Managing Alarms to Support Operational Discipline

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

April 2016

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

Keywords: Process Safety, Alarm Management, Rationalization, Prioritization, Independent Protection Layers, Nuisance Alarms

Abstract

Process alarms, coupled with operator action, are frequently cited as a safeguard in a Process Hazard Analysis (PHA) and an Independent Protection Layers (IPL) in a Layer of Protection Analysis (LOPA), but does the alarm management system really support the safeguard/IPL?

According to ISA-18.2 / IEC 62682 an alarm must indicate an equipment malfunction, process deviation, or abnormal condition that requires a timely operator action. If no action is taken, then the alarm is either invalid or the operator is not doing their job. Both scenarios represent a breakdown in operational discipline for alarm management as does the presence of nuisance alarms and alarm floods. This breakdown in operational discipline for alarms has been cited as a contributing factor in many significant safety incidents, some of which will be analyzed in this paper. If operational discipline for alarms is lacking, then it is very possible that the desired risk reduction for a process alarm used as an IPL will not be achieved and the probability of an ineffective operator response will increase.

As systems have evolved from hardwire to computer control, alarms have become easier and less expensive to implement leading to more and less purposeful alarms. Operators must contend with multiple alarms at one time with only their experience to determine priority. Alarms may be added to or removed from a control system without proper management of change. Systems may include alarms for which there is no possible action, or inadequate action time. What can an organization do to take control of their process alarms and improve operational discipline?

Conclusion

Process alarms and operator action is heavily relied upon as an independent protection layer in the process safety model. Four events have been analyzed demonstrating how this safety layer can be rendered ineffective when an operator is faced with too many alarms, unclear priorities, and nuisance alarms. Alarms where operator action is unclear, or there is inadequate time to affect response can lead to deadly consequences. A successful alarm management system can filter out useless alarms, direct notifications to responsible parties, and address design flaws that generate nuisance alarms. It supports documentation of process knowledge that can be used in operator training and become the basis for operator help. Discipline is established in alarm management giving the operator the tools needed to do the right thing, the right way every time.

Introduction

Operational discipline is the practice of doing the right things the right way every time. Success is predicated on having a well-defined process and trained personnel. The process is usually described through operating procedures, work instructions and tools. Personnel are trained to follow the procedures, understand the instruction and use the tools. An organization can become very experienced and repeatable in executing the well understood normal processes. By definition, alarms are triggered when there is an abnormal condition in the process. The situation may or may not be addressed in the procedures, instructions, tools and operator experience. In many control rooms, alarms sound so frequently that operators miss important alarms in the constant flow across the alarm banner. Worse yet, they become accepting of the condition as 'normal' and no longer recognize alarms as a warning of potential trouble. This paper describes techniques to establish an alarm management program that will equip operators to take the correct action every time they are presented with an alarm.

Notation

BDI	Burst Disk Indication
DCS	Distributed Control System
ISA	International Society of Automation
I/O	Input/Output
IPL	Independent Protection Layers
KPI	Key Performance Indicator
LOPA	Layer of Protection Analysis
MOC	Management of Change
OD	Operational Discipline
OSHA	Occupational Safety & Health Administration
PHA	Process Hazard Analysis
PLC	Programmable Logic Controller

Role of Alarm Management in Operational Discipline

Background

Prior to the advent of DCS and PLCs in the 50s, process control systems consisted of a few wires and mechanical devices. Each device required a capital investment so theoretically, every control loop and interlock were well thought out and justified in the design process. Process alarms were so rare that each one was taken very seriously by operators. As DCS/PLC capabilities have evolved, it has become cheaper and easier to implement alarms. Control system designers will often enable multiple alarms (3, 5 or more) by default per analog I/O point without thinking about whether they are really needed. Many are configured as a matter of routine. PHA and quality control interest may dictate additional alarms to make the operator aware of a condition trending toward abnormal. The result is a situation where operators are presented with so much information that they cannot effectively manage the influx of data and are likely to miss critical situations. An operator may correctly identify an alarm, but the time between alarm and event is inadequate for an operator to effect corrective action. Frequent alarms with no corrective action may desensitize operators so they become slow to act in response to a truly abnormal event. Alarm overload, inadequate response time and nuisance alarms have been contributing factors in industrial accidents. Specific examples are described in the sections below.

The Human Element

Operational Discipline (OD) is defined as the deeply rooted dedication and commitment by every member of an organization to carry out each task the right way every time [1]. For effective operational discipline, procedures are well documented and codified into best practices. Three personal characteristics are required of employees in an organization with effective OD [2]:

- Awareness – the ability to anticipate potential problems and recognize unusual situations;
- Knowledge – an understanding of how to do a task correctly and safely; • Commitment – dedication to doing the task the right way, every time.

Unfortunately, many organizations use alarm management practices that diminish operator effectiveness and undermine operational discipline. When alarm management procedures are not defined and the expected operator response to alarms is not documented, how do operators gain knowledge to act correctly? A process plagued by nuisance alarms reinforces negative behaviors and breeds indifference to certain alarms. Alarm floods mask real problems within a deluge of alarm signals making it difficult for the operator to be aware of what is occurring within the process. If metrics are not established to monitor alarm system performance, issues that negatively impact OD go unidentified. An undefined alarm management program cannot be audited and improved to achieve best practice.

The operator is charged with the responsibility to detect abnormal situations (awareness), diagnose the situation (knowledge) and respond to correct the condition (commitment). D.G. Dunn, et al. [3] performed a study of eleven incidents to analyze the mechanisms where operational discipline broke down and the alarm protection layer failed. The mechanisms studied in the review are summarized in Figure 1.

