Alarm Management and ISA-18 – A Journey, Not a Destination

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

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

Abstract

Poor alarm management is one of the leading causes of unplanned downtime, contributing to over $20B in lost production every year, and of major industrial incidents such as the one in Texas City. Developing good alarm management practices is not a discrete activity, but more of a continuous process (i.e., it is more of a journey than a destination). This paper will describe the new ISA-18.2 standard -"Management of Alarm Systems for the Process Industries"[1]. This standard provides a framework and methodology for the successful design, implementation, operation and management of alarm systems and will allow end-users to address one of the fundamental conclusions of Bransby and Jenkinson that "Poor performance costs money in lost production and plant damage and weakens a very important line of defense against hazards to people." [3] Following a lifecycle model will help users systematically address all phases of the journey to good alarm management. This paper will provide an overview of the new standard and the key activities that are contained in each step of the lifecycle.

Conclusion

The new ISA-18.2 standard provides a framework for the successful design, implementation, operation, and management of alarm systems in a process plant. It utilizes a lifecycle approach consisting of distinct stages which are similar in many respects to the lifecycle methodology of the ANSI/ISA-84 Functional Safety Standard. Although the use of lifecycle is common to both standards, alarm management is more of a continuous activity, due to the scale and the processing of all alarms by the operator, requiring ongoing performance evaluation and adjustment. Similar to the functional safety standard, ISA-18.2 is expected to be accepted as "good engineering practice" by insurance companies and regulatory agencies. The lifecycles are analogous, though there are some key differences and at the same time there are also some key differences in terminology.

Introduction

Alarm systems play a critical role in plant operations. A control room operator in a chemical plant or refinery may have responsibility for multiple unit operations with thousands of instruments. The purpose of an alarm is to draw the operator's attention to abnormal conditions requiring action. This was clearly and concisely stated by Campbell Brown "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 minimize, plant upset, asset or environmental damage, and to improve safety" [4]

It takes very little effort to add an alarm in modern control systems. Nimmo provided good insight into the problem of Abnormal Situation Awareness or Management (ASA or ASM) associated with the modern control system when he stated "having good situation awareness means that the operator has an accurate perception of the current condition of the process and equipment, and an accurate understanding of the meaning of various trends in the unit. The most common issue raised by operators and supervisors around the world is the loss of the big picture, when a company evolves to computer control rather than the panel mounted instruments. This complaint is echoed by the findings of the Health and Safety Executive in their report on the explosion and fires at the Texaco Refinery in Milford Haven." [5][6] As a result many alarm systems perform poorly, and can negatively impact an operator's ability to respond to an event. Poor alarm management was identified as a contributing factor in many major process incidents. A new standard, ANSI/ISA-18.02 Management of Alarm Systems for the Process Industries (ISA-18.2), provides

guidance that will help users design, implement, and maintain a well performing alarm system. The recommendations in the standard provide a methodology for preventing and eliminating the most common alarm management problems. Per Reising and Montgomery, “There is no ‘silver bullet’ or ‘one shot wonder’ for good alarm management.” [9]

The ISA-18.2 Lifecycle

The ISA-18.2 standard is organized around the alarm management lifecycle (Figure 1) [1]. The key activities of alarm management are executed in the different stages of the lifecycle. The products of each stage are the inputs for the activities of the next stage. Since many automation professionals are familiar with the safety instrumented systems lifecycle (Figure 2) from ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) Functional Safety: Safety Instrumented Systems for the Process Industry Sector (ISA-84)[2], it may be helpful to compare the two lifecycles to highlight the similarities and differences.

It is important to distinguish a comparison of the lifecycles from the interaction of the lifecycles. Alarms can be a means of risk reduction, and so be a part of the safety instrumented system lifecycle. Most safety instrumented systems generate alarms, which follow the alarm management lifecycle. The interactions between the lifecycles will be explored in another paper.

An important difference between the two lifecycles, and the related standards, is that the safety lifecycle and ISA-84 deals with instrumented functions for safety, where as the alarm management lifecycle and ISA-18.2 addresses all alarms, of which only a fraction are safety related. ISA-18.2 is written in more general terms as a result of this difference.

