders of magnitude depending upon the situation. Safety IPL alarms are most likely to be generated only during significant plant upset conditions. This means they would be accompanied by lots of other alarms and the need to make quick decisions.

| **Component** | **PFD** |
|---|---|
| Human performance (trained, no stress) | 1.0 x $10^{-2}$ to 1.0 x $10^{-4}$ |
| Human performance (under stress) | 0.5 to 1.0 |

Table 3. Operator PFDs per IEC 61511/ISA-84 [10]

One of the contributors to operator stress is the performance of the alarm system. If the operator is overloaded with alarms or is constantly subjected to nuisance alarms, their ability to respond will be affected. For example the investigation of the accidents at the Dupont Belle West Virginia plant determined that safety-critical alarms were ignored because they were often nuisance alarms. [14]

Another issue is that operators may be reluctant to take an action that has a major effect on process throughput. Operators are often under pressure to keep the plant running as much as possible. Every responsible operating company will promulgate a “safety comes first” attitude, and may even state that anyone has the right to shut down the process if they see a safety problem. Nevertheless, operators—and, perhaps to a greater extent, supervisors—may feel obligated to avoid a manual shutdown if at all possible, for fear of repercussions from senior management. The pressure may be even more acutely felt in cases where the incident would lead to economic harm (e.g. damage to a large compressor) but there is no safety or environmental impact. In such cases, it is necessary to provide clear instructions and training to the operator that takes away the need to make a complex judgement call in a moment of crisis. The alarm response manual needs to state explicitly that, when alarm X comes and condition Y is met, the operator is authorized and required to carry out action Z.

Table 4 presents representative PFD values for estimating PFD $_{\text{Operator}}$ based on operational practices.

| Category | Description | Probability that Operator responds successfully | PFD | SIL |
|---|---|---|---|---|
| 1 | **Normal Operator Response** – In order for an operator to respond normally to a dangerous situation, the following criteria should be true:<br>• Ample indications exist that there is a condition requiring a shutdown<br>• Operator has been trained in proper response<br>• Operator has ample time (> 20 minutes) to perform the shutdown<br>• Operator is ALWAYS monitoring the process (relieved for breaks) | 90% | 0.1 | 1 |
| 2 | **Drilled Response** – All of the conditions for a normal operator intervention are satisfied and a "drilled response" program is in place at the facility.<br>• Drilled response exists when written procedures, which are strictly followed, are drilled or repeatedly trained by the operations staff.<br>• The drilled set of shutdowns forms a small fraction of all alarms where response is so highly practiced that its implementation is automatic<br>• This condition is RARELY achieved in most process plants | 99% | 0.01 | 2 |
| 3 | **Response Unlikely / Unreliable** – ALL of the conditions for a normal operator intervention probability have NOT been satisfied | 0% | 1.0 | 0 |

Table 4 – Simplified Technique for Estimating Operator Response [15]

Reviewing this table shows that there are specific conditions that must be met for a PFD of 0.1 or 0.01 to be appropriate. It is very rare that conditions in a process plant would be conducive to claiming a 0.01 PFD. For situations requiring a more detailed calculation of operator response PFD, various human factors techniques exist for quantifying human error.

## Example PFD Calculations for Safety IPL Alarms

In this section we will calculate the PFD for an alarm layer of protection using the representative values defined earlier.

$$PFD_{\text{Safety IPL Alarm}} = PFD_{\text{Alarm}} + PFD_{\text{Operator}} + PFD_{\text{System Response}} \quad \text{[Eq. 1]}$$

| # | Scenario | PFD $_{Alarm}$ | PFD $_{Operator}$ | PFD $_{System\ Response}$ | PFD $_{Safety\ IPL\ Alarm}$ |
|---|---|---|---|---|---|
| 1 | BPCS Hardware with good operator reliability | 1.83E-02 | 1.0E-1 | 2.71E-2 | 1.45E-1 |
| 2 | BPCS Hardware with excellent operator reliability | 1.83E-02 | 1.0E-2 | 2.71E-2 | 5.54E-2 |
| 3 | BPCS Hardware with fair operator reliability | 1.83E-02 | 5.0E-1 | 2.71E-2 | 5.45E-1 |
| 4 | SIL-Rated Hardware with good operator reliability | 1.15E-2 | 1.0E-1 | 1.25E-2 | 1.24E-1 |
| 5 | SIL-Rated Hardware with excellent operator reliability | 1.15E-2 | 1.0E-2 | 1.25E-2 | 3.40E-2 |
| 6 | SIL-Rated Hardware with fair operator reliability | 1.15E-2 | 5.0E-1 | 1.25E-2 | 5.24E-1 |
| 7 | SIL-Rated Hardware, with monthly PVST, excellent operator reliability | 1.15E-2 | 1.0E-2 | 9.11E-3 | 3.06E-2 |

