Get a Life(Cycle)!
Connecting Alarm Management and Safety Instrumented Systems

White Paper

exida
80 N. Main St.
Sellersville, PA
www.exida.com

April 2010

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

Abstract

Alarms and operator response are one of the first layers of defense in preventing a plant upset from escalating into an abnormal situation. The new ISA 18.2 standard [1] on alarm management recommends following a lifecycle approach similar to the existing ISA84/IEC 61511 standard on functional safety. This paper will highlight where these lifecycles interact and overlap, as well as how to address them holistically. Specific examples within ISA 18 will illustrate where the output of one lifecycle is used as input to the other, such as when alarms identified as a safeguard during a process hazards analysis (PHA) are used as an input to alarm identification and rationalization. The paper will also provide recommendations on how to integrate the safety and alarm management lifecycles.

Conclusion

Alarms and safety have always gone hand-in-hand. With the release of ISA-18.2, the connection between the alarm management lifecycle and the functional safety lifecycle has become more apparent and more actionable. This paper has explored some of the interactions between the lifecycles and has shown examples of where performance is dependent on successfully addressing both lifecycles simultaneously. This will help practitioners from both disciplines take a holistic approach leading to increased plant safety, reduced risk and better operational performance.

Introduction

The disciplines of alarm management and functional safety have always been interconnected. Alarms are often used as a means of risk reduction (layer of protection), sometimes in conjunction with a safety instrumented function (SIF), to prevent the occurrence of a process hazard, as shown in Figure 1. The performance of the alarm system may have a direct effect on the integrity requirement of a SIF, as it may limit what level of risk reduction can be credited to an alarm. Safety instrumented systems (SIS) may generate alarms as part of their function and to indicate a change in state of the SIS. Poor alarm system management can reduce the effectiveness of these indications and has been cited as a significant contributor to some of the worst process safety accidents on record (including Bhopal, Milford Haven, Buncefield, and Texas City).

The preface of Bransby and Jenkinson [2] describes a fictional tale of a typical operator reacting to a sequence of events within a typical process facility. Due to the poor alarm system performance the operator misses a critical alarm that is the impetus for a major incident. One of the fundamental conclusions of Bransby and Jenkinson is that “Poor performance costs money in lost production and plant damage and weakens a very important line of defense against hazards to people.” [2] Furthermore, Donald Campbell Brown stated the fundamental objective of an alarm system clearly and concisely, “the fundamental goal is that Alarm Systems will be designed, procured and managed so as to deliver the right information, in the right way and at the right time for action by the Control Room Operator (where possible) to avoid, and if not, to minimise, plant upset, asset or environmental damage, and to improve safety” [3].