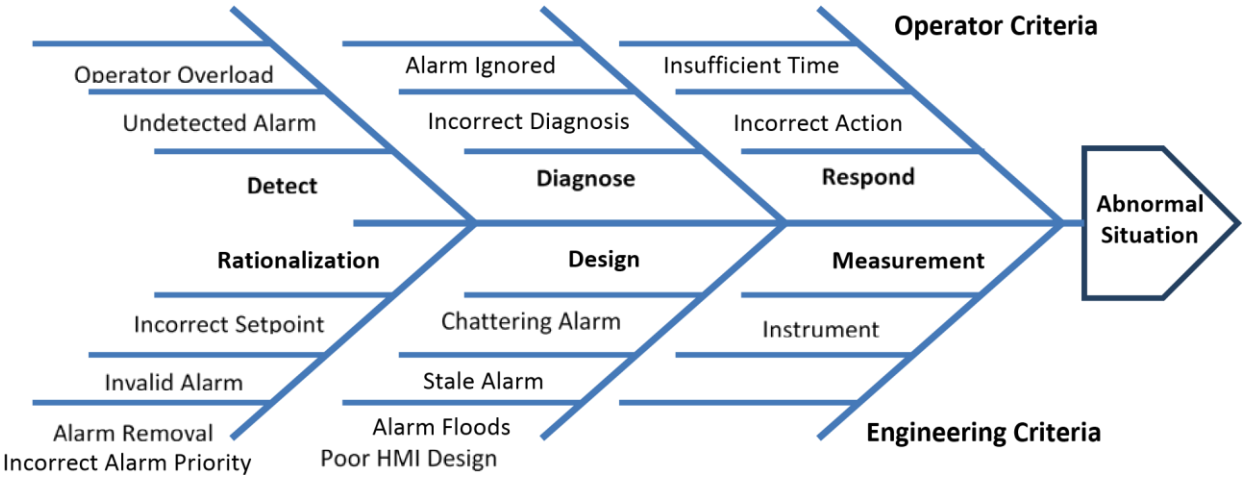


Figure 1. Failure Mechanisms (Fishbone)[1]

Poorly designed alarms (chattering, stale, flood) lead to operator overload and undetected alarms. Absence of a rationalization process can lead to alarms with incorrect priority or presence of invalid alarms drawing operator attention away from a more important situation, hinders diagnosis and produces a culture of ignoring alarms. Poorly defined alarms and incorrect set points lead to incorrect response and inadequate operator response time. A well-defined and executed alarm management program includes OD principals to eliminate alarm failure mechanisms.

Metrics

For a brownfield facility the best place to start development of an Alarm Management program is to understand the types of existing operational issues. Some performance indicators can be extracted from existing operating logs, while other information may be gleaned from antecedent evidence. Though a formal process is necessary long term, useful insights can be gained by performing a clipboard test and informally documenting alarm activity for a period of 20 minutes [4]. Information such as the number of new alarms, operator actions taken, and standing alarms should be noted. The highest priority alarm and alarms remaining active for the test period should be captured. Operator response to alarms should be noted. Do the operator(s) show signs of stress, or desensitization? Impressions from the informal test should be considered alongside statistics collected from the alarm history.

Analytical information is an important tool to assess the health of the alarm management system. Initial data should be analyzed to identify the types of alarm issues that are present in order to set priorities for improvement, and identify gaps in other parts of the overall process safety program (e.g. design, training). A successful alarm management program includes routine monitoring and periodic auditing. Metrics considered in the preliminary analysis will form the basis of long term metrics. Within the Alarm Philosophy, a set of Key Performance Indicators (KPIs) should be established and a process for routine monitoring of the KPIs established. Goals should be determine for system performance, and threshold limits for performance tolerance. Figure 2 is an example set of KPIs.

[1] Reference [3], pg. 4.

Metric	Target	Action Limit
Average alarm rate per operator, alarms/day	<300	>600
Average alarm rate per operator, alarms/10 minutes, %	1-2	>4
Time alarm system is in flood, i.e., >10 alarms/10 minutes, %	<1	>5
Hours with >30 alarms, %	<1	>5
Average number of alarms out of service, %	<1	>5
Low priority alarms in total alarms, %	~ 80	<50
Medium priority alarms in total alarms, %	~ 15	>25
High priority alarms in total alarms, %	~ 5	>15
Top ten most frequent alarms' contribution to total alarms, %	<1 - ~ 5	>20
Number of stale alarms, i.e., active for > 24 hours, on any day	<5	>5
Number of chattering and fleeting alarms	0	>5

Figure 2. Monthly Performance Metric Analysis

A key OD paradigm is that there is "no improvement without action". Routine monitoring will identify alarms where initial rationalization failed to achieve desired results. These should be re-rationalized challenging original assumptions and evaluating supplementary information. In addition to the routine monitoring, periodic audits must be performed. The audit should look at the entire process comparing actual implementation against the processes defined in the philosophy. A comparison of the DCS configuration against the alarm rationalization tool is useful to identify gaps in the management of change process. Action items from the audit need to be tracked and closed out in a timely manner.

Establishing Best Practice

Anatomy of an Alarm Management Program

Operator action in response to alarms is an important safeguard that is frequently credited as an Independent Protection Layer (IPL). Safety incidents do occur when the alarm response layer fails.

Mistakes happen when operators must filter through overwhelming or confusing alarm information to determine what situations need action, which is most important to resolve, or what action should be taken. A robust alarm management system will reduce alarms to a manageable level, establish clear priorities, and provide direction to the operators. The lifecycle approach described in ISA 18.2 [5] provides a best practice approach to defining alarms, monitoring performance, managing change and Auditing progress. The lifecycle is given in Figure 3.