A second significant difference is that safety instrumented functions are evaluated individually. Each SIF is designed for a specific hazard and its design verified. Each alarm is also evaluated individually, but because all alarms are processed by the operator before the associated action is taken, the alarm system must also be evaluated as a whole. The alarm rate, the priority distribution, and false alarms (analogous to spurious trips) have been shown to 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” [7].

Another difference between the two lifecycles is that a plant will usually have few safety instrumented functions, but may have hundreds or thousands of alarms. The difference in scale drives different methods for assessing performance.

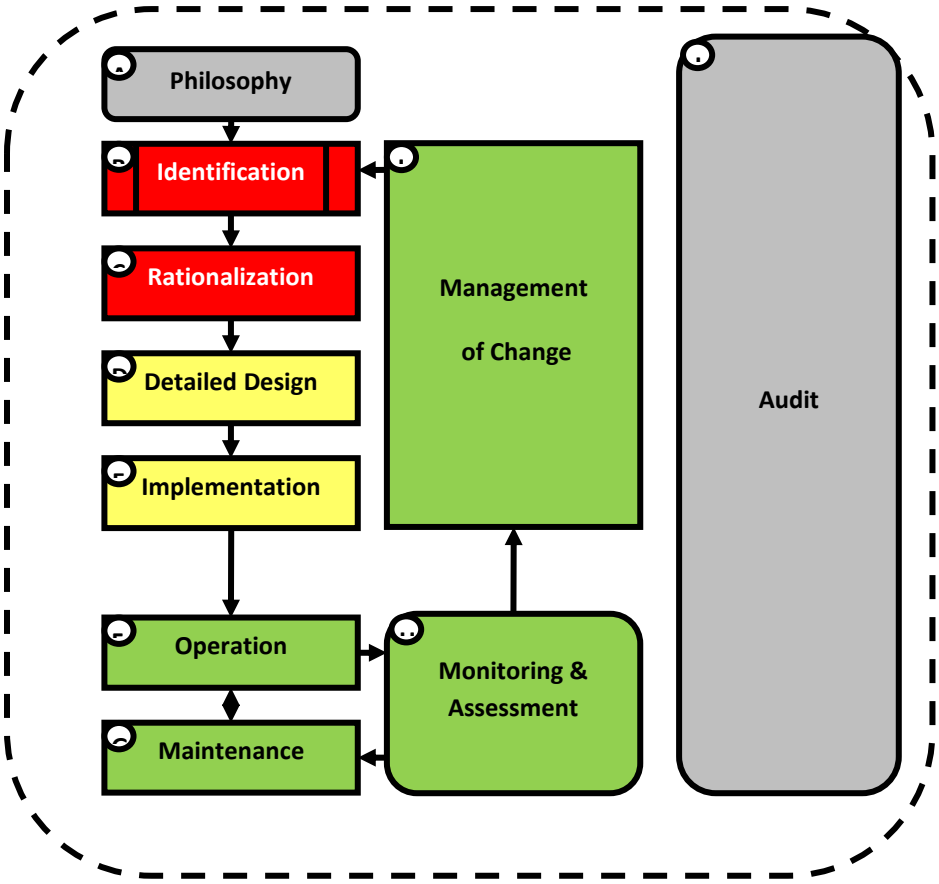

Figure 1. The Alarm Management Lifecycle

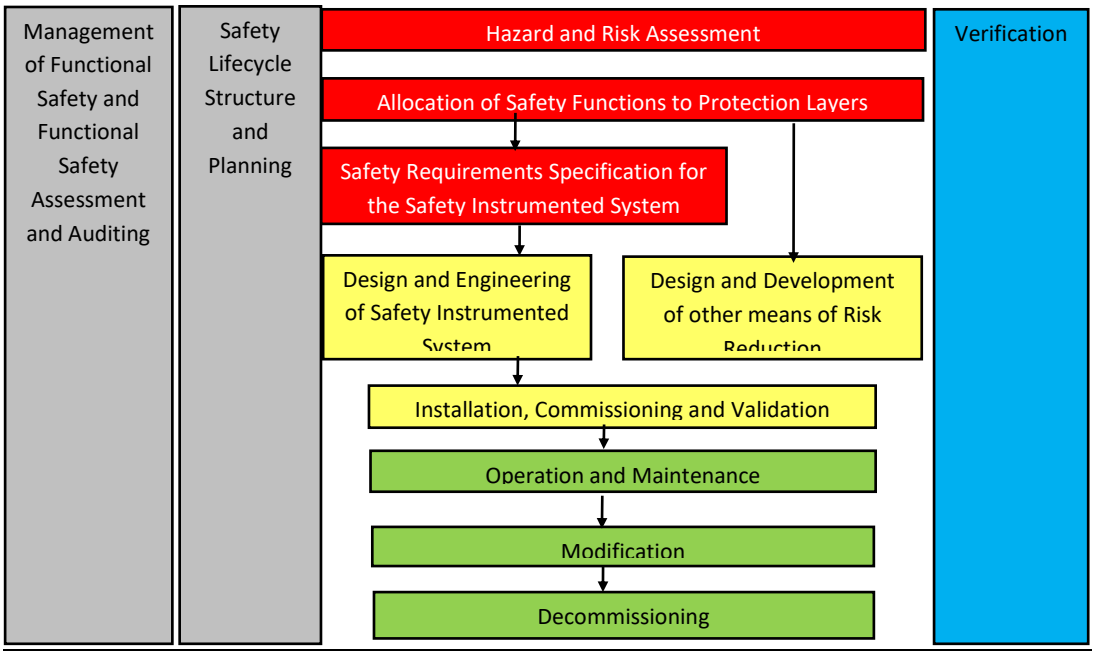

Figure 2. The Safety Instrumented System Lifecycle

Philosophy

The usual starting point in the alarm lifecycle is the development of an alarm philosophy. The philosophy provides guidance for all of the other lifecycle stages. It includes key definitions like the definition of an alarm, which by itself is a critical element to alarm management.

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

One of the most important principles of ISA-18.2 is that an alarm requires a response. This means if the operator does not need to respond, then there should not be an alarm. Following this cardinal rule will help eliminate many potential alarm management issues. 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." [8] Utilization of a philosophy must be embraced by all affected personnel (operator, technician, engineer and manager) within a facility and is a required element of ISA18.2. In addition, these individuals must take ownership of the process throughout its "Lifecycle".

The philosophy stage of the alarm management lifecycle is similar to the safety lifecycle structure and planning stage of the safety instrumented system lifecycle and is the foundation to successful alarm management. The philosophy ensures the processes for other lifecycle stages are planned and documented.

Identification