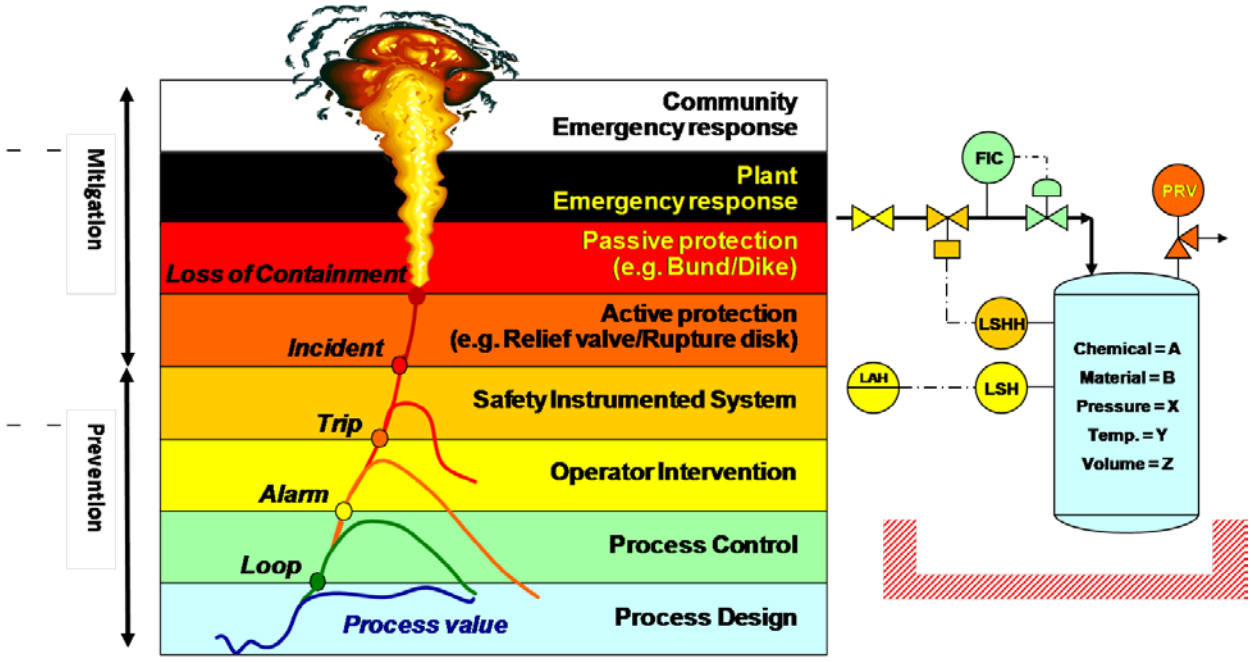

Figure 1. Layers of Protection and Their Impact on the Process

The connection between poor alarm management and process safety accidents was one of the motivations for the development of ANSI/ISA-18.2, *"Management of Alarm Systems for the Process Industries"* (ISA-18.2) [1]. With the release of this new standard in 2009, the discipline of alarm management now has a standard comparable to the well-established functional safety standard ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod 1) *"Functional Safety: Safety Instrumented Systems for the Process Industry Sector"* [4]. ISA-18.2 is expected to be "recognized and generally accepted good engineering practice" (RAGAGEP) by both insurance companies and regulatory agencies as ISA-84 is today.

Similar to the activities in the functional safety standard, alarm management activities are structured to follow a lifecycle approach. The two lifecycles share many similarities, yet have some important differences. A detailed comparison of similarities and differences is the subject of another paper [5]. This paper will examine the areas where the activities of the alarm management and functional safety lifecycles intersect. It will also address treating these two lifecycles (and disciplines) holistically.

The Alarm Management Lifecycle (ISA – 18.2)

The alarm management standard provides a framework for the successful design, implementation, operation and management of alarm systems in a process plant. It provides guidance to solve or prevent the most common alarm management problems and sustain the performance of the alarm system over time. It is organized around the alarm management lifecycle (Figure 2) [1]. The key activities of alarm management are executed in the different stages of the lifecycle. The products of each stage are the inputs for the activities of the next stage.

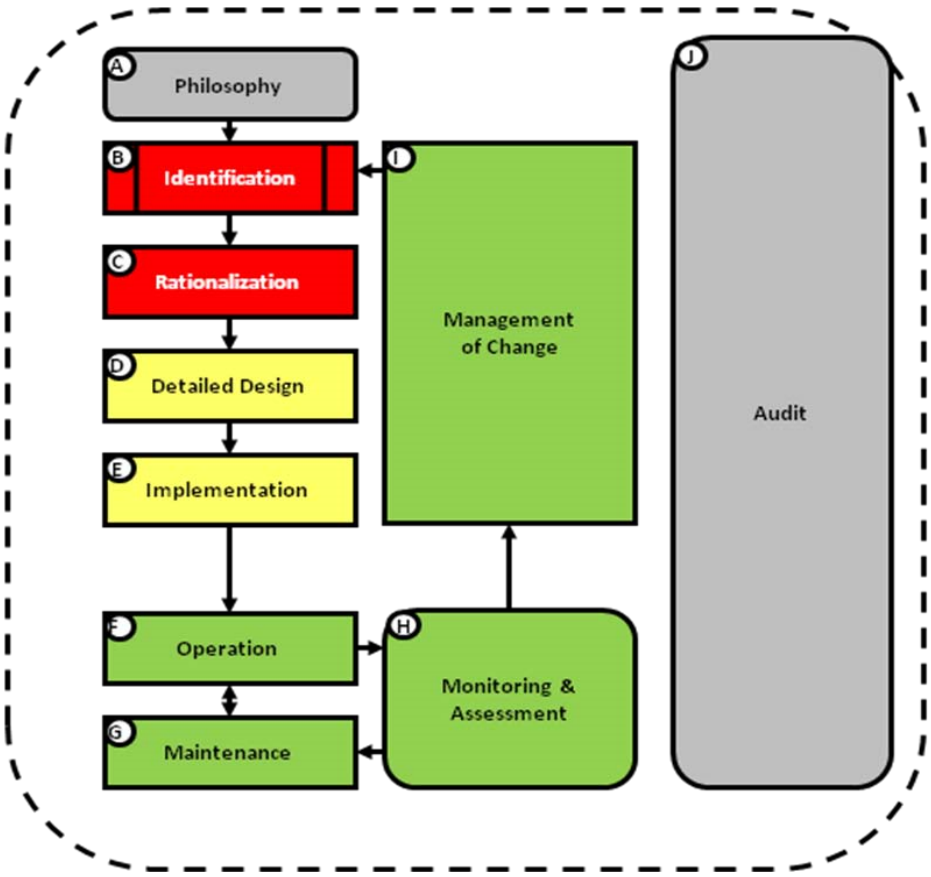

Figure 2. The Alarm Management Lifecycle [1]

The alarm lifecycle has three starting points: philosophy, monitoring & assessment, and audit. Site needs and system status dictate which is the appropriate starting point. Philosophy is the typical starting point for a new system, while monitoring & assessment or audit may be the starting point for an existing system.