Table 5. Example PFD Calculations for Safety IPL Alarms

Some interesting conclusions can be drawn from these example calculations. The dominant factor in the PFD of a safety IPL alarm is the reliability of the operator. However, the reliability of the hardware serves to define a lower limit for PFD. In examples #2 and #5 the PFD contribution for the hardware (the sum of PFD $_{Alarm}$ and PFD $_{System\ Response}$) is .045 and .024 for BPCS and SIL-rated hardware respectively. This means that it would be virtually impossible to achieve an overall PFD of 0.01 for a Safety IPL Alarm, even with perfect operator performance.

For the example PFD values chosen the selection of hardware (SIL rated vs. non-SIL Rated) had only a secondary effect on the risk reduction of the overall layer. This is largely because the HMI's reliability (PFD of 0.011) was the primary contributor to the calculation of PFD $_{Alarm}$.

## Alarms as Independent Protection Layers

The criteria for being considered an independent protection layer (IPL) are well established in the literature. [15] They can be applied to the operator response to alarms as shown below.

- Specific – The alarm must be specifically designed to prevent the consequences under consideration.
- Auditable – It should be proof tested and maintained. Audits of operation are necessary to ensure that the specified level of risk reduction is being achieved.

- Independent – The alarm must operate completely independently of all other protection layers; no common equipment can be shared with other protection layers, or with the initiating cause or the related SIF.
- Dependable – The alarm must be able to dependably prevent the consequence from occurring.

In addition to the criteria above, the authors propose that additional specific criteria, taken from the ISA-18.2 standard, should be met in order for the alarm to be deemed a valid IPL.

- **The alarm must be proven to be valid when it is first proposed / identified.** – It must meet the criteria for being an alarm as defined in the relevant alarm philosophy document. To ensure that alarms identified in a HAZOP or LOPA are not determined later to be invalid or ineffective during alarm rationalization, the following should be discussed and documented during the associated safety design activity:
    - Does the alarm require a timely operator action in order to avoid defined consequences?
    - What is the required operator action (response)?
    - Does the operator action put them in danger?
    - Will there be sufficient time available for the operator to complete the actions comprising the response?
    - Will the operator be able to deduce the root cause of the abnormal situation from this alarm?
    - Is the alarm (annunciation) independent from the cause?
- **The alarm system must be rationalized**. - This means that all of the configured alarms have been systematically reviewed to ensure that they meet the criteria for being an alarm as defined in the relevant alarm philosophy document. The rationalization process includes evaluation / determination of alarm priority, limit (setpoint), classification and documentation of the cause, consequence, and corrective action.
- **Alarm system performance must be measured and proven to be adequate** - To ensure performance is acceptable it must be measured and compared to key performance metrics (targets) defined in the relevant alarm philosophy. Relevant performance metrics are defined in the ISA-18.2 standard.

    As shown below, ISA-18.2 recommends that operators should receive no more than ~12 alarms / hour (average) for the situation to be “manageable”. Thus if the operator is inundated with an average of 60 alarms per hour, then the probability that they fail to respond correctly to a Safety IPL alarm is increased (thus impacting the reliability of this layer of protection). In this scenario it would NOT be appropriate to claim credit for Safety IPL alarms until the actual performance of the alarm system is improved.