The identification stage of the alarm lifecycle includes activities like P&ID reviews, process hazard reviews, quality reviews, layer of protection analysis, and environmental permits that identify potential alarms. ISA-18.2 does not prescribe requirements for alarm identification methods. These methods are already well documented. To ensure that the results are useful as an input to the alarm rationalization stage, it is helpful to document the cause, potential consequence, and the time to respond for each identified alarm.

The identification stage of the alarm management lifecycle is analogous to the hazard and risk assessment phase of the SIS lifecycle where the process hazards that may need a SIF (safety instrumented function) are identified.

Rationalization

In the rationalization stage of the alarm lifecycle each potential alarm is tested against the criteria documented in the alarm philosophy to justify that it meets the requirements of being an alarm. The consequence, response time, and operator action are documented.

Alarms are analyzed to define their attributes (such as limit, priority, classification, and type). Alarm priority should be set based on the severity of the consequences and the time to respond. Classification identifies groups of alarms with similar characteristics (e.g. environmental or safety) and common requirements for training, testing, documentation, or data retention. Alarms coming from a Safety Instrumented System (SIS) may be classified as safety alarms, which fall under requirements for "highly managed alarms". The results of the rationalization are documented in a Master Alarm Database (MAD).

The rationalization stage is analogous to the allocation of safety function to protection layers and the safety requirement specification for the safety instrumented system stages of the SIS lifecycle where the potential need for a safety instrumented function is identified and where the Safety Integrity Level (SIL) of each safety instrumented function (SIF) is documented along with its functional requirements. The product of rationalization is a list of requirements in the Master Alarm Database (MAD) which corresponds to the documentation provided in a Safety Requirements Specification (SRS).