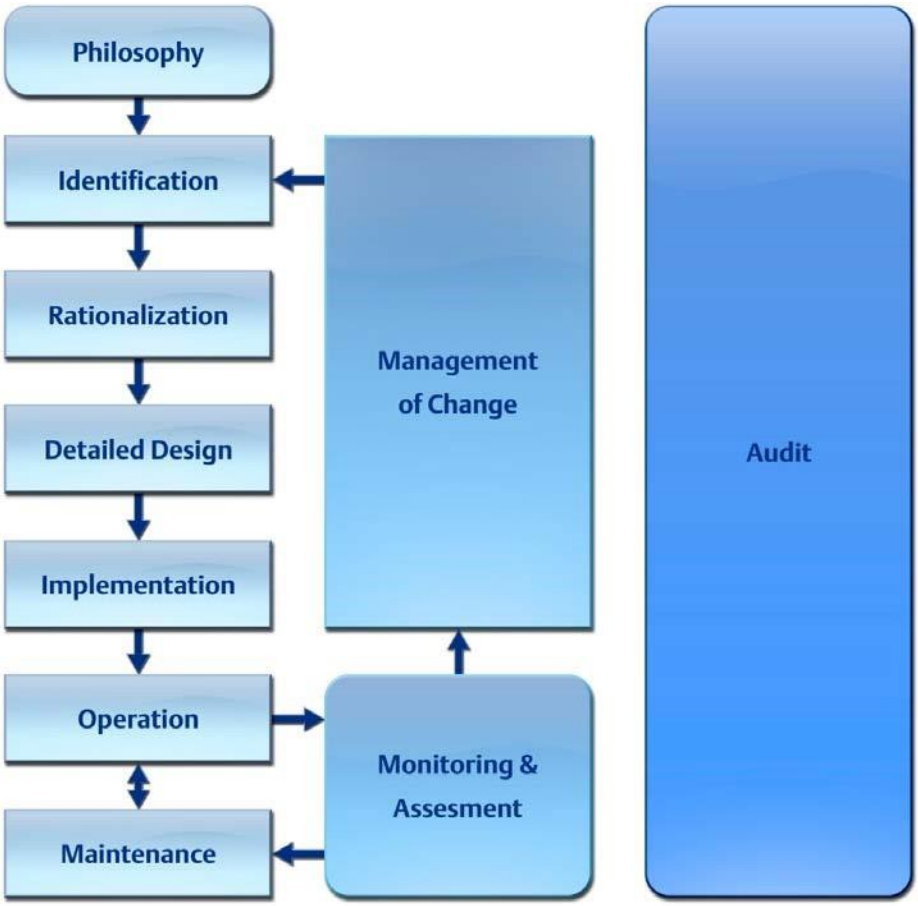


Figure 3. ANSI/ISA-18.2 Alarm Management Lifecycle

Implementation of an alarm management system is a journey that requires an ongoing commitment. A detailed discussion on how to implement a program is available in the July 2012 issue of Chemical Engineering Progress (CEP) [6]. Key elements of an alarm management program are summarized here as background to illustrate how specific OD issues cited within this paper can be addressed.

Alarm Philosophy

The first step in developing a robust alarm management system is to document the philosophy. The philosophy is a statement of best practices and establishes lifecycle activities, roles and responsibilities, procedures and processes, and monitoring metrics. It will define the alarm and non-alarm notification categories, provide rules for prioritization and disposition of alarms and non-alarm notifications, and

document the alarm rationalization procedure, Guidance should be included on how to establish alarm set points to allow an operator adequate time to respond to alarms. Techniques to handle fleeting, chattering and other nuisance alarms, as well as advanced alarm management should be included. Finally the procedure for monitoring alarm performance, metrics to measure success, management of change requirements, personnel training and auditing intent is included.

Defining Alarms

When faced with an alarm overload situation an operator only has a short time to process and address each alarm signal they receive. The situation is greatly improved by sorting out what is truly an alarm from other notifications, and redirecting the notifications away from the alarm banner. ISA 18.2 defines an alarm as:

> An audible and/or visible means of indicating to the operator an equipment malfunction, process deviation or abnormal condition requiring a (timely) response.

Within a DCS, the modules for process variables include a default set of configuration points (high, high-high, low, etc.) that offer a means to identify a potentially abnormal process condition and communicate when the condition is met. These are often referred to as alarm points. In practice people refer to events generated from these configuration points as alarms. In reality, a large percentage of these communications do not meet the ISA definition of alarm and should actually be considered as different types of notifications. When alarm points are rationalized, they should first be sorted into alarm and non-alarm categories. Figure 4 illustrated four major categories and the rationale for each.

	Operator Must Act	FYI to the Operator
Abnormal	Alarm	Alert
Normal	Prompt	Message

Figure 4. Notification and Alarm Categories

The categories may be further subdivided based on the responsibility for and method of disposition. Some characteristics include:

- An alarm must be due to an abnormal condition and have a defined operator response. There must be adequate time for the operator to carry out the response. Each alarm presented to the operator should be useful, relevant and unique. The alarm will alert the operator of the condition, inform them of the proper response, and guide operator action. Examples: High level alarm on a storage tank; high rate of temperature increase in a reactor.
- A prompt is a normal condition that requires an operator response. Prompts are usually associated with a routine batch type operation where operator intervention is required to proceed to the next stage. Examples: Signal for operator to perform manual charge in a batch reaction; indication that truck unloading is complete.

- An alert communicates to the operator that an abnormal situation has occurred, but there is no action to be performed by the operator or the timeframe for response is long (e.g., extends beyond a single shift). They are typically displayed to the operator on a separate screen from the alarm list. Alerts may require action by others and may also be communicated directly to the responsible parties. Examples: A bad measurement signal indicating that a transmitter requires maintenance attention; an indication that an interlock has tripped.
- A message includes things that are both normal and informative. It includes communication that requires no action but may be relevant in a diagnostic or reporting perspective. Examples include: indication of an automated pump run status, indication that an automated regeneration cycle has completed a particular step.