| **Alarm Performance Metrics**<br>**Based upon at least 30 days of data** | | |
|---|---|---|
| **Metric** | **Target Value** | |
| Annunciated Alarms per Time: | Target Value: Very Likely to be Acceptable | Target Value: Maximum Manageable |
| Annunciated Alarms Per Day per Operating Position | ~150 alarms per day | ~300 alarms per day |
| Annunciated Alarms Per Hour per Operating Position | ~6 (average) | ~12 (average) |
| Annunciated Alarms Per 10 Minutes per Operating Position | ~1 (average) | ~2 (average) |
| **Metric** | **Target Value** | |
| Percentage of hours containing more than 30 alarms | ~<1% | |
| Percentage of 10-minute periods containing more than 10 alarms | ~<1% | |
| Maximum number of alarms in a 10 minute period | ≤10 | |
| Percentage of time the alarm system is in a flood condition | ~<1% | |
| Percentage contribution of the top 10 most frequent alarms to the overall alarm load | ~<1% to 5% maximum, with action plans to address deficiencies. | |
| Quantity of chattering and fleeting alarms | Zero, action plans to correct any that occur. | |
| Stale Alarms | Less than 5 present on any day, with action plans to address | |
| Annunciated Priority Distribution | 3 priorities: ~80% Low, ~15% Medium, ~5% High or<br>4 priorities: ~80% Low, ~15% Medium, ~5% High, ~<1% “highest”<br>Other special-purpose priorities excluded from the calculation | |
| Unauthorized Alarm Suppression | Zero alarms suppressed outside of controlled or approved methodologies | |
| Unauthorized Alarm Attribute Changes | Zero alarm attribute changes outside of approved methodologies or MOC | |

Table 6. ISA-18.2 Alarm Performance Metrics [3]

# Optimizing the Performance of the Operator Response to Alarm IPL

This section discusses additional considerations that should be applied when evaluating the use of operator response to alarms as an independent protection layer (IPL). It also describes techniques for maximizing the actual risk reduction achieved.

## *Specific*

To be effective there should be only one set of operator responses defined for a safety IPL alarm. If the operator is expected to determine which of several possible responses is appropriate, then the likelihood of operator error is increased and the alarm may not be effective at preventing the consequence.  A safety IPL alarm should be linked to a relatively small number of cause / consequence pairs (ideally just one).

## *Auditable*

### Testing

To ensure the integrity of a safety IPL alarm, it is critical to perform periodic testing.  Alarms should be proof tested at the frequency that is necessary to deliver the appropriate PFD. The interval selected is dependent on the criticality of the alarm in question and the statistical likelihood of the alarm failing. Testing should verify the integrity of all of the components that make up the IPL from sensor to final element; the alarm annunciation, the operator, and the system response.  To maximize the effectiveness of the proof test, the alarm should be generated via the process (not simulated). The proof test should verify that the operator responds correctly to the alarm within the allowable time and that the system responds as expected.

One of the findings from the Buncefield investigation was that the design and location of the independent high level safety switch made it difficult to test. It also highlighted the importance of being able to verify alarm integrity. According to the investigation “the detection of ultimate high liquid level in storage tanks often relies on a switch mounted on the roof of the tank (or on the uppermost level of the tank wall). The operation of the switch cannot be tested fully in situ other than by raising the liquid level in the tank to the ultimate high level. Any other means of testing will leave a number of potential failure modes uncovered and so leave the switch in a faulty state unbeknownst to the operator or maintenance staff.” [1]

Verifying the performance of sensor hardware requires that the equipment is proven not to be in a state of failure.  In practice, this could be achieved by performing a battery of tests that disprove the occurrence of a large fraction of known failure modes.  For example, consider a high pressure alarm triggered by a sensor that is prone to fouling.  In order to demonstrate the sensor is not fouled, we must show that it responds correctly and quickly to changes in pressure.  It may not be necessary to raise the pressure to the alarm setpoint, since we can reasonably assume that if it is capable of sensing other pressures within its working range, it will also sense pressure at the setpoint; there is no known failure mode (relating to fouling, at least) that would prevent it from doing so.  This indicates that a knowledge of the most credible failure modes can allow us to develop a feasible and effective testing regime. Failure modes can be determined by techniques such as Failure Modes, Effects & Diagnostics Analysis (FMEDA).  Good record keeping would also enable operating companies to apply their own experience of failure events.