Detailed Design

In the detailed design stage of the alarm lifecycle, an alarm is designed to meet the requirements documented in the alarm philosophy and the rationalization. Poor design and configuration practices are a leading cause of alarm management issues. Alarm design includes the basic alarm design, setting parameters like the alarm deadband or off-delay time, advanced alarm design, like using process or equipment state to automatically suppress an alarm, and HMI design, displaying the alarm to the operator so that they can effectively detect, diagnose, and respond to it. During the detailed design phase, the information contained in the Master Alarm Database (such as alarm limit and priority) is used to configure the system.

Reising and Montgomery found that "good alarm system performance requires a battery of techniques and practices, from alarm rationalization upfront, to ongoing maintenance activities such as addressing worst actors." In addition, 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." [9] 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. [10]) will need to be utilized, thus allowing the operator to achieve our goal of accessing the alarm and responding appropriately [11].

The detailed design stage of the alarm lifecycle is analogous to the design and engineering stage of the SIS lifecycle. The Human Machine Interface (HMI) design is an explicit requirement of both standards.

Implementation

The implementation stage of the alarm lifecycle addresses putting the alarms into operation. It includes the activities of training, testing, and commissioning. Testing and training are ongoing activities, particularly as new instrumentation and alarms are added to the system over time or process designs changes are made.

Demands on the operator in the petrochemical work environment are an everyday challenge. Training is a critical element that enables the operator to be effective, yet the typical training methods and strategies have been identified as inadequate [12]. "Particularly, current training practices are observed to have a significant negative impact on ASM performance"[13]. "Effective training for ASM requires the development of a training program that targets task-appropriate competencies and establishes a continuous learning environment"[14]. For alarms to be effective, it is fundamental that the operator know what to do when he receives the alarm; thus, continuous training is necessary due to the dynamic nature of the petrochemical plant environment.

The implementation stage is analogous to the installation, commissioning, and validation stage of the SIS lifecycle. Both transition from design to operation and include testing and training.

Operation

During the operation stage of the alarm lifecycle, an alarm performs its function of notifying the operator of the presence of an abnormal situation. Key activities in this stage include exercising the tools the operator may use to deal with alarms, including shelving and placing alarms out-of-service. Shelving is critical for helping an operator respond effectively during a plant upset by manually hiding less important alarms. Alarms that are shelved will reappear after a preset time period so that they are not forgotten. Operator performance can be improved by making available the information fleshed out during rationalization such as an alarm's cause, potential consequence, corrective action, and the time to respond.

The operation stage of the alarm lifecycle is in part analogous to the operation and maintenance stage of the SIS lifecycle. Again as highlighted above, operator training is, of necessity, an important activity.

Maintenance

The maintenance stage of the alarm lifecycle is distinct from the operation stage. The process of placing an alarm out-of-service transitions the alarm from the operation stage to the maintenance stage. In the maintenance stage the alarm does not perform its function of indicating the need for the operator to take action. The standard describes the recommended elements of the procedure to remove an alarm from service and return an alarm to service. 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.

Depending on the alarm priority, classification, and time to respond the act of taking an alarm out of service may necessitate internal administrative procedures to effectively mitigate the hazard during the period which the alarm is out of service. These procedures need to provide clear guidance on who must be notified and what other indication the operator will utilize to avert the existing abnormal situation for the specified alarm. The alarm priority and consequence may be severe enough to require management approval before the operator removes the alarm from service.

The maintenance stage of the alarm lifecycle is in part analogous to the operation and maintenance stage of the SIS lifecycle, particularly where repair, replacement, and testing take place.

Monitoring and Assessment

Monitoring and assessment of the alarm system is a separate stage of the alarm lifecycle because it encompasses data gathered from the operation and maintenance stages. Assessment is the comparison of the alarm system performance against the stated performance goals in the philosophy.

