When Good Alarms Go Bad:
Learning from Incidents

White Paper

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

January 2015

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

Abstract

Some of the significant process industries incidents occurred by overflowing vessels, including BP Texas City and Buncefield. In many overflow incidents, alarms were designed to signal the need for operator intervention. These alarms may have been identified as safeguards or layers of protection, but they did not succeed in preventing the incident. This paper reviews several overflow incidents to consider the mechanical integrity and human factors elements of the failures.

Conclusion

Alarms are often cited as safeguards or independent protection layers to prevent hazardous events, yet incidents continue to occur where the alarm did not prompt action to prevent the consequence. The investigation of these incidents focuses on the root causes, but there is an opportunity to also examine the contributing factors that allowed the protection layers to fail. A set of failure mechanisms for alarms can map the failure to the activities of the alarm management lifecycle and the operator feedback model from ANSI/ISA-18.2 [1]. Many of the failures can be related to human factors failure mechanisms, or situational awareness demons. A set of similar overflow incidents are analyzed using this methodology to develop recommendations.

Introduction

The most famous incident in the field of alarm management is the Milford Haven incident at the Texaco refinery in Pembroke South Wales in July of 1994. 20 tonnes of hydrocarbons were released from the knock-out pot on the flare header resulting in a massive explosion. Hundreds of alarms inundated the operators in the last minutes before the release. The Health Safety Executive's investigation report [2] identified the concern that alarms on the distributed control systems (DCS) can overwhelm the operator, and instead of improving safety, can have the opposite effect and contribute to the event.

While alarms are used to provide an indication to the operator that their action is required to prevent an undesired consequence, too many alarms or other failures in the alarm system, can keep the operator from responding correctly to the alarm. Bransby and Jenkinson [3] describes a fictional tale of a typical operator reacting to a sequence of events within a typical process facility and 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.”[3]

The paper is divided into three sections. The first section provides background information on the concepts that are referenced in the incident analysis. The second section provides an overview of selected tank level incidents along with an analysis of failure modes. The third section summarizes the conclusion and lessons learned.

Background

What is an Alarm?

The purpose of an alarm is to notify the operator of an equipment malfunction, process deviation or abnormal condition that requires a timely response [1]. Alarms help the operator keep the process within normal operating conditions. Alarms also play a significant role in maintaining plant safety, providing a means of risk reduction (layer of protection) to prevent the occurrence of harm from an escalating process hazard as shown in Figure 1 [4]. 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" [5].

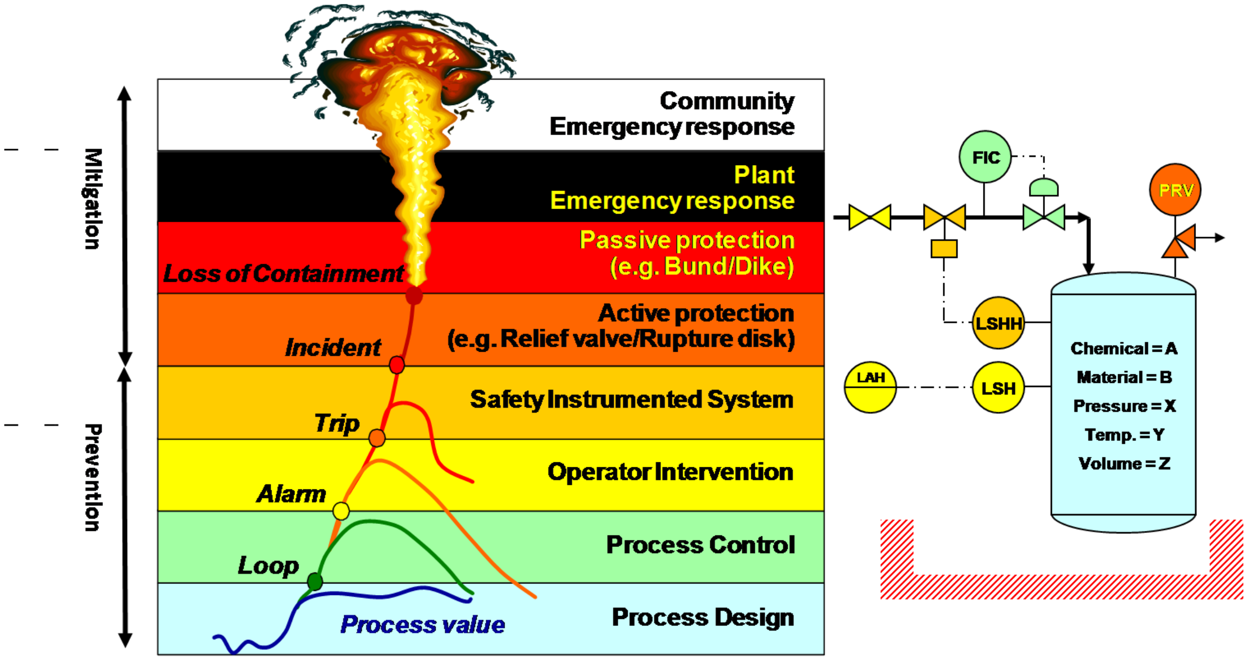

Figure 1. Layers of Protection and Their Impact on the Process [4]

Unlike other safeguards or layers of protection, such as a relief valve or safety instrumented system (SIS), the operator's response to an alarm is not an automatic action but instead is a manual action which is subject to human error. Thus the potential failure modes for operator response to alarm include hardware, software, and human behavior.