The Functional Safety Lifecycle (ISA-84)

The lifecycle for safety instrumented systems from ISA-84 (Figure 3) addresses the application of safety instrumented functions in the process industries [4]. It is a performance-based standard that details the activities and requirements to ensure that SIFs provide the needed reliability of protection from process hazards. It includes the concept of Safety Integrity Level (SIL) which is a method for quantifying a level of risk reduction. Alarms may be allocated as layers of protection and assigned risk reduction factors.

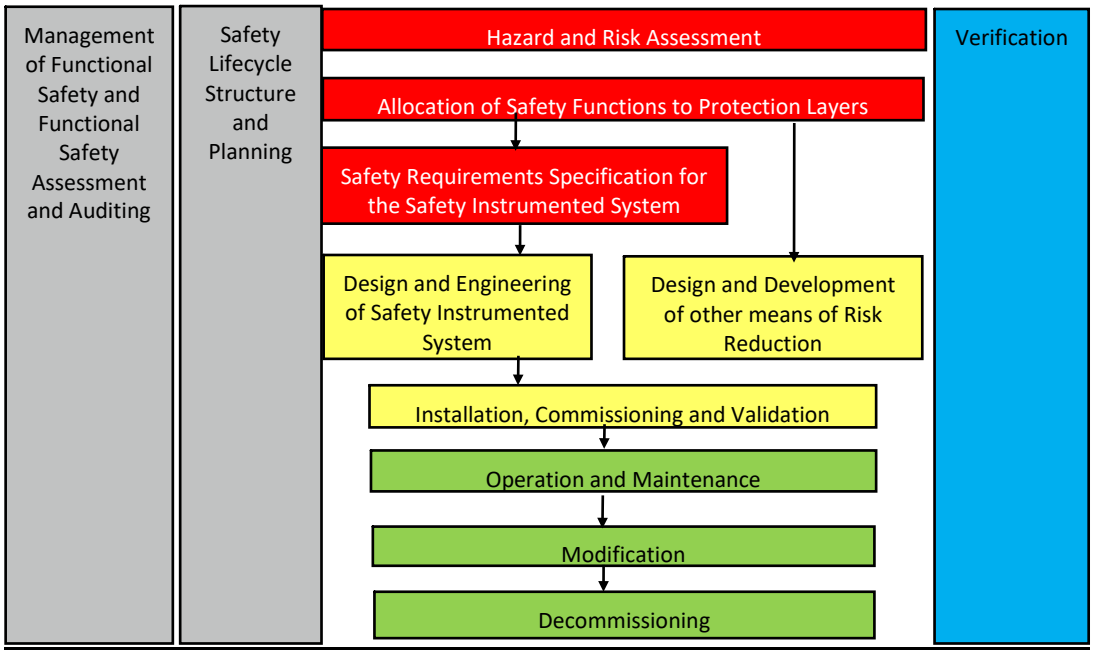

Figure 3. The Safety Instrumented System Lifecycle [4]

The functional safety lifecycle has one main starting point. The identification of process hazards is often viewed as the starting point, but the lifecycle really begins with the management of functional safety stage.

Alarm Management and Safety Lifecycles: Similarities and Differences

To take a holistic approach to the functional safety and alarm management lifecycles it is important to understand their basic similarities and differences. A plant will usually have only a few 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 for a specific hazard. Each 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 rate, the priority distribution, and nuisance alarms (analogous to spurious trips) have been shown to have a significant impact on the probability that an operator will take the correct action on a true alarm. Campbell Brown provides a good overview of this probability and specifically termed it “the consequences of failure to act” [6]. Specifically, Campbell Brown states that “For all assets there are a range of severities associated with the Operator failing to respond to an alarm, as characterized by the prioritisation of the alarm” [6].

Defining What is an Alarm

A key step in alarm management is defining an alarm.

Alarm: An audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition ***requiring a response*** [1].