This is roughly analogous to the recording of demand on a safety instrumented system that takes place during the operation and maintenance stage of the SIS lifecycle. This highlights an important difference between alarms and SIFs. Each SIF is designed to achieve a target availability. The availability of an alarm

is dependent on the performance of the operator. The availability of each alarm is somewhat dependent on the alarm system as a whole. This can be seen in ANSI/SA-84.00.01-2004 Part 3 (IEC 61511-3 Mod) [17] where the PFD for a stressed operator vs. an operator with no stress can increase by a factor of 100 – 10,000. The reliability of an alarm cannot be determined without an understanding of the overall performance of the alarm system.

One of the key metrics is the rate alarms are presented to the operator. In order to provide adequate time to respond effectively, an operator should be presented with no more than one to two alarms every ten minutes. A related metric is the percentage of ten minute intervals in which the operator received more than ten alarms (which indicates the presence of an alarm flood). ISA-18.2 recommends using no more than three or four different alarm priorities in the system. To help operators know which alarms are most important so they can respond correctly, it is recommended that no more than 5% of the alarms be configured as high priority. Table 1 from ISA-18.2 provides several of the key metrics highlighted in the standard.

A key activity during this stage is identifying "nuisance" alarms - which are alarms that annunciate excessively, unnecessarily, or do not return to normal after the correct response is taken (e.g., chattering, fleeting, or stale alarms). Reising and Montgomery conducted a study which correlated many of the metrics which were originally published by EEMUA, 1999 [15]. In addition, they highlighted in their paper multiple success stories which detailed positive results of implementing alarm management [9].

The monitoring and assessment stage is in part analogous to the activities that take place in the operation and maintenance stage of the SIS lifecycle, where demands on the safety system are documented and any problems investigated. Because of the scale of the alarm system, monitoring is automated and assessment is frequent.

Table 1 - ISA-18.2 Alarm Performance Metrics

Alarm Performance Metrics Based upon at least 30 days of data		
Metric	**Target Value**	
Annunciated Alarms per Time:	Target Value: Very Likely to be Acceptable	Target Value: Maximum Manageable
Annunciated Alarms Per Day per Operating Position	~150 alarms per day	~300 alarms per day
Annunciated Alarms Per Hour per Operating Position	~6 (average)	~12 (average)
Annunciated Alarms Per 10 Minutes per Operating Position	~1 (average)	~2 (average)
Metric	**Target Value**	
Percentage of hours containing more than 30 alarms	~<1%	
Percentage of 10-minute periods containing more than 10 alarms	~<1%	

Maximum number of alarms in a 10 minute period	≤10
Percentage of time the alarm system is in a flood condition	~<1%
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	~<1% to 5% maximum, with action plans to address deficiencies.
Quantity of chattering and fleeting alarms	Zero, action plans to correct any that occur.
Stale Alarms	Less than 5 present on any day, with action plans to address
Annunciated Priority Distribution	3 priorities: ~80% Low, ~15% Medium, ~5% High or 4 priorities: ~80% Low, ~15% Medium, ~5% High, ~<1% "highest" Other special-purpose priorities excluded from the calculation
Unauthorized Alarm Suppression	Zero alarms suppressed outside of controlled or approved methodologies
Unauthorized Alarm Attribute Changes	Zero alarm attribute changes outside of approved methodologies or MOC

Management of Change

The management of change stage of the alarm lifecycle includes the activity of authorization for all changes to the alarm system, including the addition of alarms, changes to alarms, and the deletion of alarms. Once the change is approved, the modified alarm is treated as identified and processed through the stages of rationalization, detailed design and implementation again. Documentation like the MAD is updated and the operators are trained on all changes since they must take the actions.

The management of change stage is analogous to the modification and decommissioning stages of the SIS lifecycle, where SIFs are modified or removed.

Audit

The audit stage of the alarm lifecycle is primarily focused on the periodic review of the work processes and performance of the alarm system. The goal is to maintain the integrity of the alarm system throughout its lifecycle and to identify areas of improvement. The alarm philosophy document may need to be modified to reflect any changes resulting from the audit process. This may necessitate the need to review the existing alarms and to cycle back through the other stages of the alarm lifecycle. Remember, "with alarm management – you will never, ever be finished." [16]

The audit stage is similar in part to the management of functional safety and functional safety assessment stage of the SIS lifecycle, which includes auditing compliance with requirements.

