Breathing life into the alarm management lifecycle

Sarah Manelick
Principal Specialist, Alarm & Process Safety Management
aeSolutions, Anchorage, AK

Abstract

‘Evergreen’ and ‘lifecycle’ have become two common buzz words in our industry. They are thrown around in a variety of topics, processes, and philosophies as descriptions of how management plans should be set up. But what does it really mean to have an evergreen process? How does one keep a lifecycle alive? This is especially relevant when it comes to topics such as alarm management, where it is commonly touted that once a plant rationalizes their entire system, they have completed alarm management. This paper will deconstruct the alarm management lifecycle and pinpoint key aspects that can be integrated into process safety management systems and work processes that already exist. Tying the alarm management lifecycle to what is already being done as part of process safety and good engineering practice will help to ensure it remains ‘evergreen’ and delivers the intended benefits.

What is alarm management?

Alarm management is the collection of processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems. It is characterized by design principles including hardware and software design, good engineering practices, and human factors. [1]

The Alarm Management Lifecycle

Figure 1 is a graphical representation of the alarm management lifecycle from the ISA 18.2 standard. [1]

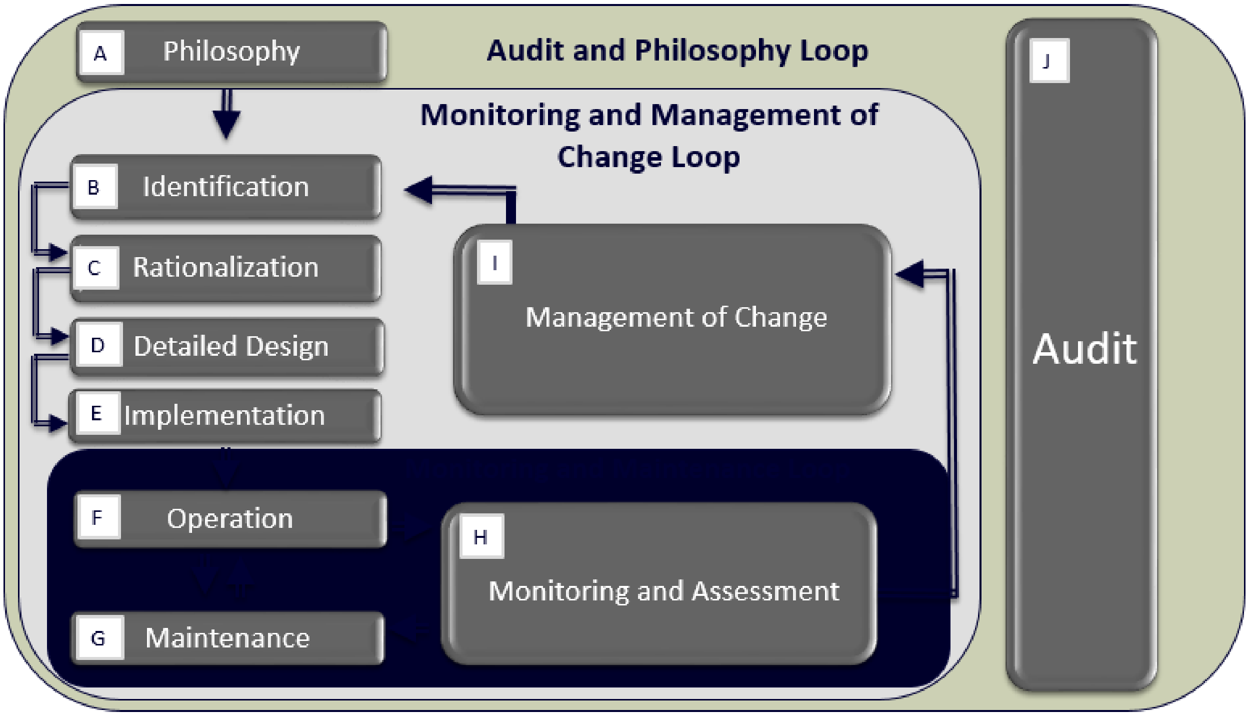

Figure 1: Alarm Management Lifecycle

The lifecycle is essentially a circle; there is no beginning or end. There are different places an organization may choose to enter it, but the overall lifecycle follows the "Plan-Do-Check-Act" process for the life of the operating unit. An organization may have developed a philosophy, rationalized alarms, and implemented them, but that does *not* mean they have 'completed' alarm management. As processes and equipment evolve and change (e.g., removing or introducing equipment, changing flow rates, changing chemicals, etc.), different steps of the lifecycle come back into importance. The goal of alarm management should be to keep the lifecycle updated and evergreen.

Integration of the Alarm Management, Functional Safety and Cybersecurity Lifecycles

After reviewing the different parts of the lifecycle, it may seem overwhelming to figure out how it will be possible to not only perform all the stages of the lifecycle, but to also keep the entire lifecycle evergreen. The question then becomes how can an organization integrate these items into what they are already doing to keep the lifecycle active?