## Classification

Alarms that have been credited with risk reduction should be assigned to an appropriate classification (such as Safety IPL, LOPA Listed, HAZOP Safeguard) during alarm rationalization. Classification allows groups of alarms with similar characteristics and requirements for training, testing, documentation, data retention, reporting, or management of change to be lumped together for easier management. This makes it easier to identify which alarms in the system are being used to provide risk reduction.

## Performance of the Safety IPL Alarm

As part of the audit process the following information should be documented and reviewed for each safety IPL alarm.

a) number of times the alarm was activated
b) the percent of time the alarm was active
c) the number of times the alarm became stale (was active continuously for > 24 hours)
d) the number of times the alarm was suppressed (shelved)
e) the percent of time the alarm was suppressed (shelved)
f) the number of times the alarm was taken out-of-service
g) the percent of time the alarm was out-of-service

The alarm frequency for a IPL alarm can be used to determine the actual initiating event frequency. A high alarm rate can indicate a higher than anticipated initiating event frequency.

The stale alarm time for a IPL alarm may indicate the time at risk of a hazardous event or the time the alarm is not an indicator of the initiating event. The shelved and out-of-service time for an IPL alarm may indicate the time the alarm is not available as a layer of protection.

### *Independent*

To be an effective IPL, the safety IPL alarm must be independent from the cause of the failure and from other layers of protection associated with the hazard. It is interesting to note that the tank high level alarm in the Buncefield depot incident would not have qualified as an IPL since the alarm was not independent from the initiating event (the failure of the associated tank level measurement). To achieve independence in practice, safety IPL alarms often use dedicated sensor hardware and have separate and dedicated HMIs for use by the operator in the event that their traditional basic process control system (BPCS) displays fail. Alternatively, they can be equipped with diagnostics (such as deviation alarms) that allow hardware failures to be detected immediately, even when the process is not in the alarm state.

It is not recommended to take credit for more than one safety IPL alarm per demand scenario. It would be inappropriate to have one safety IPL alarm “back up” another, because if the control room operator fails to successfully respond to the first alarm then it is likely they will fail to respond to the second one. An exception is when a different set of hardware is used for the alarm annunciation (e.g., local alarm vs. control room alarm ) and a different operator is responsible for responding (e.g., field operator vs. control room operator).

### *Dependable*

#### Use of Alarm Response Procedures

For safety alarms to be dependable, it is critical that the operator know what to do in the event of the alarm. This is best achieved through training and by making alarm response procedures available. Training on how to respond to safety IPL alarms is especially important as these alarms will not occur frequently and because they are most likely to occur during stressful situations such as a major plant upset. Providing operators with alarm response procedures is a best practice that should be considered mandatory for safety IPL alarms. The alarm response procedure, which contains key information documented during rationalization (such as the cause, consequence, corrective action and confirmation), can be provided in context to the operator from within the HMI.

#### Measuring and Analyzing Alarm System Performance

Alarm system performance has a significant effect on dependability. In a properly designed system every alarm requires an operator response; therefore, if there is no response then the consequences will occur. In a poorly performing system many of the annunciated alarms can be ignored by the operator without consequence (they are not valid alarms).  If the operators are overloaded with alarms or inundated with nuisance alarms, then they will in fact ignore alarms (to save their sanity). Problems occur when the operators develop a culture that it is acceptable to ignore alarms. This should be prevented. There may come a scenario when an alarm which was previously ignored without incident, is actually a legitimate notification of a critical situation (e.g., the incident at the Dupont Belle, WV plant).

Alarm system performance should be measured on a regular basis (at least monthly) and compared to the recommended performance metrics of ISA-18.2 and those defined in the alarm philosophy. If the alarm system performance is consistently well outside the recommended metrics, then the safety IPL alarm should be considered invalid until the performance gap is addressed.

#### Alarm Rationalization

To maximize dependability the operator must believe that every alarm is valid and requires their response. Alarm rationalization is the process for ensuring that every alarm configured in the system is valid and justified.  Rationalizing the alarms in the system helps to improve the operator's trust in the alarm system, and serves to document the cause and corrective action. It also defines the priority of the alarm, which is a measure of the alarm's criticality. Priority, which is typically assigned based on the severity of the potential consequences and the time available for the operator to respond, tells the operator which alarm they should respond to first.  In general safety IPL alarms would typically be set to the higher priority levels if not the highest priority level.