Starting Points

Another important difference between the alarm and SIS lifecycles is that there are different starting points in the alarm lifecycle and only one point to start the SIS lifecycle. This difference comes mostly from the focus of the lifecycle. The alarm lifecycle has three starting points: philosophy, monitoring, and audit. The appropriate starting point depends on the site needs. Alarm philosophy is a good place to start for a new system, while monitoring or audit can be an ideal starting point for an existing alarm system.

The SIS lifecycle truly starts with management of functional safety, but is often viewed as starting with the identification of the process hazard.

Terminology

Although similar in many respects, the alarm management and functional safety standards differ in the meaning and application of key terminology. Since these words / applications appear in both standards but have different meanings it may be helpful to understand how the usage may vary.

Assessment

Assessment in the alarm lifecycle refers to the frequent comparison of alarm system performance against the goals stated in the alarm philosophy. This is usually an automated process because of the amount of data involved. In the safety lifecycle, assessment is more of an event where the safety functions protecting against a hazard are evaluated by a team of people.

Diagnostic

Diagnostic in the alarm lifecycle is an attribute desired in each alarm to indicate a specific abnormal situation, equipment malfunction, or process deviation. In the safety lifecycle, diagnostic is a function to detect a failure. System diagnostic alarms indicate a detected failure in a safety instrumented function or system.

Requirements Specifications

In the alarm lifecycle, an alarm system requirements specification (ASRS) may be written to ensure the alarm system functionality is included in the control system, since the alarm system is a part of the basic process control system (BPCS). The ASRS describes system level functionality necessary to meet the objectives in the alarm philosophy. Safety instrumented systems (SIS) are typically independent of the BPCS. The SIS is designed and engineered to meet the safety requirements specification (SRS). The SRS provides integrity and functional requirements for each SIF.

Time to Respond

In the alarm lifecycle, the maximum allowable response time is the limit of the time period between the annunciation of the alarm (ack delay) and the time when the operator takes corrective action (operator

response delay). It must be short enough that the process has time to react to the corrections made, considering the process deadtime and response delay, so the process variable does not exceed the consequence threshold.