Although a prompt, alert and message are not truly alarms, they are often assigned an alarm priority if the DCS alarm system is to be used to communicate all types of operator notifications. The alarm philosophy document will define the various categories and establish priority and communication criteria for each. This may be presented in the form of a guidance table. Figure 5 is an example:

Alarm Category	**Alarm Priority**	**Alarm Summary** (Where the alarm appears)
Safety shower and eye wash alarm	High	Alarm List
Gas Monitors (low O2, NO2,NOx N2)	High	Alarm List
Process interlock trip with no corrective action required	Alert	Alert List
Process interlock trip with corrective action required	Per Alarm Prioritization matrix (Refer to section 5.4)	Alarm List
Bad process variable of a BPCS sensor	See note 1	Alarm List, Maintenance Alarm List
Power System Diagnostic alarms	Medium	Alarm List , Maintenance Alarm List
Note 1: The alarm priority should be set equal to the highest priority alarm condition of the tag. If no alarms are configured for the tag, the priority of a BAD_PV alarm should be set equal to Alert.		

Figure 5. Example Alarm Priority by Category

Alarm Rationalization and Prioritization

Since an alarm's priority should be indicative of its relative importance, when presented with multiple alarms, the operator diagnose and respond process may be confounded by alarm priorities assigned in a subjective fashion rather than by rationalization. Many alarm systems are configured based on a simple perception of the importance of an alarm, leading to a near even distribution between low, medium and high priority alarms, or a disproportionally high percentage of the alarms assigned to the highest priority. In a stressful situation, an operator faces additional decision challenges when the most critical priority level includes alarms the operator believes to be of lower significance. ISA 18.2 recommends the distribution for annunciated alarm priorities given in Figure 6.

Priority	3 Priority Distribution	4 Priority Distribution
Highest	N/A	~1%
High	~5%	~5%
Medium	~15%	~15%
Low	~80%	~80%

Figure 6. ISA 18.2 Annunciated Alarm Priority Distribution

The alarm philosophy will establish prioritization levels for alarms and the criteria for each level. Three and four level schemes are most common. Priority is established based on the immediate consequence of operator inaction, and the time requirement for operator response. An example of consequence decision criteria is given in Figure 7.

Type of Consequence (Impact Area)	Direct Consequence of Inaction or Incorrect Action			
	NEGLIGIBLE	MINOR	MAJOR	SEVERE
Personnel	Injury requiring medical treatment with no lost time.	Injury requiring medical treatment, time off work and rehabilitation.	Permanent disabling injury and/or long term time off work.	Fatality
Public or Environment	Negligible impact	Onsite impact	Short-term, offsite impact	Long term impact.
Financial	Event or lost production costing <$100K.	Event or lost production costing $100K to $1M	Event or lost production costing $1M to $10M	Event or lost production costing >$10M

Figure 7. Example Alarm Consequence Description

The consequence of operator inaction is assessed based on the next immediate (direct) consequence in the chain of events, not the ultimate consequence in the scenario. For example, in a tank overflow scenario, the immediate consequence of operator failure to act on the high alarm may be the activation of a high-high interlock stopping feed to the tank. If tripping the interlock would cause a process upset costing the organization more than $100K in lost production, the consequence would be defined as minor per the consequence criteria in Figure 7.

Operator response time is the second factor used to set priority. The operator response time is the maximum time between the annunciation of the alarm and the time the operator must take corrective action to avoid the consequence. Priority is typically determined by considering both response time and severity of the consequences. An example of a priority matrix is given in Figure 8.

Time Available to Respond	Alarm Priority			
	Event has Negligible Consequence	Event has Minor Consequence	Event has Major Consequence	Event has Severe Consequence
Not Urgent (>30 Min)	No Alarm	Re-engineer the alarm for urgency (Invalid)	Low/ Re-engineer the alarm for urgency	Medium/ Re-engineer the alarm for urgency
Prompt (<30 Min)	No Alarm	Low	Low	Medium
Rapid (<15 min)	No Alarm	Low	Medium	High
Immediate (<5 min)	No Alarm	Medium	High	Invalid

Figure 8. Example Alarm Prioritization Matrix

The operator action timeline is important to the decision criteria. In the minor consequence example above, if the relative set points of the high alarm and high-high interlock were defined so that at the fill rate an operator had less than 5 minutes response time to avoid interlock trip, the priority would be set to Medium per Figure 8. Available response time of significantly more than 5 minutes would deliver a priority of Low.

The success of alarm prioritization is predicated on the assumption that the priority matrix accurately reflects company business / risk criteria. At the end of the day when multiple alarms are presented to the operator at the same time, the priority should indicate which one is more critical to safety and the business.

Operator training is also important. Operators must be trained to immediately respond to every alarm and use alarm priority to determine relative importance when multiple alarms are active at the same time. For example, a board operator receiving a high and medium priority alarm at the same time would assign a field operator to the high alarm first, then seek assistance from a different field operator to

address the medium alarm. Figure 8 includes notations in the chart that indicate different disposition is required.

- "No Alarm" is assigned whenever the consequences are negligible. These may be handled as messages or alerts if the rationalization team feels there is value in having a notification, or they can be disabled.
- "Re-engineer the alarm for urgency": These alarms may be set to the indicated priority or should be considered for re-engineering to ensure that there is a level of urgency to the response (for consistency with other types of alarms).
- "Invalid" indicates a design scenario that should be avoided (< 5 mins to prevent significant consequences such as a fatality). Alarms falling into this band should be re-engineered to automate the response, incorporate additional safeguards, or utilize inherently safer design.

Detect (Awareness)

A nuisance alarm is one that annunciates excessively, unnecessarily or does not return to a normal state after correct response has been taken. It will lead to ignoring of alarms and failure to detect an abnormal condition. Too often organizations respond to the nuisance condition by failure of operational discipline. Reflexive silencing, removing annunciation, ignoring visual indication or inhibiting/disabling the alarm are common responses.