Using Alarms to Reduce Risk

To evaluate an alarm's effectiveness at preventing hazardous events, it is important to consider the behavior of the alarm system as a whole in addition to the individual alarm. If the design and management of the alarm system or its actual performance are not satisfactory, then the operator's dependability will be compromised. This is particularly critical during abnormal situations such as might accompany a tank high level event. If operators are flooded with alarms during the upset, or nuisance alarms are already present, then they might miss a critical high level alarm, respond incorrectly, or not in time. Thus alarm system design and performance can have a significant impact on the probability that an operator will take the correct action. Campbell Brown provides a good overview of this probability and specifically termed it “the consequences of failure to act” [6].

Alarm Management Lifecycle

The standard ANSI/ISA-18.2, “Management of Alarm Systems for the Process Industries” (ISA-18.2) provides guidance that can help users design, implement and maintain an alarm system in order to optimize performance for an operator response to alarm [1]. Alarm management activities are structured to follow a lifecycle approach wherein the key activities are executed in the different stages of the lifecycle [1][7][8]. The products of each stage are the inputs for the activities of the next stage. For the purposes of this paper, the activities of Rationalization, Detailed Design, Operation, and Maintenance will be highlighted

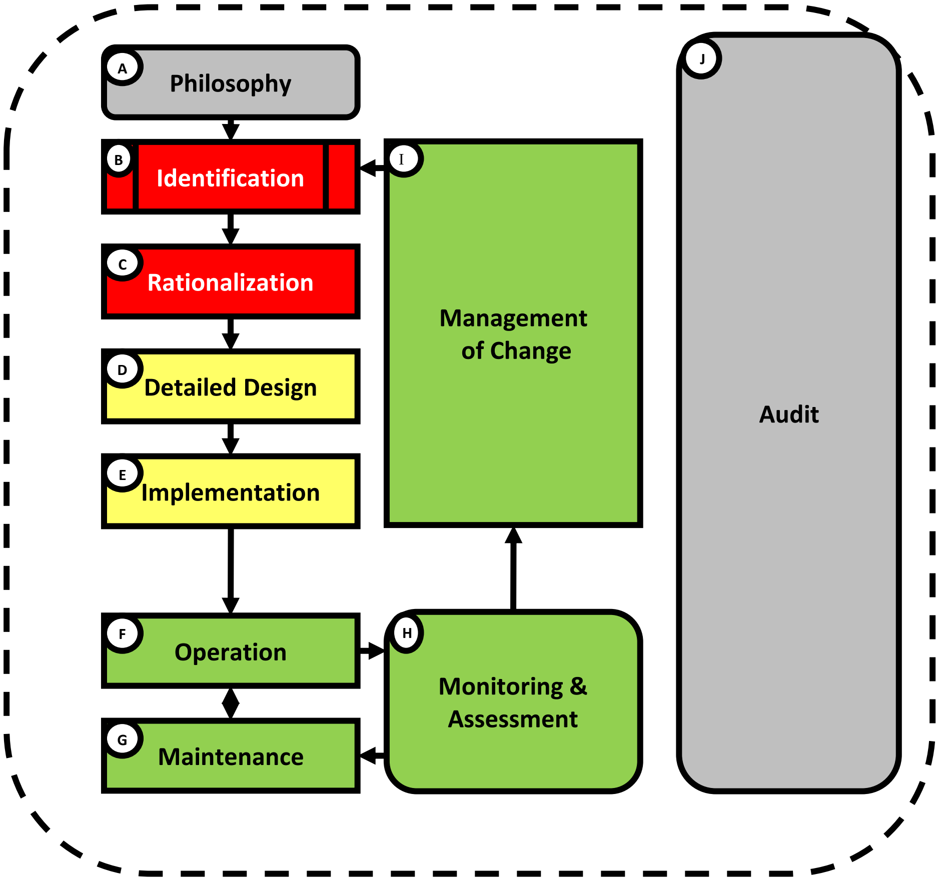

Figure 2. Alarm Management Lifecycle [1][7][8]

Failure Mechanisms

There are many ways to identify failure mechanism for alarms. The approach taken in this review is to use the lifecycle to group failure mechanisms and to further focus on the situation awareness factors that contribute to operator diagnosis errors. Figure 3 is a classic fishbone diagram for the failure mechanisms in this review. The lower half shows failure mechanisms related to the rationalization, detail design, and maintenance stages of the lifecycle. The top half of the fishbone shows failures mechanisms related to the operator response in the operation stage of the lifecycle. The fishbone does not show all failure mechanisms, but includes those related to the incidents in this review.