One of the most important principles of ISA-18.2 is that an alarm requires a response. This means if the operator does not need to respond, then there should not be an alarm. Following this cardinal rule will help eliminate many potential alarm management issues.

ISA-18.2 also defines the following terms that are useful in describing the interactions of the alarm management and safety instrumented system lifecycles.

Safety alarm: An alarm that is classified as critical to process safety or to the protection of human life.

Safety function alarm: An alarm that indicates a demand on a safety function.

Manual Safety function alarm (Safety related alarm): An alarm that indicates an operator action is required to complete a safety function (e.g., operator initiated instrumented function).

System diagnostic alarm: An alarm generated by the control system to indicate a fault within the system hardware, software or components (e.g., communication error).

Highly managed alarm: An alarm belonging to a class with more requirements than general alarms (e.g. a safety alarm).

It is worth noting that an alarm from a safety instrumented system is not necessarily a safety alarm, though a manual safety function alarm is. Safety alarms are highly managed alarms. These definitions should be included in the alarm philosophy.

Philosophy

The usual starting point in the alarm lifecycle is the development of an alarm philosophy document, which defines how a company or site will address alarm management throughout all phases of the lifecycle. It includes key definitions, provides practices and procedures, and documents roles and responsibilities. It contains guidelines on how to classify and prioritize alarms, what colors will be used to indicate an alarm in the HMI, and how changes to the configuration will be managed. It also establishes key performance benchmarks, like the acceptable alarm load for the operator. For new plants, the alarm philosophy should be fully defined and approved before commissioning.

This is emphasized by Nimmo when he stated that “successful alarm management projects have a clear alarm philosophy that is well documented and understood by all disciplines……and a management mandate to solve the problem once and for all.” [7] Utilization of a philosophy must be embraced by all affected personnel (operator, technician, engineer and manager) within a facility and is a required element of ISA18.2. In addition, these individuals must take ownership of the process throughout its “Lifecycle”. Per Reising and Montgomery, “There is no ‘silver bullet’ or ‘one shot wonder’ for good alarm management. The most successful sites will likely approach alarm management as an ongoing, continuous improvement activity, not unlike preventive maintenance or total quality management programs.” [8]

The alarm philosophy is used to develop the alarm system requirements specification (ASRS), a description of required system level functionality.

If safety alarms are part of the alarm system, especially safety alarms with an independent operator interface, additional functions may be needed.

Identification

The identification stage of the alarm lifecycle is focused on identifying potential alarms from sources such as P&IDs, incident investigations, operating procedures, environmental permits, and ISO quality reviews, to name a few. Potential alarms may be identified during the following stages of the safety lifecycle:

- Hazard and Risk assessment
- Allocation of Safety Functions to Protection Layers
- Safety Requirements Specification for the Safety Instrumented System
- Design and Engineering of the Safety Instrumented System

Hazard and Operability Studies (HAZOPs) are a common technique used during the Hazard and Risk Assessment stage of the safety lifecycle. This safety lifecycle activity often singles out alarms as safeguards or results in recommendations to implement specific alarms to mitigate risk (as shown in the "Actions Required" column of Figure 4).

STUDY TITLE: PROCESS EXAMPLE								**SHEET:** 1 of 4	
Drawing No.:			**REV. No.:**					**DATE:** December 17, 1998	
TEAM COMPOSITION:			LB, DH, EK, NE, MG, JK					**MEETING DATE:** December 15, 1998	
PART CONSIDERED:			**Transfer line from supply tank A to reactor**						
DESIGN INTENT:			**Material:** A **Activity:** Transfer continuously at a rate greater than B **Source:** Tank for A **Destination:** Reactor						
No.	**Guide word**	**Element**	**Deviation**	**Possible causes**	**Consequences**	**Safeguards**	**Comments**	**Actions required**	**Action allocated to**
1	NO	Material A	No Material A	Supply Tank A is empty	No flow of A into reactor Explosion	None shown	Situation not acceptable	Consider installation on tank A of a low-level alarm plus a low/low-level trip to stop pump B	MG
2	NO	Transfer A (at a rate >B)	No transfer of A takes place	Pump A stopped, line blocked	Explosion	None shown	Situation not acceptable	Measurement of flow rate for material A plus a low flow alarm and a low flow which trips pump B	JK
3	MORE	Material A	More material A: supply tank over full	Filling of tank from tanker when insufficient capacity exists	Tank will overflow into bounded area	None shown	Remark: This would have been identified during examination of the tank	Consider high-level alarm if not previously identified	EK

Figure 4 – Sample HAZOP results identifying the need for Alarms [9]

Alarms identified during a HAZOP will be further analyzed and "designed" during the Rationalization stage.