The January 2010 Methyl Chloride release at the DuPont Belle, WV facility [7] occurred when a nuisance rupture disk burst indication alarm went un-addressed for an extended period of time. The rupture disk is located on a common vent line between two reactors and a scrubber. A 0.5 inch weep hole (source of leak in the incident) was installed in the piping just downstream of the rupture disk inside the process building, and the main discharge line vented to the roof. The rupture disk burst indication (BDI) had a long history of nuisance alarms, mostly due to a low battery signal on the BDI sensor. Operators became accustomed to frequent alarms but experienced only a few true activations, so they had become desensitized to the alarm. In the four-month turnaround just prior to the event, the rupture disk style had been changed to one with a more reliable indication, and the indicator power source was converted from a battery (monthly replacement) to a continuous power supply. The disk is believed to have ruptured during outage and the alarm had been ignored (became stale) because there were no process hazards present at the time of the alarm. When chemicals were reintroduced into the process several weeks later, operators did not recognize the stale alarm as a concern because of the nuisance history. An estimated 2,000 pounds of methyl chloride was released over 5 days until a process area gas detection alarm brought the situation to the attention of operators and the process was shut down.

Nuisance alarms undermine operational discipline. They distract and desensitize the operator leading them to ignore alarms. Frequent, chattering or fleeting alarms increase operator stress and can lead to missing other alarms.

Frequently occurring alarms, or bad actors, annunciate excessively but rarely indicate a true problem. The DuPont rupture disk burst indication event is a classic example. The alarm was originally configured so that the operators received the same signal for a low battery warning as they did for a burst disk indication. Operators had become so desensitized to the alarm being active from battery warnings, that it became a stale alarm and was not cleared prior to start-up following the outage. Because the operators were accustomed to seeing a false alarm, they failed to act in the correct way and resolve the alarm before introducing hazards into the process. Prioritizing the low battery indication as an alert

separately from the burst indication alarm would have reduced the number of alarms and would have retained the importance of the BDI indication.

Diagnose (Knowledge)

The DuPont Belle, WV incident [7] is an example where a nuisance alarm was tolerated and fortunately, the consequences were minor. The general (evacuation) alarm on the Deepwater Horizon [8, 9] is an example of where inhibiting an alarm so as to avoid a potential nuisance alarm can have fatal consequences. It also illustrates how operational discipline can crumble in a high stress situation when operators are uncertain of the proper response to a situation.

The April 2010 Macondo well blowout on the Deepwater Horizon Rig provides a lesson on the importance of well-considered alarm management practices. The event occurred during temporary abandonment[2] operations of the well. A kick[3] escalated to a blowout[d], then to an explosion and fire that continued two days until the rig sank [8, 9]. Eleven people were killed, 17 critically injured and almost 5 million barrels[4] of oil discharged into the Gulf of Mexico. The general alarm system on the rig was operating in "inhibited" mode[f] so the general alarm would not automatically trip on actuation of multiple area gas detection alarms in different areas of the rig. According to testimony of the chief electronics technician, the system was configured in inhibit mode because "they did not want people woke up at 3 o'clock in the morning due to false alarms" [10]. According to the event times reported in the US Department of the Interior report[5], multiple local gas alarms sounded 1-2 minutes before the first explosion, but the general alarm was not sounded until about 10 minutes after the explosion. Witness testimony suggests there was some uncertainty as to when personnel should manually trigger the general alarm. The investigation Panel[6] determined:

> The *Deepwater Horizon* operated a manually-functioned general alarm system. If the general alarm of the *Deepwater Horizon* had been set to automatically sound when "high-high" gas alarms sounded in multiple compartments of the rig, personnel in the pump room likely could have moved to a location where their chances of survival were greater. **The "inhibited" general alarm system was a possible contributing cause of the response failure.**[i]

Assurance that the operator is equipped to 'do the right thing every time' requires an assessment of the hazards, documented required operator action, operator training, and tools to assist operators. The alarm rationalization process will identify and document likely cause(s), consequence, confirmation and corrective action related to an alarm. Figure 9 is an example of SILAlarm rationalization documentation.

---

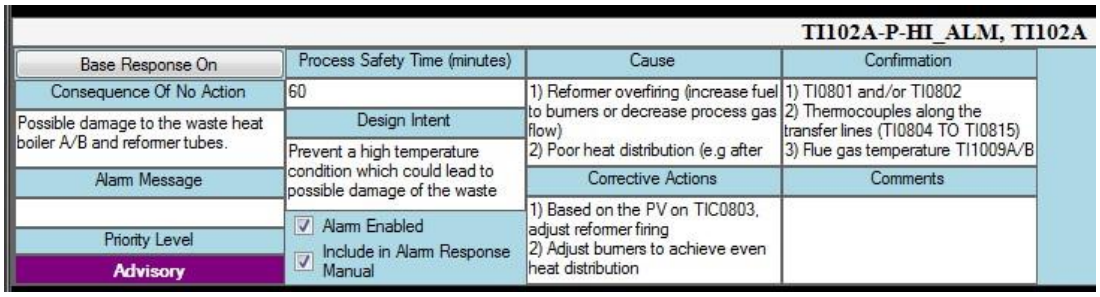
[2] The temporary closure of a well so that the drill rig can be moved off and a production rig can be put in place.

[3] An unplanned flow of fluids into the wellbore. [d] An uncontrolled hydrocarbon release into the environment.

[4] Reference [9], pg. 31. [f] Reference [8], pg. 4.

[5] Reference [8]

[6] The Joint Investigation Team of the Bureau of Ocean Energy Management, Regulation and Enforcement ("BOEMRE") and the United States Coast Guard. [i] Reference [8], pg. 114.