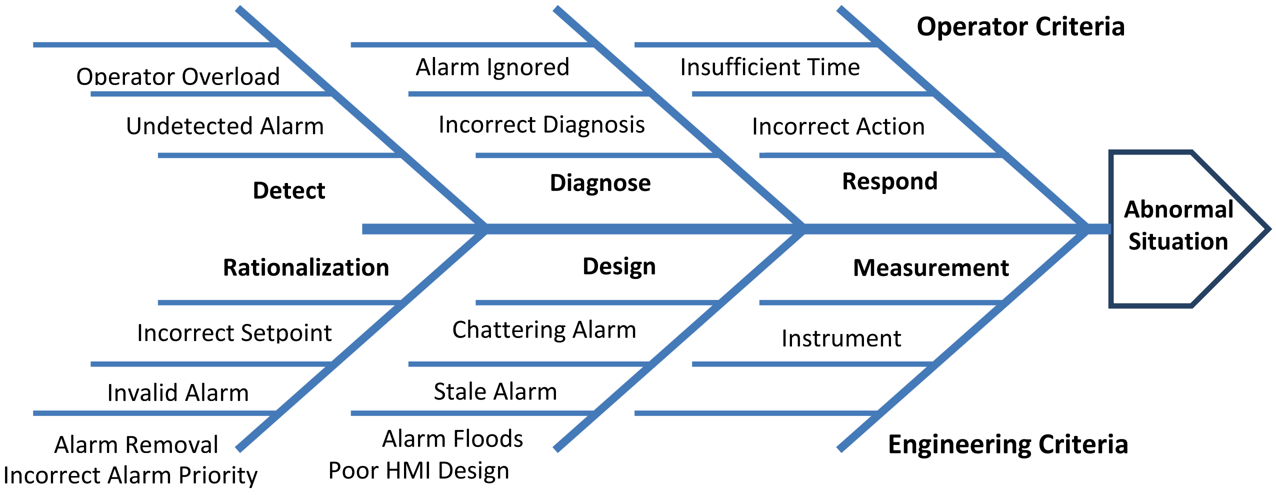

Figure 3. Failure Mechanisms (Fishbone)

Alarm Rationalization

Alarm Rationalization involves reviewing and justifying potential alarms to ensure that they meet the criteria for being an alarm as defined in the alarm philosophy document. It includes defining the attributes of each alarm (such as limit, priority, classification, and type) as well as documenting the cause, consequence, allowable response time and operator action (response). The rationalization process is performed by a multifunctional team which typically includes the process engineer, controls engineer, lead operator(s), and safety / risk management engineer (as required). The rationalization process is guided by an alarm philosophy document. 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.”[9] 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 and IEC62682. Finally, 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.”[10]

Failure mechanisms associated with alarm rationalization include:

- Invalid Alarm – the alarm does not meet the definition of alarm, and should have been eliminated through rationalization
- Incorrect Setpoint – the alarm setpoint was not correctly determined and is too close to the normal operating range or does not allow enough time for operator response
- Incorrect Alarm Priority – the alarm priority does not correctly correspond to the urgency of the operator response
- Incorrect Alarm Removal – alarm rationalization incorrectly removed needed alarms

Detailed Design

There are three components of detailed alarm design; basic alarm design, advanced alarm design, and HMI (Human Machine Interface) design.

- Basic alarm design includes setting alarm attributes like deadband and time delays to prevent an alarm with the right setpoint from becoming a chattering or fleeting alarm.
- Advanced alarm design includes suppressing the alarm based on plant or equipment states, preventing an alarm from becoming a stale alarm, or other type of nuisance alarm.
- HMI design includes making the alarm indication salient to the operator and communicating the alarm priority.

Reising and Montgomery found that their “study results indicate that more sophisticated alarm handling techniques (Campbell Brown, 2002), such as dynamic alarming and/or alarm suppression, will have to be applied for alarm flood situations.”[10] While good basic alarm design is fundamental to alarm management, it may only get you part of the way, advanced alarm handling techniques such as alarm filtering or dynamic alarming (O’Hara et. al. [11]) will need to be utilized, thus allowing the operator to achieve the goal of assessing the alarm and responding appropriately [12].

Failures mechanisms associated with detailed design include:

- Chattering Alarm - alarm deadbands or delays not correctly selected
- Stale Alarm - alarm does not return to normal when process conditions are normal
- Alarm Floods – the alarm rate is greater than the operator can effectively manage
- Poor Alarm HMI Design – the alarms are not clearly indicated in the HMI

Alarm Maintenance

The maintenance stage of the alarm lifecycle includes activities for testing and repair of instruments and alarms as well as the returning alarms to service. It is important to note that the state of out-of-service is not a function of the process equipment, but describes an administrative process of suppressing (bypassing) an alarm using a permit system. One of the main purposes of maintenance is to verify the integrity of the alarm to ensure that it will activate when needed.