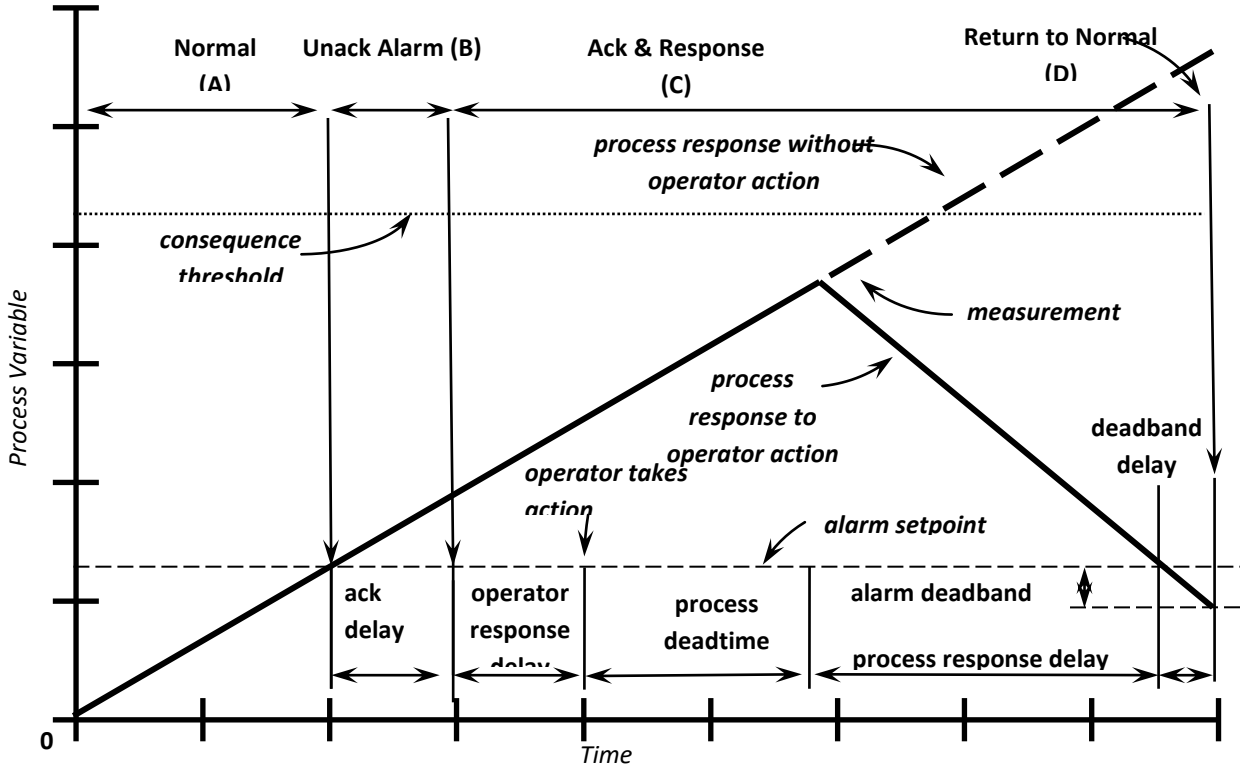

Figure 3. Alarm Response Timeline

In the safety lifecycle, process safety time is the time between the initiating event and the occurrence of a hazardous event. The combination of the diagnostic test interval, the time for corrective action, and the reaction time to achieve a safe state should be less than the "process safety time", see Figure 4.

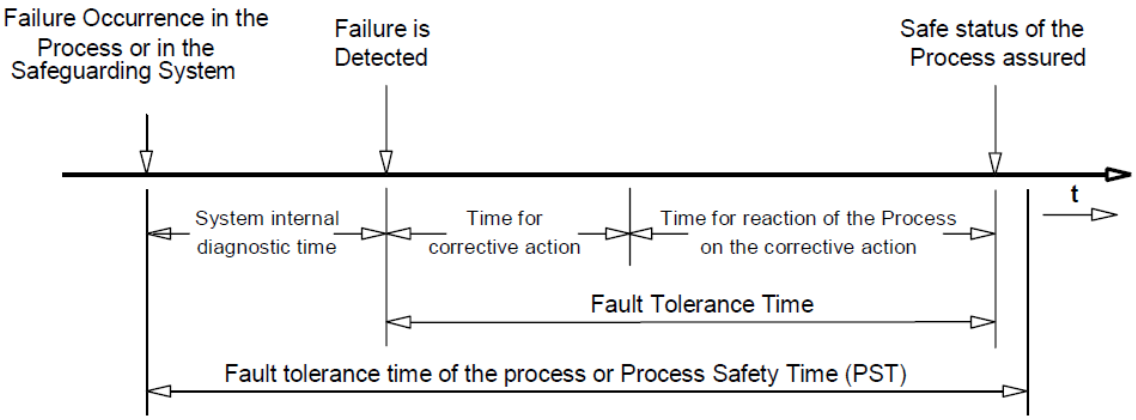

Figure 4. Timing diagram of DIN V 19251 as applicable for a single channel SRS with ultimate self tests executed within the PST [18]

The process safety time includes the time to detect the event and the process response delay, in addition to the maximum allowable response time.