Alarms can also be identified during the Allocation of Safety Functions to Protection Layers stage of the safety lifecycle. One of the most common techniques for calculating the required SIL target is the Layer of Protection Analysis (LOPA). 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 times the frequency of the initiating event. In the example LOPA of Figure 5, the reliability of the alarm system and the operator's response are included in the calculation. This LOPA uses a PFD of 0.2 for the alarm and the operator's response, which means that that operator is successful 80% of the time.

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 5. Example Layer of Protection Analysis (LOPA) Calculation

Assuming an 80% success rate might seem conservative, but studies have shown that human error is one of the leading causes of industrial accidents. Per Ian Nimmo, "many incident investigations have focused on the layer involving the BPCS, the supervisor, critical alarms and operator intervention as root cause for many incidents…….If the BPCS is not considered an IPL, the supervisor is not supervising, and the alarms are not functioning, then the IPL must then be left to operator intervention. This is highly variable due to the reliability of people and the factors that impact human performance." [10] As shown in Table 1, the performance of the alarm system and operator can be a significant variable in safety lifecycle calculations (PFD ranging between 0.01 to 1.0), effecting the design of the SIS. Taking a holistic approach ensures that safety alarms (such as those listed in a LOPA) are properly designed. Major problems could occur if the performance of the alarm system compromises the operator's ability to respond to the alarm - which would mean an increased PFD and corresponding increased risk of an accident.

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." [10]

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: • Ample indications exist that there is a condition requiring a shutdown • Operator has been trained in proper response • Operator has ample time (> 20 minutes) to perform the shutdown • 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. • Drilled response exists when written procedures, which are strictly followed, are drilled or repeatedly trained by the operations staff. • The drilled set of shutdowns forms a small fraction of all alarms where response is so highly practiced that its implementation is automatic • 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 1 – Simplified Technique for Estimating Operator Response [11]

Potential alarms can also be identified via the Safety Requirements Specification (SRS) or added during Design and Engineering. Alarms can be created to support the integrity of the safety system by indicating a demand on a safety layer, a failure of a partial stoke test, or a detected failure in safety system hardware that does not take the process to a safe state.

Rationalization

The purpose of Rationalization is to find the minimum set of alarms that are needed to keep the process safe and in the normal operating range. Rationalization involves reviewing and justifying potential alarms to ensure that they meet the criteria for being an alarm as defined in the philosophy. It also involves defining the attributes of each alarm (such as limit, priority, classification, and type) as well as documenting the consequence, response time, and operator action. Although safety alarms generally

tend to be some of the most critical in a plant, they still must go through the rationalization process. The product of rationalization is a list of configuration requirements recorded in the Master Alarm Database (MAD).

During rationalization, each alarm is examined to ensure it indicates an abnormal condition requiring a response from the operator. The allowable response time is documented. This information can be used to determine if an alarm should be used as a layer of protection.

Classification is an important activity during rationalization. The purpose of classification is to identify groups of alarms with similar characteristics and common requirements for training, testing, documentation, data retention, report generation, or management of change. The following are examples of classifications that might be assigned to safety-related alarms to help track and manage them through the entire lifecycle:

- Critical to Process Safety
- Critical to Environmental Protection

These classes are examples of Highly Managed Alarm (HMA) classes, and are subject to special requirements for operator training, frequency of testing, and archiving of alarm records for proof of regulatory compliance.

Alarm class is useful for managing alarms in the alarm system. It does not assist the operator. Alarm class may be related to the consequence associated with the alarm, but it is more often dependent on the method used to identify the alarm.

Prioritization is another important part of rationalization. Alarm priority is typically determined based on the severity of the potential consequences and the time to respond. Analysis of the severity of consequences is an activity that is common with the safety lifecycle. Most companies have a well established risk matrix that may be used for risk assessments and SIS design, typically established by a corporate risk management group. If possible the information in this risk matrix (consequence descriptions and categories) should be used as a basis for formulation of an alarm severity matrix for consistency. Risk matrices can often be large (example 6 x 6). ISA-18.2 recommends no more than 3 – 4 different alarm priorities in a system, so sometimes modifications are necessary to adjust for the reduced granularity.