The failure mechanisms in maintenance include:

- Instrument Failure – the instrument has ceased to perform its intended function and the data being conveyed is erroneous
- Annunciator failure – the alarm system component that provides the audible or visual alarm indication fails to operate
- Suppressed alarm – the alarm does not annunciate due to suppression

Operation

In the operation stage of the lifecycle, the alarm performs its function and the opertor responds to the alarm. To analyze the failures in the operator response to an alarm it is helpful to define a model for evaluation. For this study the operator response model is defined to consist of the following three components:

- **Detect** – the operator becomes aware of the deviation from the desired condition

- **Diagnose** – the operator uses knowledge and skills to interpret the information, diagnose the situation and determine the corrective action to take in response

- **Respond** –the operator starts and completes corrective action in response to the deviation

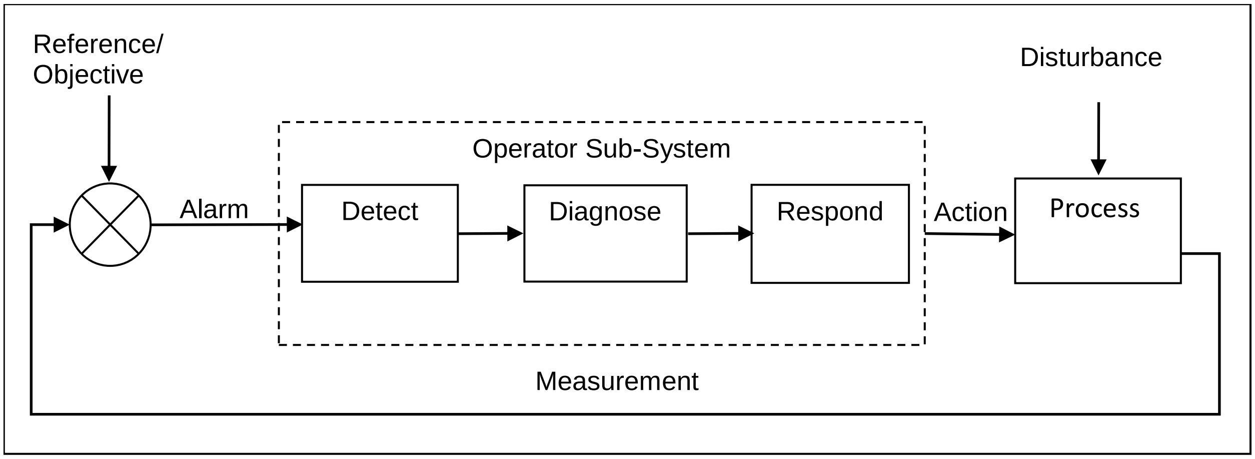

Figure 4. Feedback Model of Operator Process Interaction [1]

The failure mechanisms within the operator response model are the subcomponents of the operator sub-system “Detect”, “Diagnose” and “Respond”.

The failure mechanisms in the “Detect” component of operator response include:

- Undetected Alarm - the alarm is annunciated but the operator does not notice the alarm
    - Stale alarms can indicate an alarm condition existed previously
    - Alarm floods can hide an alarm in a large number of alarms
    - Poor alarm HMI design may make alarm annunciation difficult to detect

The failure mechanisms in the “Diagnose” component of operator response include:

- Alarm ignored – the operator receives the alarm indication and fails to take any action.
    - Chattering alarms can cause an alarm to be ignored because of frequent annunciation
    - Stale alarms can cause an alarm to be ignores because it is accepted as normal
- Insufficient training – the operator does not have enough knowledge to take the corrective action.
- Incorrect Diagnosis – the operator does not have sufficient knowledge but fails to identify the corrective action.

The failure mechanisms in the “Respond” component of operator response include:

- Incorrect Action – the operator determines the correct response but fails to take the correct action
- No Action – the operator determines the correct response but fails to take the corrective action.

Situation Awareness

The concept of Situation Awareness will be applied to help evaluate and categorize failures in the operator criteria of the fishbone. Situation Awareness (SA), which comes from the study of human factors and is more widely known in the airline industry, can be defined as "being aware of what is happening around you and understanding what that information means to you now and in the future."[13] As such, SA drives effective decision making and performance.

As a framework for categorizing SA failures, eight (8) factors have been identified which undermine effective situation awareness. These factors, called SA Demons [13], are described below in terms related to alarm management:

- **Attentional Tunneling** – Focusing on one area or issue to the extent that alarms from another area or issue are excluded.
- **Requisite Memory Trap** – Over dependence on operator memory for effective response to alarms, perhaps under different operating conditions.
- **Workload, Anxiety, Fatigue, and Other Stressors** – (WAFOS) physical or psychological stress that can impact performance
- **Data Overload** – Over dependence on the operator to make sense of excessive amounts of alarm information.
- **Misplaced Salience** – Incorrect alarm priority or HMI representation of alarm importance and other status information
- **Complexity Creep** – complex response or complex HMI features that increase response complexity
- **Errant Mental Models** – Thought process that incorrectly interprets alarms or mistakenly discounts relevant alarms
- **Out-of-the-Loop** Syndrome – Process or response automation that causes the operator to not know what to do when automation fails

The SA demons are not mutually exclusive from the failure mechanisms identified in the fishbone, but additive. Primarily the SA demons provide a method to further analyze operator diagnosis failures.