#### Management of Change

To ensure that the safety IPL will annunciate when required, it is important to have an effective management of change process in place. In particular, safety IPL alarms should not be able to be disabled or have their limit (setpoint) changed by the operators. Any changes to safety IPL alarms should go through a rigorous management of change review and approval process before implementing.

### Alarm Suppression

To ensure alarms are only presented to the operator when they are relevant and to reduce alarm load during upsets, many systems implement alarm suppression. One scenario where suppression of safety IPL alarms can be critical is when equipment is out-of-service or offline. It is important to explicitly consider whether it is acceptable to suppress a safety IPL alarm during any scenarios. There are many examples where accidents have occurred when equipment was offline with some alarms suppressed that should not have been.

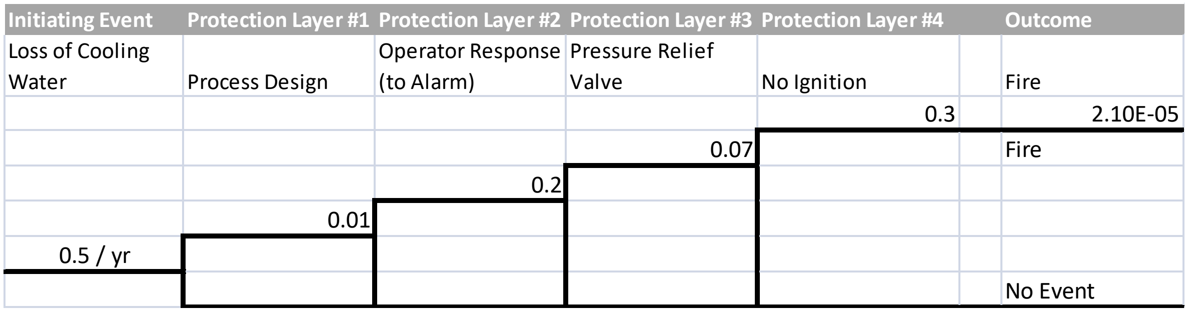
### HMI Design

It is important that the operator's HMI process graphic screens be designed to support situation awareness. Providing appropriate overview displays is one key to achieving this. It is also important that graphic displays be designed with an appropriate level of process and equipment information for the operator to verify or confirm the existence of an alarm. Poor graphics, including alarm depiction deficiencies, have been identified as contributing factors to several major industrial accidents (such as Buncefield). Alarms should be integrated into the displays so that the operator's attention is clearly drawn to the presence of an alarm (they "jump off the page") and is not clouded by the presence of other less important information (like pump status). Also, the alarm descriptions should be clear and easily understandable. Descriptions should point specifically to the relevant equipment (e.g. "Aqueous waste tank 1") and not simply repeat information otherwise provided by the system (e.g. "high level"). Any abbreviations used must be consistent, and there should be a readily available glossary to help interpret them. The same considerations apply to the instructions provided in the alarm response manual.

## Performing a Layer of Protection Analysis

Layer of Protection Analysis is one of the most commonly used techniques for risk assessment in the functional safety lifecycle. The primary goal of a LOPA is to determine if there are adequate protective devices or features in the process to produce a tolerable risk level. These protective devices or features are called Protection Layers or Independent Protection Layers (IPLs). Examples of potential protection layers include the basic process control system (BPCS), operator intervention, the mechanical integrity of a vessel, physical relief devices, and a safety instrumented function.

In a LOPA the frequency of a potentially dangerous event is calculated by multiplying the probability of failure on demand (PFD) of each individual layer of protection by the frequency of the initiating event. In the example LOPA of Figure 4, the likelihood of a fire occurring after the release of flammable materials is calculated assuming that the initiating event (the loss of jacket cooling water) occurs once every two years. In this example the operator response to alarm layer was assigned a $PFD_{\text{Safety IPL Alarm}}$ of 0.2.