	Consequence Category 1	Consequence Category 2	Consequence Category 3	Consequence Category 4	Consequence Category 5
Personnel	Negligible	Minor or no injury, no lost time.	Single injury, not severe, possible lost time.	One or more severe injury(s).	Fatality or permanently disabling injury.
Community	Negligible	No injury, hazard, or annoyance to public.	Odor or noise annoyance complaint from public.	One or more minor injury(s).	One or more severe injury(s)
Environmental	Negligible	Recordable with no agency notification or permit violation.	Release which results in agency notification or permit violation.	Significant release with serious offsite impact.	Significant release with serious offsite impact and more likely than not to cause immediate or long term health effects.
Financial	Minimal equipment damage at an estimated cost of less than $10,000.	Some equipment damage at an estimated cost of $100,000 to $1,000,000	Some equipment damage at an estimated cost of $100,000 to $1,000,000	Major equipment damage at an estimated cost of $1,000,000 to $10,000,000	Major or total destruction to process area(s) estimated at a cost greater than $10,000,000.

Table 2. Example Risk Matrix

Alarm priority is an attribute which is used to help the operator determine which alarm should be addressed first. To optimize operator response it is recommended that no more than three or four different priorities be used. Priority should be set based on the severity of the consequences and the time to respond as shown in Figure 6. For a safety alarm it is important to work with the direct (proximate) consequences and not the ultimate consequences which could occur after a series of failures.

Maximum Time To Respond	Consequence Severity: **MINOR**	Consequence Severity: **MAJOR**	Consequence Severity: **SEVERE**
> 30 Minutes	**No Alarm***	**No Alarm***	**No Alarm***
10 to 30 minutes	**Low**	**Low**	**Medium**
3 to 10	**Low**	**Medium**	**Medium**
< 3 minutes	**Medium**	**High**	**High**

Figure 6. Example Alarm Priority Matrix [12]

Determination of the alarm setpoint (limit) is another key activity during rationalization. Limits for safety alarms should be set taking into account the rate of change of the PV, process deadtime, the consequence threshold, and the operator's time to respond– which is part of the process safety time.

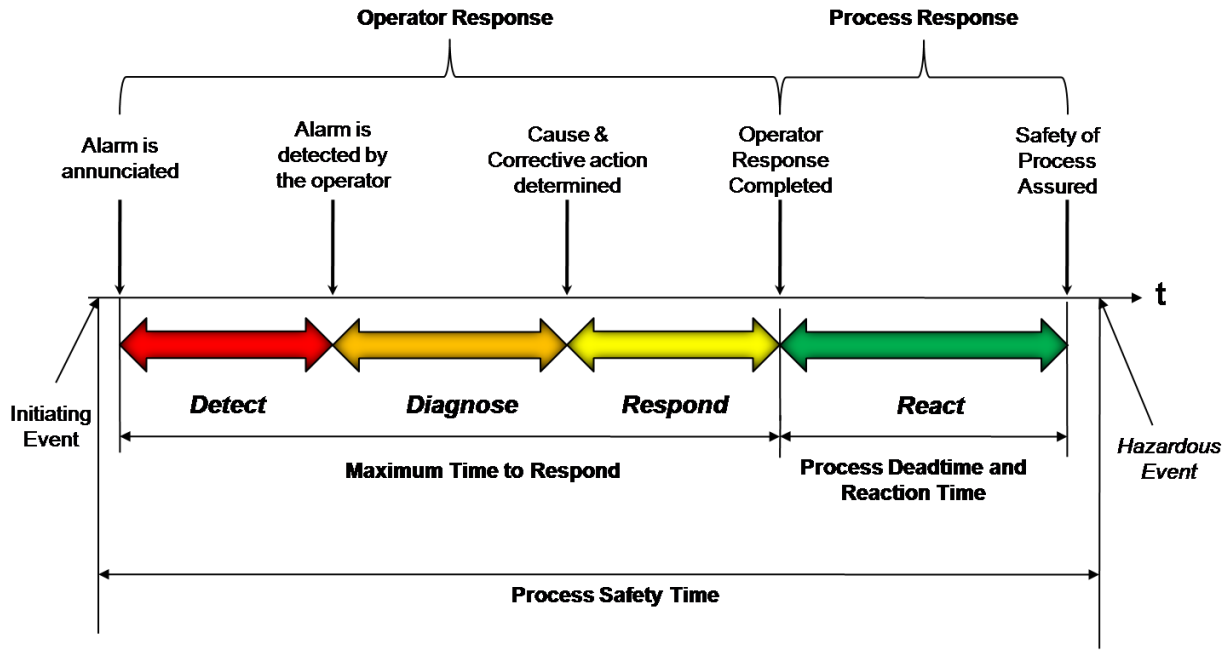

Figure 7 Operator Response Time vs. Process Safety Time

Design

In the detailed design stage of the alarm lifecycle, an alarm is designed to meet the requirements documented in the alarm philosophy and the Master Alarm Database. The alarm design stage includes the basic alarm design, setting parameters like the alarm deadband or off-delay time, advanced alarm design, where process or equipment state is used to automatically suppress an alarm, and HMI design, displaying the alarm to the operator so that they can effectively detect, diagnose, and respond.