Incident Analysis

Milford Haven [2]:

A lightning strike started a fire in the crude distillation unit of the refinery. Control operators on duty were charged with calling out the fire brigade, executing an emergency shutdown of the crude unit and maintaining operation in the FCCU (deethanizer, debutanizer, naptha splitter). The upset caused a loss of hydrocarbon flow to the deethanizer, which feeds the debutanizer. The system was designed to prevent total loss of liquid in these two vessels; consequently, the falling levels caused the discharge valves in the deethanizer and debutanizer to close.

The operators were able to successfully restore flow to the deethanizer, which renewed the flow to the debutanizer. The debutanizer discharge valve however, remained closed even though it showed open in the control system. This caused the debutanizer to become liquid logged resulting in venting via a pressure relief valve to a KO drum and flare. Extended venting caused the KO drum to be filled with liquid beyond its design capacity leading to a rupture of a discharge line and subsequent explosion.

The facts related to the alarm system failures can be stated as follows:

- There were an increased number of activities per operator due to the lightning strike and resulting fire.
- The debutanizer discharge valve remained closed even though it indicated open in the control system.
- The operator situation awareness was limited due to HMI configuration (no process overview)
- The operator did not respond to the flare KO drum high level alarm.
- The operators were not adequately trained for the abnormal situation.

The failures can be mapped to the following failure mechanisms:

- Detect Failure
  - Operators did not respond to the flare KO drum high level alarm.
    - Alarm Floods – Operator was flooded with 275 alarms in 11 minutes.
- Diagnose Failure
  - Operator failed to recognize that the discharge valve indication was incorrect.
    - Incorrect Diagnosis - Operator did not correctly diagnose the situation. *Note – This failure is not a failure of operator diagnosis of an alarm and is not included in the tabulation.*
  - Operators were not provided with adequate training.
    - Insufficient Training - Operators were not provided with training for abnormal situations.
- Design Failure
  - Operator situation awareness was limited due to no process overview.
    - Poor HMI Design – HMI Design did not allow visualization of the overall process. *Note – This failure is not a failure of operator diagnosis of an alarm and is not included in the tabulation.*

The failures can be mapped to the following SA conditions:

- Errant Mental Models
  - Operator did not connect that there was no flow going from the debutanizer to the naptha splitter.
- Workload, Anxiety, Fatigue and Other Stressors
  - Operators were charged with performing multiple stressful tasks at the same time.
- Data Overload
  - Operators failed to respond to the flare KO drum high level alarm.
    - Operators were subjected to an alarm flood.

BP Texas City [14]:

At the BP Texas City refinery, a series of failures led to explosions during the startup of a hydrocarbon isomerization unit after a month-long turnaround. The explosions occurred when a distillation tower was overfilled with hydrocarbons and was overpressurized leading to overfilling of a blowdown drum and stack, causing a geyser-like release from the vent stack. Explosions and fires killed 15 people and injured another 180, alarmed the community, and resulted in financial losses exceeding $1.5 billion.

The facts related to the alarm system failures can be stated as follows:

- The distillation tower level instrumentation provided false indication that the tower level was declining when it was actually overfilling.
- The distillation tower redundant high level alarm did not activate.
- The control board display did not provide adequate information on the imbalance of flows in and out of the tower to alert the operators to the dangerously high level.
- Operators were not provided adequate training on how to handle abnormal situations, including infrequent and high hazard operations such as startups and unit upsets.
- The process unit was started despite previously reported malfunctions of the tower level indicator, level sight glass, and a pressure control valve.

The failures can be mapped to the following failure mechanisms:

- Measurement Failure
  - The distillation tower redundant high level alarm did not activate.
    - Instrument Failure - Alarm failed to activate when high level was reached.
- Diagnose Failure
  - Level instrumentation provided false indication that the tower level was declining.
    - Incorrect Diagnosis - Operator did not connect the false level indication.
  - Operators were not provided adequate training on abnormal situations.
    - Insufficient Training - Operators did not recognize the situation.
- Detect Failure
  - The distillation tower redundant high level alarm did not activate.
    - Instrument Failure - Alarm failed to activate when high level was reached.
    - Poor HMI Design – HMI Design did not allow operator to recognize the alarm.
- Design Failure
  - HMI design was not adequate to provide relevant process information.
    - Poor HMI Design – HMI Design did not support operator in recognizing abnormal situation.

The failures can be mapped to the following SA conditions:

- Errant Mental Models
  - Operator did not connect that the level instrumentation was providing false indication.
  - HMI did not provide adequate information on the imbalance of flows.
  - Operators were not provided adequate training on abnormal situations.