TI102A-P-HI_ALM, TI102A

Base Response On	Process Safety Time (minutes)	Cause	Confirmation
Consequence Of No Action	60	1) Reformer overfiring (increase fuel to burners or decrease process gas flow) 2) Poor heat distribution (e.g after	1) TI0801 and/or TI0802 2) Thermocouples along the transfer lines (TI0804 TO TI0815) 3) Flue gas temperature TI1009A/B
Possible damage to the waste heat boiler A/B and reformer tubes.	Design Intent	Corrective Actions	Comments
Alarm Message	Prevent a high temperature condition which could lead to possible damage of the waste	1) Based on the PV on TIC0803, adjust reformer firing 2) Adjust burners to achieve even heat distribution	
	☑ Alarm Enabled		
Priority Level	☑ Include in Alarm Response Manual		
Advisory			

Figure 9. Example Alarm Response Procedure

In the rationalization example, the potential consequences of inaction, causes for the alarm, means to confirm that the alarm is real, and corrective action for each cause is identified. The information clarifies operator response action and timeline to the rationalization team for priority ranking, and provides important information for operator training and operating procedure content. The information captured during the rationalization exercise can be displayed to the operator in the form of an interactive help file (in some systems) or from the alarm response procedure (manual) shown in Figure 10.

SILALARM

Alarm Response Procedure Report

Tag ID	TI102A			
Tag Description	Compressor Bearing Temp A			
Location	REACTORS_AREA/ UM_REACTOR_1 /			
Range	0	To	100	no units
Alarm Name	TI102A-P-HI_ALM			
Alarm Message				
Alarm Type	High			
Priority	Advisory			
Limit	95			
Time to Respond	15-30 Minutes			
Classifications	• 4 - HAZOP Safeguard			
Cause	1) Reformer overfiring (increase fuel to burners or decrease process gas flow) 2) Poor heat distribution (e.g after burning and tubes with high DPs)			
Confirmation	1) TI0801 and/or TI0802 2) Thermocouples along the transfer lines (TI0804 TO TI0815) 3) Flue gas temperature TI1009A/B			
Consequence Of No Action	Possible damage to the waste heat boiler A/B and reformer tubes.			
Corrective Actions	1) Based on the PV on TIC0803, adjust reformer firing 2) Adjust burners to achieve even heat distribution			

Figure 10. Example SILAlarm Alarm Response Manual

Well trained operators should possess knowledge necessary to diagnose an alarm; however, as the Deepwater Horizon incident illustrates, in times of stress, operator decision processes can be slow and/or incorrect. Making this type procedure available to the operator will support operational discipline by providing information that can improve the speed and accuracy of diagnose, especially in times of stress.

Respond (Commitment)

Operator response time is dependent on the process dynamics (including rate of change) and alarm set point. In a properly rationalized system, the operator will view alarm priority as an indicator of which alarm needs attention first. In a system where alarms are not rationalized, the multiple alarms may sound with the same priority, or with priorities that are inconsistent with operator experience. The operator may not know where to respond first and may not have adequate response time available to be effective. Alarms are cited as a protection layer in a PHA and/or LOPA; however, the review teams don't always accurately consider the operator's ability to respond in a given timeframe. This can lead to a situation where the operator can do the right thing and still have an undesirable outcome.

The 2008 Bayer CropScience runaway (decomposition) reaction in Institute, West Virginia [11] is an example of the operator doing the right thing without sufficient response time built into the design of the alarm. The event occurred during restart of the methomyl unit following a control system and residue treater replacement. Operational discipline failed in several ways enabling the event conditions:

- During start-up, operators failed to complete steps that would pre-fill the residue treater with solvent prior to introducing methomyl containing flasher bottoms feed.
- The start-up was complicated because some systems were still being modified and the operators were not completely familiar with the new control system workstations and their function.
- Issues with centrifuge operation resulted in high methomyl centrate eventually reaching residue treater. This coupled with the solvent pre-fill error led to a much more reactive composition than normal in the residue treater prior to startup of the vessel.
- On start-up of the residue treater, recirculation and minimum temperatures interlocks were bypassed.

The vessel was heated and recirculation was established. As the contents began to react, the temperature rate of increase moved from 0.6°C/min to 2°C/min while pressure held steady, until the critical decomposition temperature was reached and pressure began increase. By the time the high-pressure alarm sounded, vessel pressure was climbing rapidly. The lead operator dispatched two operators to the area for troubleshooting and manually switched to full cooling. The vessel exploded 8 minutes after the high-pressure alarm sounded. The explosion, fire and toxic chemical release resulted in the death of two operators, eight injured and shelter in place ordered for 40,000 people.

Thoughtful determination of alarm and set point is critical to assure that operators have adequate time to address the alarm to avoid the immediate consequences. The 2008 Bayer CropScience runaway reaction illustrates the consequence of improper alarm selection and set point determination. The multiple failures leading to the runaway scenario had not been identified in a PHA, therefore was not considered in alarm design. However, an analysis of the chemical reaction behavior may have identified an improved alarm design providing operators more response time to resolve the situation. Figure 12 is a chart of process indication leading up to the vessel rupture.