| Initiating Event | Protection Layer #1 | Protection Layer #2 | Protection Layer #3 | Protection Layer #4 | | Outcome |
|---|---|---|---|---|---|---|
| Loss of Cooling Water | Process Design | Operator Response (to Alarm) | Pressure Relief Valve | No Ignition | | Fire |
| | | | | 0.3 | | 2.10E-05 |
| | | | 0.07 | | | Fire |
| | | 0.2 | | | | |
| | 0.01 | | | | | |
| 0.5 / yr | | | | | | |
| | | | | | | No Event |

Figure 7. Example Layer of Protection Analysis (LOPA) Calculation [15]

## References

1. “The Buncefield Investigation” - www.buncefieldinvestigation.gov.uk/reports/index.htm
2. Hatch, D, and Stauffer, T., “Operators on Alert: Operator response, alarm standards, protection layers keys to safe plants”, Intech, September 2009.
3. ANSI/ISA ISA18.00.02-2009 “Management of Alarm Systems for the Process Industries”.
4. Stauffer, T., Sands, N., and Dunn, D., “Alarm Management and ISA-18 – A Journey, Not a Destination”, Texas A&M Instrumentation Symposium (2010).
5. Stauffer, T., Sands, N., and Dunn, D., “Get a Life(cycle)! Connecting Alarm Management and Safety Instrumented Systems”, ISA Safety & Security Symposium (2010).
6. Suttinger, L. and Sossman, C., “Operator Action within a Safety Instrumented Function”, WSRC-MS-2002-00091.
7. “Deepwater Horizon Alarm System Was Partly Disabled Prior To Explosion, Technician Tells Congress”, http://www.huffingtonpost.com/2010/07/23/deepwater-horizon-alarm-s_n_657143.html
8. “The Explosion and Fires at the Texaco Refinery, Milford Haven, 24 July 1994”, HSE Books, Sudbury, U.K. (1995).
9. “Three Mile Island Accident”, http://en.wikipedia.org/wiki/Three_Mile_Island_accident
10. ANSI/ISA-84.00.01-2004 Part 3 (IEC 61511-3 Mod) “Functional Safety: Safety Instrumented Systems for the Process Industry Sector- Part 3”.
11. EEMUA (2007), Alarm Systems: “A Guide to Design, Management and Procurement Edition 2”. The Engineering Equipment and Materials Users Association.
12. Coco, James, editor, The 100 Largest Losses of 1972-2001, Marsh Risk Consulting Practice, February 2003
13. Nimmo, I., “The Operator as IPL,” Hydrocarbon Engineering, September 2005.
14. U.S. Chemical Safety And Hazard Investigation Board Final Report, E.I. DUPONT DE NEMOURS & CO., INC., Belle, West Virginia, Report No. 2010-6-I-WV, September 2011.
15. Marszal, E. and Scharpf, E. “Safety Integrity Level Selection”. ISA (2002)
16. Additional references not cited:
17. “BP America Refinery Explosion” U.S. CHEMICAL SAFETY BOARD www.chemsafety.gov/investigations
18. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) “Functional Safety: Safety Instrumented Systems for the Process Industry Sector”
19. Stauffer, T., Bogdan, J., and Booth, S., “Managing Alarms Using Rationalization”, Control Engineering, March 2011
20. Stauffer, T. “Making the Most of Alarms as a Layer of Protection”, Safety Control Systems Conference – IDC Technologies (May 2010).

## Revision History

### Authors: Todd Stauffer, Dr. Peter Clarke

Prepared for Presentation at 8th Global Congress on Process Safety

## *exida – Who we are.*

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

### *Training*

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

### *Knowledge Products*

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

## Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool

  - PHAx™ (Process Hazard Analysis)
  - LOPAx™ (Layer of Protection Analysis)
  - SILAlarm™ (Alarm Management and Rationalization)
  - SILect™ (SIL Selection and Layer of Protection Analysis)
  - Process SRS (PHA based Safety Requirements Specification definition)
  - SILver™ (SIL verification)
  - Design SRS (Conceptual Design based Safety Requirements Specification definition)
  - Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
  - PTG (Proof Test Generator)
  - SILstat™ (Life Event Recording and Monitoring)
- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
  - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
  - CyberSL™ (Cyber Security Level Verification)

***Tools and Products for Manufacturer Support***

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC

80 N. Main Street

Sellersville, PA, 18960

USA

+1 215 453 1720

+1 215 257 1657 FAX

info@exida.com