Buncefield [15]:

At the Buncefield Oil Depot, a failure of a tank level sensor prevented its associated high level alarm from being annunciated to the operator. As the level in the tank reached its 'ultimate' high level, a second protection layer, an independent safety switch, failed to trigger an alarm to notify the operator and failed to initiate a trip which would have automatically shut off the incoming flow. The tank overflow and ensuing fire resulted in a £1 billion (1.6 billion USD) loss.

The facts related to the alarm system failures can be stated as follows:

- Tank level gauge failed showing 2/3 full and the associated high level alarm failed to go off.
- Ultimate high level switch failed to annunciate and failed to activate the automatic shutdown.
- HMI Design did not allow operator to detect that the level gauge had failed or that the tank had completed its filling operation.

The failures can be mapped to the following failure mechanisms:

- Measurement Failure
  - Tank level gauge failed showing 2/3 full and the associated high level alarm failed.
    - Instrument Failure – The high level alarm failed to activate.
  - Ultimate high level switch failed to annunciate and failed to activate the automatic shutdown.
    - Instrument Failure - The high-high level alarm failed to activate.
- Detect Failure
  - Tank level gauge failed showing 2/3 full and the associated high level alarm failed to go off.
    - Instrument Failure - Alarm failed to activate when high level was reached.
    - Poor HMI Design – HMI Design did not allow operator to recognize high level.
- Design Failure
  - Tank level gauge failed showing 2/3 full and the associated high level alarm failed to go off.
    - Poor HMI Design – HMI Design did not allow operator in recognizing a high level situation.

The failures can be mapped to the following SA conditions:

- None – It should be noted that while not a failure of operator diagnosis of an alarm, there was an Errant Mental Model formed by the operators as they did not connect that there was abnormal situations present even though there were no alarms.

Tank 1 Refining & Chemical Company:

A leak occurs from a reagent transfer pump seal in a small diked area. The diked area sump filled triggering the high alarm and the high-high alarm. The reduced reagent flow caused an upset in the neutralization unit. The operator focused on the neutralization upset and did not respond to the sump alarms. Approximately 10,000 gallons of material was spilled.

The sump high level alarm was also used to start the sump pump and the sump low level alarm was used to stop the sump pump.

The investigation concluded that the sump high level alarm had become a nuisance alarm.

The facts related to the alarm system failures can be stated as follows:

- The operator was focused on alarms and the upset in the neutralization area.
- The operator did not respond to the sump high level or high-high level alarm.
- The sump high level alarm was a frequent nuisance alarm that did not require a response from the operator.

The failures can be mapped to the following failure mechanisms:

- Diagnose Failure
  - Operator did not respond to the sump high-high level alarm
    - Operator was focused on the upset in the neutralization area.
    - Operator did not connect the upset in neutralization with a loss of reagent caused by seal leak on the transfer pump and filling the tank sump.
    - Operator did not consider sump level alarms required response based on experience.
- Rationalization Failure
  - Sump high level alarm did not require a response and was not an abnormal condition (it was part of the automation of the sump pump).

The failures can be mapped to the following SA conditions:

- Attention Tunneling
  - Operator was focused on the upset in the neutralization area.
- Errant Mental Model
  - Operator did not connect the upset in neutralization with a loss of reagent caused by seal leak on the transfer pump and filling the tank sump.

Tank 2 Refining & Chemical Company:

A leak occurs from an open manway on an out-of-service tank in a diked area due to misvalving. The diked area primary sump fills, and the sump pump is overwhelmed with the flow, triggering the high level alarm. The primary sump overflows, and the secondary sump fills, and the sump pump are overwhelmed with the flow, triggering the high level alarm. The operator detects the alarms, but knows the tank is out-of service. Eventually a field operator investigates and identifies the loss of containment. The release is eventually contained after over 100,000 gallons of material was spilled.

The sump high level alarm was also used to start the sump pump and the sump low level alarm was used to stop the sump pump.

The investigation concluded that the sump high level alarm had become a nuisance alarm.

The facts related to the alarm system failures can be stated as follows:

- The operator did not respond to the sump high level alarm.

- The operator did not respond to the initial alarms because the equipment was out of service.
- The sump high level alarm was a frequent alarm and did not require a response from the operator.

The failures can be mapped to the following failure mechanisms:

- Diagnose Failure
    - Operator did not respond to the sump high-high level alarm
        - Operator did not think the sump alarm was important because it was associated with an out-of –service system.
        - Operator did not consider sump level alarms a required response based on experience.
- Rationalization Failure
    - Sump high level alarm did not require a response.

The failures can be mapped to the following SA conditions:

- Errant Mental Model
    - Operator did not think the alarms on out-of-service equipment required a response.

Tank 3 Refining & Chemical Company:

An automated drain valve on an equipment set fails to close which generates an alarm and halts the automation sequence. The operator advances the automation sequence and starts feed to the equipment, which drains through the open valve to a diked area. The diked area fills triggering a high level alarm, and overflows to tertiary containment dike. The tertiary containment area fills triggering the high level alarm. Eventually a field operator investigates and identifies the loss of containment. The release is eventually contained after over 100,000 gallons of material was spilled.