Poor basic design and configuration practices are a leading cause of alarm management issues. Good configuration of alarm parameters like deadband and on/off delays can help prevent nuisance alarms, which obscures the operator's view, and false trips of safety alarms.

HMI design is concerned with the presentation of the alarm to the operator so that they can effectively diagnose, detect, and respond to it. Optimal use of color, text and patterns help make it easy for the operator to distinguish changes in alarm status. Reserving specific colors for alarms by priority ensures that alarms "jump off the page" at the operator. In cases where independent HMIs are used for SIS and BPCS (such as when an alarm has a risk reduction factor > 10), the SIS alarm status may be brought into the BPCS HMI (read only) as a means of providing the operator with the "big" picture, which is important for operator situational awareness.

In advanced alarm design, equipment or plant state (called plant mode in ISA-84) may be used to automatically suppress an alarm. In general, designed suppression is used to ensure that only alarms relevant to current plant conditions are annunciated to the operator. The display of safety alarms should typically not be suppressed without significant process and engineering analysis. On the other hand if safety alarms can be triggered during conditions when they are not relevant, then the design should be modified to take this into account.

Implementation

Implementation is the stage where an alarm is put into operation. It consists of training, testing, and commissioning. The functional safety lifecycle includes an analogous stage for installation, commissioning and validation. Testing and training are ongoing activities, particularly as new instrumentation and alarms are added to the system over time or process designs changes are made. Commissioning of safety instrumented systems may include the implementation of alarms. Alarms that are part of a SIF will also be validated.

For alarms to be effective, it is fundamental that the operator know what to do in response to the alarm. Initial and periodic training are necessary due to the dynamic nature of the process plant environment. Training on how to respond to safety alarms is critically important as these alarms will not occur frequently. As demonstrated in Table 1, the operator's ability to respond correctly to an alarm (as influenced by training) is clearly linked to its value as an independent layer of protection in an SIS.

Operation

During the operation stage, the alarm system performs its function of notifying the operator of the presence of an abnormal situation. The HMI provides multiple tools to help the operator manage and respond to alarms. These include the ability to shelve alarms and to place alarms out-of-service. Shelving is critical for helping an operator respond effectively during a plant upset by manually hiding less important alarms and keeping more important alarms, such as safety alarms, in the operator's view. Alarms that are shelved will reappear after a preset time period. The alarm philosophy should state if shelving of safety alarms is allowed.

Operator response can be improved by making available the information fleshed out during rationalization. Providing the alarm's cause, potential consequence, corrective action, and time to respond, all in context can maximize the likelihood that the operator responds correctly. Alarms that indicate an activation or a malfunction of the SIS may require an investigation and may kick off the process to perform a timely component repair (to be < the MTTR).

Maintenance

Maintenance is the stage where an alarm is taken out-of-service for repair, replacement, or testing. The process of placing an alarm out-of-service transitions the alarm from the operation stage to the maintenance stage, where it is no longer capable of performing its function of indicating the need for the operator to take action. ISA-18.2 defines the recommended elements of the procedure to remove an alarm from service and return it to service. The out-of-service state is not a function of the process equipment, rather an administrative process of suppressing (bypassing) an alarm using a permit system.

Safety alarms may require management approval and additional safe guards implemented before the operator removes them from service. These additional elements may be the use of internal administrative procedures to effectively mitigate the hazard during the period which the alarm is out of service or the use of other equipment or systems. It is important that clear guidance is provided by these procedures on who must be notified and what other indication will be provided to the operator to avoid the abnormal situation. It is also recommended that all out-of-service alarms be reviewed before starting up a unit or piece of equipment that had been down for maintenance. This is particularly important for safety alarms. The Chemical Safety Board investigation found that the explosion at the Texas City Refinery was in part caused by a malfunctioning level alarm whose operation had not been verified before restarting the isomerization unit. [13]

The safety lifecycle calls for regular testing of safety instrumented functions to verify the integrity of the system. Alarms that are part of a SIF should be tested regularly to verify operation and if possible that the operator responds correctly.