References

1. ANSI/ISA ISA18.00.02-2009 “Management of Alarm Systems for the Process Industries”.
2. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) “Functional Safety: Safety Instrumented Systems for the Process Industry Sector”.Bransby ML and Jenkinson J., The Management of Alarm Systems, HSE Contract Research Report 166/1998 ISBN 07176 15154, First published 1998.
3. Campbell Brown, D., “Horses for Courses – A Vision for Alarm Management,” IBC Seminar on “Alarm systems,” London, June 26-27, 2002.
4. Nimmo, I., “Abnormal Situation Awareness – The Need for Good Situation Awareness,” Advances in Process Control 7 ‘Tomorrow’s Control Today,’ York, September 20-21, 2004.
5. Health & Safety Executive “The explosion and fires at Texaco Refinery, Milford Haven, 24 July 1994”, HSE, 1997
6. Campbell Brown, D., “Alarm System Performance – One Size Fits All?”, Measurment & Control, May 2003.
7. Nimmo, I., “Rescue Your Plant from Alarm Overload,” Chemical Processing, January 2005.
8. Reising, D.V. and Montgomery, T., “Achieving Effective Alarm System Performance: Results of ASM Consortium Benchmarking against the EEMUA Guide for Alarm Systems,” 20th.
9. 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, Wasington, DC, US Nuclear Regulatory Commision, 1994.
10. Reising, D.V., Downs, J.L. and Bayn, D., “Human Performance Models for Response to Alarm Notifications in the Process Inducstries: An Industrial Case Study,” Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting, 2004, Santa Monica, CA, pp.1189-1193.
11. Errington, J. and Bullemer. P.T., "Designing for Abnormal Situation Management®", AICHE conference on Process Plant Safety, Houston TX, March 1998. ® Abnormal Situation Management and ASM are registered trademarks of Honeywell International
12. Bullemer, P. and Nimmo, I. “A Training Perspective on Abnormal Situation Management: Establishing an Enhanced Learning Environment,” Proceedings of the 1996 AICHE Conference on Process Plant Safety, Houston, TX. 1996.
13. Bullemer, P. and Nimmo, I. “Tackle Abnormal Situation Management with Better Training,” Chemical Engineering Progress, January, 1998.

14. Engineering Equipment and Materials User Association, Alarm systems: A guide to design, management, and procurement (Pub. No. 191), London: EEMUA, 1999.
15. Errington, J., DeMaere, T., & Reising, D. (2004). After the alarm rationalization: Managing the DCS alarm system. Paper presented at the AIChE 2004 Spring Meeting, New Orleans, LA, April 25-29.
16. ANSI/ISA-84.00.01-2004 Part 3 (IEC 61511-3 Mod) "Functional Safety: Safety Instrumented Systems for the Process Industry Sector"
17. DIN V 19251, MC Protection Equipment Measurement & control equipment: Requirements and measures for safeguarding functions (1995).

Revision History

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

Presented at the 2010 Texas A&M Instrumentation Symposium

Author Biographies

Todd Stauffer is responsible for marketing and business development of exida's alarm management products and services (training, consulting, engineering tools). Previously he worked for Siemens Energy & Automation where he held Product Management responsibility for APACS and PCS 7, as well as led key activities around alarm management and control system security. He is an editor and voting member of the ISA-18.2 standards committee on alarm management. A graduate of Penn State University, Todd holds a BS in Mechanical Engineering and earned a Master's degree in Mechanical Engineering from the University of Pennsylvania. Todd is currently a registered professional engineer in the State of Pennsylvania.

Nicholas P. Sands is currently a process control engineer working for DuPont's Kevlar® and Nomex® businesses. In his 19 years with DuPont he has been a business process control leader, site process control leader, process control consultant, and plant control engineer in several different businesses. Nick is Co-chair of ISA Standards & Practices committee 18 working on Alarm Management, and was involved in the development of the Certified Automation Professional program. Nick's path to instrumentation and control started when he earned his BS in Chemical Engineering from Virginia Tech. When not working or reading, Nick and his wife Ruth run a recreational sled dog team.

Donald G. Dunn was employed by Diamond Shamrock from 1991-1998 as an IEA & Controls Engineer and with Equistar Chemicals from 1998-2006 were he was employed as a Principal IEA & Controls Engineer. Since 2006, he has been employed by Aramco Services Company in a Consulting Engineering group. He is currently a senior member of the IEEE (24 years) and the ISA. He has been active in standards development, peer review of technical papers, paper authorship and presentations since 1994 and has been an invited presenter at various industry forums. He is a member of the IEEE Standards Association and a Director and Vice President Elect on the ISA Standards & Practices Board. He currently chairs IEEE P1714 and API540 and co-chairs ISA18 in addition to being active in other standards development organizations and working groups. Mr. Dunn has been an active member within IEEE Industry Application Society PCIC (1994) and now serves on the IEEE IAS Executive Committee as the Education Department Chairman. Since 1999, he has actively volunteered on the IEEE Houston Section Executive Committee and was elected Section Chairman in 2001-2002 and again in 2006.

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