There were very few alarms at the time of the incident. The valve malfunction alarm and the containment area level alarms were not nuisance alarms.

The facts related to the alarm system failures can be stated as follows:

- The operator did not respond correctly to the valve malfunction alarm.
- The operator did not respond to the high level alarms in the containment areas.
- The sump valve malfunction alarm and the containment level alarms were not nuisance alarms.

The failures can be mapped to the following failure mechanisms:

- Diagnose Failure
    - Operator did not respond correctly to the valve malfunction alarm.
        - Operator action was to over-ride the automation sequence leading to the loss of containment.
    - Operator did not respond to the containment area high level alarms.

The failures can be mapped to the following SA conditions:

- Out-of-the-loop-syndrome
    - Operator did not understand the automation sequence of the equipment.

- Errant Mental Model
    - Operator did not connect the alarms in the containment area with the alarm on the drain valve.

Tank 4 Refining & Chemical Company:

During a plant start-up, there were operating issues on an equipment set. The upset caused a tank to overflow to a secondary containment area. The containment area high level alarm triggered. The secondary containment area overflowed to a tertiary containment area. The high level alarm triggered in the tertiary containment area. Eventually a field operator investigates and identifies the loss of containment. The release is eventually contained after over 10,000 gallons of material was spilled.

There start-up and upset conditions caused a flood of alarms that lasted through the event.

The containment area level alarms were not nuisance alarms.

The facts related to the alarm system failures can be stated as follows:

- The operator was focused on the start-up of the plant.
- The operator was flooded with alarms (>10 alarm per 10 min)
- The operator did not respond to the high level alarms in the containment areas.
- The containment level alarms were not nuisance alarms.

The failures can be mapped to the following failure mechanisms:

- Diagnose Failure
    - Operator did not respond to the containment high level alarms
        - Operator was focused on the plant start-up.

The failures can be mapped to the following SA conditions:

- Data Overload
    - The operator was flooded with alarms.
- Attention Tunneling
    - Operator was focused on the plant start-up.

Tank 5 Refining & Chemical Company:

During a batch production campaign, piping was modified for product to be delivered to a designated tank, but the piping delivered the product to a different tank. After several days of production, the high level alarm on the second tank triggered. The next day, the high high level alarm on the second tank triggered. Production continued until material overflowed the second tank. Eventually a field operator investigated and identified the loss of containment. The release is eventually contained after over 1,000 gallons of material was spilled.

The tank level alarms were not nuisance alarms.

The facts related to the alarm system failures can be stated as follows:

- The operator considered the second tank out-of-service.

- The operator did not respond to the high level alarms on the second tank.
- The second tank level alarms were not nuisance alarms.

The failures can be mapped to the following failure mechanisms:

- Diagnose Failure
    - Operator did not respond to the second tank high level alarms.
        - Operator considered the second tank out of service.

The failures can be mapped to the following SA conditions:

- Errant Mental Model
    - Operator considered the second tank out of service.

Tank 6 Refining & Chemical Company:

During normal plant operations following a DCS conversion with alarm rationalization, an incident occurred where a tank was overflowed to a secondary containment area. Eventually a field operator during normal rounds identifies the loss of containment and contacted plant operations to shutdown flow into the tank. The release is eventually contained after over 1,000 barrels of material with an OSHA permissible exposure limit (PEL) of 1 ppm for an 8 hour time weighted average (TWA).

The DCS conversion had migrated from a legacy control system with light boxes for alarms where all of the alarms were concentrated in one system. During the rationalization the high-high alarms were eliminated. Previously, normal operating procedure was to fill the tanks past the high alarm and shutoff flow once the tank reached the high-high alarm.

The facts related to the alarm system failures can be stated as follows:

- There were an increased number of alarms to each operator due to the consolidation and conversion of the control systems.
- The operator did not respond (action not taken) to the high level alarms per past operating procedures.
- The operator did not diagnose (insufficient training) the tank high level to prevent the overflow.
- The DCS conversion project did not perform appropriate alarm rationalization (high-high alarms removed).

The failures can be mapped to the following failure mechanisms:

- Diagnose Failure
    - Operator did not respond to the high level alarm
        - Operator was not trained in the new mode of operations.

The failures can be mapped to the following SA conditions:

- Data Overload
    - The operator was operating a new control system which centralized all alarms.
- Complexity Creep
    - The operator was used to a control system which included the first level of alarms and the critical alarms were visually displayed externally.

- Errant Mental Models
    - Operator considered the high level alarm the first indication.

Summary

As previously mentioned, alarms are often cited as safeguards or independent protection layers to prevent the consequences from hazardous situations. This review included a set of incidents that involved overfilling a vessel where alarms indicated an abnormal condition and the operator response to the alarm may have prevented or mitigated the consequences of the event. Typically, the investigation focuses on the root causes, but examination of the contributing factors can lead to new insights and recommendations for improvement. The fishbone in figure 3 shows some of the alarm failure mechanisms that are relevant to the analyzed incidents. Consideration of human factors, such as the situation awareness demons, can identify more refined and potentially unique recommendations for improvement that can be deployed proactively.