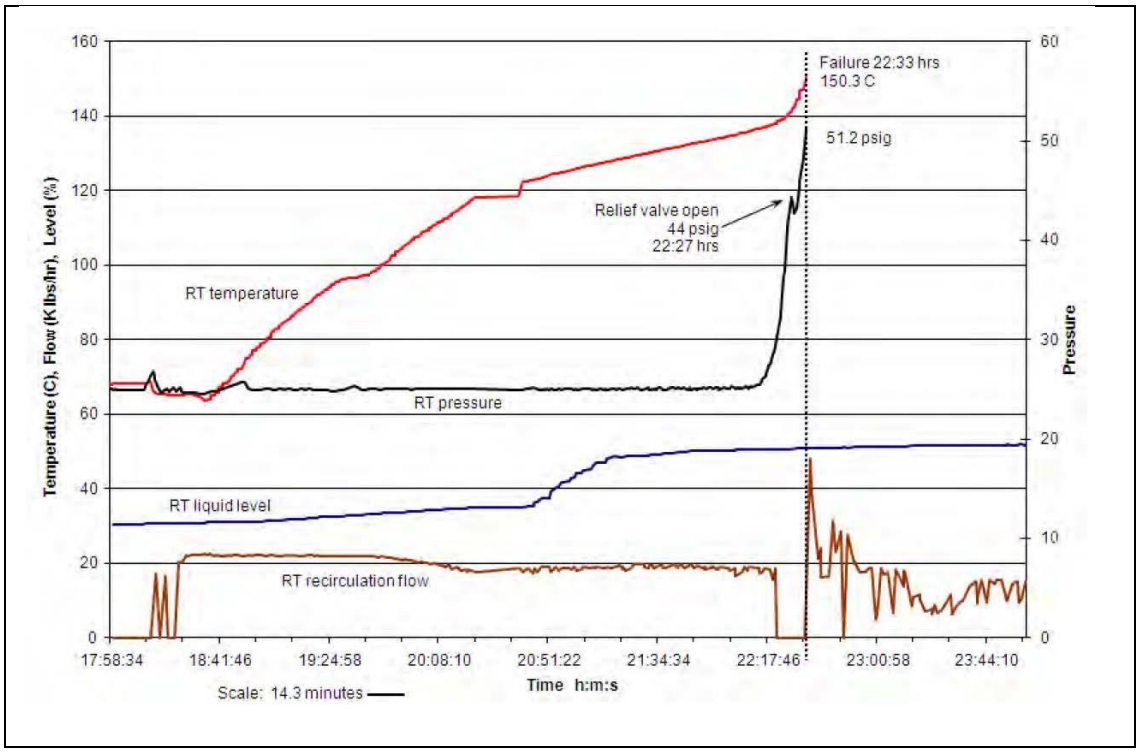


Figure 11. Residue Treater Process Variables before the Explosion[7]

Runaway and decomposition reactions often show a predictable temperature/pressure relationship. Laboratory testing can be utilized to determine the nature of this relationship. The information is then used to select the best alarm indicators for a potential event, and establish set points for those alarms. In a decomposition runaway, the temperature will increase at constant pressure until the reaction initiates, then pressure increases rapidly. The process data in Figure 11 illustrates classic decomposition reaction behavior. There is no indication in the CSB report that the operator received any temperature alarms prior to the high pressure alarm. Since the pressure alarm set point had been established with the expectation that the methomyl concentration would be much lower, and rate or pressure rise much slower, there was insufficient response time available to the operator and inadequate mechanical relief capacity.

If the chart given in Figure 11 had been available to an alarm rationalization team, they might have determined that absolute temperature or rate of temperature rise was a better indication of potential decomposition reaction and could have established a new alarm more indicative of the situation. The set point for the new temperature could be determined based on the process safety time (time from alarm set point to consequence threshold), operator response time (time for operator to detect, diagnose and respond), and process dynamics (time for process to respond to the operator action).

[7] Reference [11], Figure 11, pg. 39.

Design

Operators can possess an awareness about the operation, be highly knowledgeable about the process, and be committed to doing the right thing all the time, but a poorly designed alarm system is an enabling condition for several failure mechanisms. The incidents above illustrate what can happen if an operator is de-sensitized by nuisance alarms, has insufficient time and guidance to diagnose a problem and respond properly, or when the alarm is not the best indicator of process dynamics. This section discusses some alarm design issues that may undermined OD.

The Silent Alarm

The INDSPEC Chemical Corporation oleum release [12] demonstrates the consequences of a missed alarm. The incident occurred in an oleum storage building normally staffed 73 weekdays and as necessary on weekends. The building contained three pressure vessels used for railcar unloading, and two process tanks that fed the continuous resorcinol process in another building.

On Saturday, October 11, 2008, an operator was called into the facility to perform a periodic but routine weekend operation to prepare soda ash for the process. While on site, the operator would also transfer oleum from three railcar unloading pressure vessels to the two continuous use process tanks to ensure that the pressure vessels are empty, or nearly empty, on Monday mornings.

The three pressure vessel discharge pumps were powered by plugging individual power cords into the “Normal” or “Emergency” power supply receptacles. The process tanks were equipped with alarms that displayed locally and in the oleum storage DCS for high level (audible and amber visual indication) and high-high level (audible and red visual indication). The high-high alarm was also interlocked to shut down the transfer pump for the “Normal” power supply but not the “Emergency” power supply. During weekend operations, the operator would utilize both power supplies to speed the transfer of oleum, and would shut down operations and leave the site when tasks were complete.

On the day of the event, the operator performed operations as usual, shut down the pump connected to the “Normal” power supply, and left the facility. The operator failed to shut down the pump connected to the “Emergency” power supply, so oleum continued to transfer from the pressure vessel to the process tank. High level alarm in the process tank triggered after the operator had left the process area; however it only sounded in the oleum storage building and unoccupied control room. The alarms were not routed to the control room occupied 24/7; therefore, they went unnoticed by personnel remaining on site. The High-high alarm was not connected to emergency power supply, so transfer continued. About two hours after the initial alarm, an employee noticed a white mist escaping the oleum storage building and an emergency was declared, triggering an evacuation or shelter-in-place affecting 2500 residents of Petrolia, Bruin, and Fairview Pennsylvania. Fortunately, there were no fatalities and only one responder suffered a minor injury. INDSPEC faced over $120,000 in OSHA violations and unreported damages.

In this example, the alarm system was ineffective because it sounded in an unoccupied space and there was no operator present to detect the alarm, thus no corrective action taken. A rationalization review of the high level alarm might have detected this design flaw and resolved by relaying an alarm to the continuously staffed control room. The high-high level alarm was designed to interlock with the normal power and shut down the pump, but there was no similar interlock for the emergency power. The situation was known to operators, but since the unwritten work practice had been used for more than

25 years, it was not recognized as being a failure in operational discipline. PHAs conducted on the system failed to identify the potential hazards. The alarm rationalization process focuses specifically on identifying and documenting the cause, consequence and corrective action related to a single alarm. This level of detail often identifies potential gaps the PHA may have overlooked, and existing flaws in operational discipline.