This is where it becomes important to understand what other processes and lifecycles a company may already have in place. The Process Safety Management Program at the facility is a lifecycle process. The Alarm Management, Functional Safety Management and Cybersecurity Management Systems that represent conformance to Recognized and Generally Accepted Good Engineering Practices (RAGAGEP) from a process safety perspective are all lifecycle processes that are likely in practice at some level. Integrating the data and work flow common to these three lifecycles is the most effective means to succeed in achieving their risk management objectives. Doing so will make good use of valuable resources and help avoid the costs associated with rework. This would apply for projects along with sustaining the integrity of these systems on a daily basis.

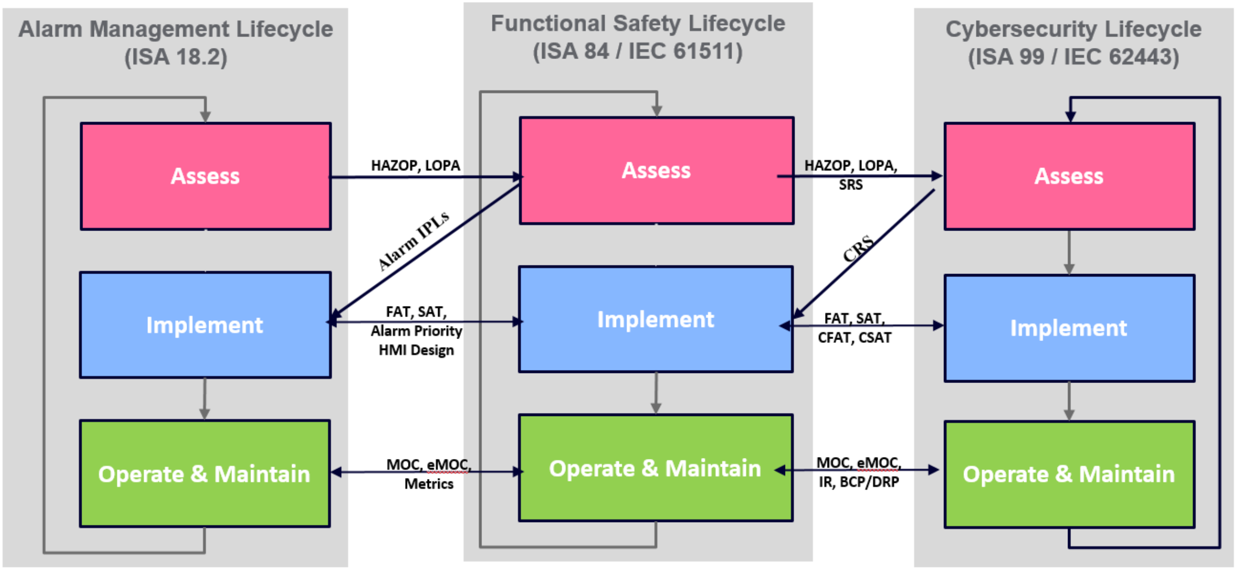

Figure 2: Integration of Lifecycles

Figure 2 shows the similarity and possible connection points between the alarm management, functional safety and cybersecurity lifecycles. Of the three, the organizations tend to be more mature with executing the functional safety lifecycle. As a result, it is the one people are most familiar with. The assess phase is where the hazard analyses are performed. This is where risk gaps are identified. Similar functions are performed in the assess phases of both the alarm management and cybersecurity lifecycles. When assessing items in cybersecurity, one is considering scenarios first identified in PHAs. The same is true in alarm management when an alarm is used as a protection layer. The PHA feeds the other lifecycles.

There is similar overlap in the implementation phase of the three lifecycles. Implementing a cybersecurity program means understanding the risks presented at the functional process level. Are your alarms and controls feeding into a secure network? Have levels of security been applied for changes to alarm and shutdown setpoints to ensure they are protected and secure? In implementation there is a connection between alarm priority, alarm setting, and human machine interface (HMI) design for the functional safety lifecycle and alarm management lifecycle. Similarly, there is quality assurance with factory and site acceptance testing (FAT/SATs) for all three lifecycles.

Management of Change

All three lifecycles also include the need for a management of change (MOC) process to ensure design changes are tracked and approved. Proper implementation of MOC is critical in keeping all three lifecycles evergreen. A change in one lifecycle may, and most likely will, impact all three lifecycles. Verify that a review of impacts between the lifecycles is performed. Even something as simple as an added check box on the site's MOC form could be critical in making sure that the information stays accurate and connected between all the lifecycles. Something as minor as altering a chattering alarm (e.g., because its setpoint was too close to a shutdown value) will impact the alarm, the master alarm database, the other lifecycles, and many different process safety information documents. If normalization of deviation is allowed (i.e., not tracking and reviewing the impact of what are believed to be minor changes), alarms will eventually become unrationalized, and things will revert back to their original, un-managed state. It is important to understand how even small changes are interrelated as they can have a cascading effect throughout the lifecycles. A well-documented MOC process will ensure that alarms are justified and used consistently, not arbitrarily, and that changes do not fall through the proverbial cracks within an organization.