As shown in Table 1, for the vast majority of the incidents in this review, the operator failed to take corrective action. In the nine incidents that were analyzed in section 2, "Diagnose" and "Errant Mental Models" were identified as FM/SA's 89/78% of the time respectively. In addition, from the analysis we find that of the total number of FM's (18) 44% were again "Diagnose" and of the 14 SA's "Errant Mental Models" constituted 57% of that group.

Table 1. Incident Failure Mechanisms/Situation Awareness Map

	Failure Mechanisms (FM)								Situation Awareness (SA)								
Incident	Rationalization	Design	Measurement	Detect	Diagnose	Respond	FM Totals		Attention Tunneling	Requisite Memory Trap	Workload, Anxiety, Fatigue…	Data Overload	Misplaced Salience	Complexity Creep	Errant Mental Models	Out-of-the-Loop	SA Totals
1				X	X		2				X	X			X		3
2		X	X	X	X		4								X		1
3		X	X	X			3										0
4	X				X		2		X						X		1
5	X				X		2								X		1
6					X		1								X	X	2
7					X		1		X			X					1
8					X		1								X		1
9					X		1					X		X	X		3
	2	2	2	3	8	0	18		2	0	1	3	0	1	7	1	14
% of FM/SA Total	11%	17%	11%	17%	44%	0%			14%	0%	7%	21%	0%	7%	57%	7%	
FM/SA % of Incidents	22%	22%	22%	33%	89%	0%			22%	0%	11%	33%	0%	11%	78%	11%	

Use of alarm response procedures can help operators diagnose and respond to alarms more effectively. The information for an alarm response procedure (cause, consequence, corrective action, time to respond) is typically documented during alarm rationalization. Since the majority of operator failures occurred during diagnosis and not response, this would seem to indicate that an effective alarm response procedure should include information to help the operator diagnose the situation correctly and develop the correct mental model. It should also be crafted to avoid attention tunneling. Typically alarm response procedures focus on defining operator responses rather than helping them confirm their diagnosis.

Using the model of situation awareness demons, the vast majority of the incidents involved an errant mental model of the process where the operator did not connect the indicated abnormal condition with the need for action or disregarded the alarm.

A potential approach to addressing the gap in mental models is training on situation awareness and mental models; training the operator that when an alarm occurs that does not make sense, investigate before disregarding the alarm. Operator training on the alarm system should focus not only on the meaning of individual alarms but on developing a deeper understanding of the process. This would help ensure that correct mental models are created during abnormal situations. Additionally operators should be trained on how to avoid SA demons (such as attention tunneling) when responding to abnormal situations.

References

1. ANSI/ISA ISA18.00.02-2009 "Management of Alarm Systems for the Process Industries".
2. Health & Safety Executive "The explosion and fires at Texaco Refinery, Milford Haven, 24 July 1994", HSE, 1997.
3. Bransby ML and Jenkinson J., The Management of Alarm Systems, HSE Contract Research Report 166/1998 ISBN 07176 15154, First published 1998.
4. Stauffer, T., Sands, N., and Dunn, D., "Get a life(cycle)! Connecting Alarm Management and Safety Instrumented Systems" ISA Safety & Security Symposium April (2010).
5. Campbell Brown, D., "Horses for Courses – A Vision for Alarm Management," IBC Seminar on "Alarm systems," London, June 26-27, 2002.
6. Campbell Brown, D., "Alarm System Performance – One Size Fits All?", Measurement & Control, May 2003.
7. IEC62682-2014 ""Management of Alarm Systems for the Process Industries".
8. Stauffer, T., Sands, N., and Dunn, D., "Alarm Management and ISA-18 – A Journey, Not a Destination" Texas A&M Instrumentation Symposium (2010).
9. *Nimmo, I., "Rescue Your Plant from Alarm Overload," Chemical Processing, January 2005.*
10. Reising, D.V. and Montgomery, T., "Achieving Effective Alarm System Performance: Results of ASM Consortium Benchmarking against the EEMUA Guide for Alarm Systems," 20th.
11. O'Hara, J.M., Brown, W.S., Higgins, & Stubler, W.F., "Human Factors Engineering Guidance for the Review of Advanced Alarm Systems", NUREG/CR-6105, Washington, DC, US Nuclear Regulatory Commission, 1994.
12. Reising, D.V., Downs, J.L. and Bayn, D., "Human Performance Models for Response to Alarm Notifications in the Process Industries: An Industrial Case Study," Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting, 2004, Santa Monica, CA, pp.1189-1193.
13. Mica Endsley, "Designing for Situation Awareness"
14. "BP America Refinery Explosion" U.S. CHEMICAL SAFETY BOARD www.chemsafety.gov/investigations
15. "The Buncefield Investigation" - www.buncefieldinvestigation.gov.uk/reports/index.htm

Revision History

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

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