Assessment & Monitoring

During the Monitoring and Assessment stage the performance of the alarm system is analyzed and compared against recommended key performance indicators stated in the philosophy. Alarm overload is a key reason why operators “miss” alarms. One key performance metric is the rate at which alarms are presented to the operator. In order to provide adequate time to respond effectively, an operator should be presented with no more than one to two alarms every ten minutes. A related metric, shown in Table 3, is the percentage of ten minute intervals in which the operator received more than ten alarms (which indicates the presence of an alarm flood). Obviously if operators are overloaded with alarms, then it decreases the likelihood that they will respond correctly in the event of a safety alarm.

Alarm Performance Metrics 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 4 priorities: ~80% Low, ~15% Medium, ~5% High, ~<1% “highest” 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 3. ISA-18.2 Alarm Performance Metrics

Another key activity during this stage is identifying “nuisance” alarms - which are alarms that annunciate excessively, unnecessarily, or do not return to normal after the correct response is taken (e.g., chattering, fleeting, or stale alarms). The presence of these alarms can interfere with the operator’s ability to detect and respond to safety alarms.

Monitoring of alarm system performance can be used to maintain the integrity of the safety system. Also the reliability of an alarm cannot be determined without an understanding of the overall performance of the alarm system. Reports can be generated which document alarms that are triggered indicating that a demand has been placed on a SIF. The frequency of LOPA alarms (alarms that are listed in a layer of protection analysis) can be used to evaluate and validate the assumptions of initiating event frequency. Overall performance has a direct impact on the operator's ability to successfully respond to individual alarms. A poorly performing alarm system correlates to the **Response Unlikely / Unreliable** level shown in Table 1.

Management of Change

The management of change (MOC) stage entails the use of tools and procedures to ensure that modifications to the alarm system (including the addition of alarms, changes to alarms, and the deletion of alarms) are properly reviewed and authorized. Once the change is approved, the modified alarm is treated as identified and processed through the stages of rationalization, detailed design and implementation. Documentation including the MAD is updated and the operators are trained on the changes so they understand how to respond.

Modifications to the SIS may include changes to alarms, which would then be subject to the alarm management MOC process. Decommissioning of a SIF or SIS may also include the need to change or remove alarms. Changes to existing safety alarms not initiated from safety lifecycle activities would require review from the appropriate personnel. It may also require SIS lifecycle calculations to support the change. Proper documentation and enforcement of MOC procedures ensures that unauthorized changes of safety alarms do not occur.

Audit

The main activities in the audit stage are the periodic review of the work processes and the performance of the alarm system. The goal is to maintain the integrity of the alarm system throughout its lifecycle and to identify areas of improvement. One example is auditing how safety alarms are handled throughout the lifecycle. This may indicate the need for additional operator training or new procedures related to management of change or testing. Changes resulting from the audit process must be rolled in to the alarm philosophy document. They may also necessitate the need to review the existing alarms and to cycle back through the other stages of the alarm lifecycle.

References

1. ANSI/ISA ISA18.00.02-2009 “Management of Alarm Systems for the Process Industries”.
2. Bransby ML and Jenkinson J., The Management of Alarm Systems, HSE Contract Research Report 166/1998 ISBN 07176 15154, First published 1998.
3. Campbell Brown, D., “Horses for Courses – A Vision for Alarm Management,” IBC Seminar on “Alarm systems,” London, June 26-27, 2002.
4. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) “Functional Safety: Safety Instrumented Systems for the Process Industry Sector”.
5. Stauffer, T., Sands, N., and Dunn, D., “Alarm Management and ISA-18 – A Journey, Not a Destination” Texas A&M Instrumentation Symposium (2010).
6. Campbell Brown, D., “Alarm System Performance – One Size Fits All?”, Measurment & Control, May 2003.
7. *Nimmo, I., “Rescue Your Plant from Alarm Overload,” Chemical Processing, January 2005.*
8. Reising, D.V. and Montgomery, T., “Achieving Effective Alarm System Performance: Results of ASM Consortium Benchmarking against the EEMUA Guide for Alarm Systems,” 20th.
9. *IEC-61882 ‘Hazard and operability studies (HAZOP studies) – Application guide’ 2001*
10. Nimmo, I., “The Operator as IPL,” Hydrocarbon Engineering, September 2005.
11. Marszal, E. and Scharpf, E. “Safety Integrity Level Selection”. ISA (2002)
12. Hollifield, B. and Habibi, E., “Alarm Management: Seven Effective Methods for Optimum Performance,” ISA, 2007
13. “BP America Refinery Explosion” U.S. CHEMICAL SAFETY BOARD www.chemsafety.gov/investigations

Revision History

Authors: Todd Stauffer, Nicholas P. Sands, Donald G. Dunn

Presented at ISA Safety & Security Symposium (April 2010)

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