Integrated Inspections and Functional Testing

An effective implementation of alarm management allows a facility to design alarms that notify operations that the process has traveled outside the optimal operating window and needs immediate intervention. To keep alarms operating effectively they need to be tested. [2] The key is to develop a testing program and schedule that works for each site and stick with it. The sooner that can be done, the better. First, identify the overall goals. Document the testing program for operations and maintenance and get management approval. Everyone needs to understand the importance of testing. This will help prevent alarm floods and long lists of bad actors due to incorrect setpoints, deadbands, on/off delay issues, etc.

Facilities covered by Pipeline and Hazardous Materials Safety Administration (PHMSA) or Department of Transportation (DOT) regulations specifically, the control room management (CRM) requirements are expected to perform an annual safety related points setpoint review. [3] Some companies have found that these annual safety related point reviews are also an effective time to not only verify the documented set point for these alarms is the same in both the HMI, and the master alarm database, but to also ensure that the setpoint that has been documented is in fact the activation point for the alarm, by field testing.

Other options to consider might be to create a testing schedule for low consequence alarms that have been identified as bad actors, and subsequently corrected. Once it has been confirmed that the alarm is functioning correctly and has passed multiple testing rounds, one may consider removing it from the test scheme. Another approach may be to segment process units and test the top five bad actors. Rotate through the process units completing a select number each month to get through all of them at least once a year. The point is, the testing philosophy is flexible and the real key to success for this phase of the lifecycle is to ensure that they are being tested and that it is occurring on a consistent schedule. The consistency of a schedule allows trouble-shooting and corrective action when a problem is identified, as well as extension of testing periods when supported by historic inspection records. Staying current on testing will help to identify and mitigate instrumentation and alarm issues down the road.

Alarm Management Training

Training on alarm management is extremely important. Accidents have happened in part because of a lack of training. One specific incident that comes to mind was at a site that had rationalized alarms, had documented corrective actions, and felt that they were making the cut for alarm management. One day one of their high safety consequence alarms came in. Having never been trained on the corrective actions, or even where to find the documents that listed them, operations personnel responded incorrectly. The situation unfortunately ended up with a fatality.

The incident investigation found that a lack of training was one of the most avoidable causes of this deadly event. If an organization goes through the whole process of implementing an alarm management program, and puts the time in for rationalization and implementation, yet skips the training requirements, everything has been for naught. Alarms are focused around the operations personnel; they are the final element of an alarm. Just as the final element of a safety instrumented function is a valve or a pump, the final element of an alarm is an operator. This means training on corrective actions is crucial for efficient and accurate operator response.

So how can an organization implement training? What are the key points to keep in mind? The first step is to decide what should be included in the training. The second might be to look at what training is already being performed as part of the other lifecycles and see where some crossover might occur. As a minimum, general alarm management training should be provided for all staff.

Management needs to understand the alarm management philosophy and goals for the site.

Engineering, operations, automation specialists, electricians and technicians need to be trained on the details of each phase of the lifecycle that pertains to them. They need to understand the goals, the resources and the tools. They need to know how to use the alarm management software, how to find the corrective actions and how to respond to alarms. They need to understand the HMI displays, the graphics, the different alarm symbols and sounds, as well as all the different priorities. There should also be ways to track training and determine whether the concepts within the training are being effectively administered.

One should also consider how *often* training should be completed. This will vary. If the facility is covered by the process safety management (PSM) regulation [4], there will already be PSM training requirements. In such cases, it might be a good idea to link alarm training along with all the other PSM training. Different sites may have different preferences, such as bi-annually, or annually. Every new person needs onboarding training, and refresher training might be done annually. Training is not a ‘one and done’ sort of thing, it is a constant process. Ongoing training is the key to success. Refresher training will reinforce the goals of alarm management and keep everyone on the same proverbial page and going in the same direction.

Every organization needs to determine who will create the training, who will present it, and what material will be covered. Perhaps a company’s existing training department can handle these tasks and integrate it all into their existing programs. Perhaps a company may have an alarm management champion who could create and lead the training. The key is to provide at least *some* sort of alarm management training. There is no universal one-size-fits-all approach. Every organization may accomplish this in different ways. Undertaking all this may sound overwhelming, much like eating the proverbial elephant. But as the old phrase goes, you eat an elephant one bite at a time, and certainly not overnight. Stalling and not providing any training at all would be a very poor choice.

Conclusion

How can an organization ensure its alarm management lifecycle is successful? The first step is to look at what is already being done at the site. What other lifecycles or processes exist that are performing similar activities and share data and resources with those within the alarm management lifecycle? Finding these connection points and integrating alarm management activities into what is already being performed is key to keeping up with the evergreen lifecycle approach. While integration of these activities will look different for each company, time has shown that success comes most easily when the MOC process, testing and training alarm management activities have been integrated into what is already being accomplished.

References

1. ANSI/ISA-18.2-2016 - Management of Alarm Systems for the Process Industries.
2. ANSI/ISA-84.91.01-2012 - Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industry.
3. 49 CFR Parts 192 and 195 | Pipeline Safety: Control Room Management/Human Factors, 2011.
4. 29 CFR 1910.119 – Process Safety Management of Highly Hazardous Chemicals, 1992