Alarm Overload

ISA 18.2 [5] recommends an alarm annunciation rate of 1-2 alarms per operator per 10 minutes. This is based on providing sufficient time for the operator to detect the alarm, diagnose the problem (retrieve relevant data from the control system, analyze the situation) and respond (perform corrective action(s)). The standard recommends that the average daily rate does not exceed 150-300 alarms in order to be manageable. Undocumented reports suggest that industry groups experience 900-2000 alarms per day or 5-8 alarms per 10 minute interval. In *exida*'s experience, more than 1000 a day is common, particularly for systems that have not undergone rationalization. The alarm overload inhibits the operator's availability to address any one alarm, and increases the probability that an important alarm will be missed. The following paragraphs discuss a few types of nuisance alarms that may be addressed with alarm design techinques.

Stale Alarm

A stale alarm is one that remains in the alarm state for an extended period of time. They can distract the operator by cluttering the alarm summary screen and may interfere with identification of new alarms. The DuPont Belle rupture disk burst indicator alarm is one example of a stale alarm. OD broke down when the operators became so accustomed to false alarms that they silenced the alarm but allowed it to remain active for an extended period of time. Another example is an alarm that indicates a sump pump has stopped after pumping out the sump (a normal operation). Operators may grow tired of the recurrent annunciation and allow it to become stale to stop the repeated cycling. The rationalization process will help determine if the indication should even be an alarm or whether it belongs in one of the other categories. If it is determined to be an alarm, the analysis will identify opportunities to make the alarm more relevant.

Chattering and Fleeting Alarms

Chattering and fleeting alarms can be annoying and difficult to diagnose. A chattering alarm will repeatedly transition between alarm and normal states often without operator interaction to clear. Fleeting alarms transition between the alarm and normal state, but do not immediately repeat. This type of alarm distracts an operator like flies at a picnic. The alarms seem to appear and clear at random. Operators spend time chasing an elusive cause, grow frustrated, and eventually fail to respond to the alarm at all. These alarms are easily identified by analyzing data from the historian, specifically alarm frequency and duration. Many of these can be addressed by analyzing the deadband (hysteresis), filters and on/off delays as part of the rationalization review.

Redundant Alarms

Redundant, or cascading, alarms are those that consistently occur within a short period of time of other alarms. They are generally associated with the same event. For example, when a pump is stopped, there may be an alarms from the motor run indication, low pressure at the pump discharge, and low flow from the downstream flow meter. This type of alarm can compromise operational discipline by

presenting an alarm (low pump discharge pressure) which may or may not be relevant and which relies on the operator to assess its validity in real time.

Redundant alarms may be addressed by using advanced alarming techniques such as conditional or designed suppression. Conditional suppression will prevent certain alarms from alarming when a specified normal condition is present. For the pump example above, low flow and low pressure alarms would be suppressed when the pump is in a STOP status. Suppression by design would be used to automatically suppress the consequential alarms associated with a planned event, such as equipment shut down (preventing stale alarms) or an unplanned event such as a compressor trip (preventing an alarm flood). To prevent an alarm flood from resulting after a compressor trip, the alarms (temperature, flow, pressure, vibration etc.) associated with the trip are included in a flood group to be suppressed, with latching enabled to identify first out, and a common trouble alarm indicating there was a trip. Advanced alarm techniques can be used to safely reduce the number of alarms sent to the operator so they are able to more quickly identify and diagnose a situation.

References

1. B. Rains, Operational Discipline: Does Your Organization Do the Job Right Every Time?, DuPont 2010.
2. J.A. Klein, and B.K.Vaughen, Implementing an Operational Discipline Program to Improve Plant Process Safety, Chemical Engineering Progress, pp. 48-52 June 2011.
3. D.G. Dunn, N.P. Sands, and T. Stauffer, When Good Alarms go Bad: Learning from Incidents, 70th Annual Instrumentation and Automation Symposium – Texas A&M University, January 2015.
4. T. Stauffer, P.E. and K. VanCamp, Making Some Alarming Moves, Chemical Processing, http://www.chemicalprocessing.com/articles/2012/make-some-alarmingmoves/, April 2012.
5. ANSI/ISA–18.2–2009. Management of Alarm Systems for the Process Industries. June 2009.
6. T. Stauffer, P.E., Implement an Effective Alarm Management Program, Chemical Engineering Progress, pp. 19-27, July 2012.
7. U.S. Chemical Safety and Hazard Investigation Board, http://www.csb.gov/, Investigation Report: E.I. DuPont DE Nemours & Co., Inc. Methyl Chloride Release, Oleum Release and Phosgene Release. Report No. 2010-6-I-WV, September 2011
8. The Bureau of Ocean Energy Management, Regulation and Enforcement, US Department of the Interior, Investigation Report Regarding the Causes of the April 20, 2010 Macondo Well Blowout. September 14, 2011
9. U.S. Chemical Safety and Hazard Investigation Board, http://www.csb.gov/, Investigation Report Volume 1: Explosion and Fire at the Macondo Well. Report No. 2010-10-I-OS, June 5, 2014
10. Testimony of Mike Williams, Joint Investigation Hearing, July 23, 2010, at 34-35, C-Span, http://www.c-span.org/video/?294728-1/investigation-deepwater-horizonexplosion-mike-williams, Accessed February 9, 2016.
11. U.S. Chemical Safety and Hazard Investigation Board, http://www.csb.gov/, Investigation Report: Pesticide Chemical Runaway Reaction Pressure Vessel Explosion. Report No. 2008-08-I-WV, January 2011
12. U.S. Chemical Safety and Hazard Investigation Board, http://www.csb.gov/, Case Study: Uncontrolled Oleum Release, Petrolia, Pennsylvania. 2009-01-I-PA. September 2009

Revision History

Authors: Denise Chastain-Knight, Todd Stauffer

Prepared for Presentation at American Institue of Chemical Engineers
2016 Spring Meeting and 12th Global Congress on Process Safety
Houston, TX

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