Alarm Management Lessons from the Process Industries

Shawn Forrest and Nicholas Sands

About the Authors

Shawn Forrest, MS, is a senior lead reviewer at the Food and Drug Administration Center for Devices and Radiological Health in Silver Spring, MD. Email: shawn.forrest@fda.hhs.gov

Nicholas Sands, CAP, PE, is an International Society of Automation fellow and a technology fellow at DuPont in Wilmington, DE. Email: nicholas.p.sands@dupont.com

The healthcare industry recognizes the need to improve medical device alarm management. During the previous 30 years, medical devices have increased in complexity and provided more alarms. Similar changes in technology caused alarm management crises in the airline, nuclear, and process industries. The process industries (e.g., chemicals, oil refining, oil and gas production, pulp and paper, pharmaceuticals, food and beverage, non-nuclear power generation) have developed standards that may provide some concepts to strengthen the healthcare industry's alarm management work.

The process industry's alarm management standards are American National Standards Institute (ANSI)/International Society of Automation (ISA) 18.2-2016[1] (updated from 2009) and International Electrotechnical Commission (IEC) 62682-2014,[2] both titled *Management of alarm systems for the process industries*. These standards outline an alarm management life cycle that assists in organizing the design and optimization of alarm management programs. These management programs include both the use of alarm equipment and a defined alarm response process. They describe various steps in the alarm system design and optimization process that ensure functions are appropriate for use.

The key standards related to alarms in the healthcare industry are IEC 60601-1-8:2006/AMD1:2012, *General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems*,[3] and human factors standards such as IEC 62366-1:2015, *Application of usability engineering to medical devices*,[4] and Association for the Advancement of Medical Instrumentation (AAMI) HE75:2009/(R)2013, *Human factors engineering—Design of medical devices*.[5] These standards all focus on the functionality of individual devices as validated and marketed by manufacturers. They do not account for any postmarket integration with other devices in the intended use environment by responsible organizations. The standards ensure that devices contain the appropriate tools for a user to implement them in a comprehensive alarm management program. However, such devices are not typically designed or tested for specific integration with other devices in the implemented environment or the specific care patterns used by an organization to mitigate risk.

Existing Effort to Improve Clinical Alarm Management

Recent alarm improvement work guided by AAMI highlights the need for data-driven unit- and hospital-specific alarm system optimization to address alarm fatigue by decreasing the number of nonactionable alarms. The most succinct published summary of this work is the AAMI Foundation's *Clinical Alarm Management Compendium*,[6] which provides several ideas for safe alarm management and example alarm parameter settings. However, the process for developing an effective alarm management program has not

been fully specified. IEC technical report (TR) 80001, *Application of risk management for IT-networks incorporating medical devices*,[7] represents one family of standards related to alarm system development by a responsible organization. However, only IEC TR 80001-2-5 directly discusses the implementation of alarm equipment in the healthcare environment, and it is focused on the transmission of alarms between devices in an alarm system.

There is an opportunity to better specify a process for effective on-site design and implementation of the complete alarm management program, which integrates medical devices of various types and manufacturers. The development of such a standard would benefit hospitals, clinicians, manufacturers, and patients by guiding system developers through the steps needed to ensure a robust design. Many care environments may already follow a formal process similar to the one described in this article. A standard could also define common risk mitigation strategies to further inform the medical device standards on alarm use patterns, which are not well defined.

An Alarm Management Model from the Process Industry

In process industry facilities (e.g., a chemical manufacturing plant), alarms are generally centralized and presented to the operator at a fixed location or console. The focus has been on managing the alarm system and all individual alarms, presentation to the operator, and training the operator on effective response to alarms. Alarm management steps are grouped into stages of the alarm management life cycle (Figure 1). This article highlights some of the key stages of the alarm management life cycle.

Philosophy

Each manufacturing plant develops a guidance document for alarm management, which includes roles and responsibilities and methods for key activities such as rationalization, including prioritization and classification. The guidance also includes performance metrics with target values and action limits, which define acceptable and unacceptable performance. Performance metrics include average alarm rate (alarms per hour per console operator) and percent time in alarm flood (percent of 10-minute intervals containing more than 10 alarms).

The definition of an alarm represents one of the most important elements of the alarm management program and is documented in the alarm philosophy. The process industry defines an alarm as an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response.[1,2]

Identification

Potential alarms for implementation are identified through a variety of processes, such as operating procedure reviews, incident investigations, and quality reviews.

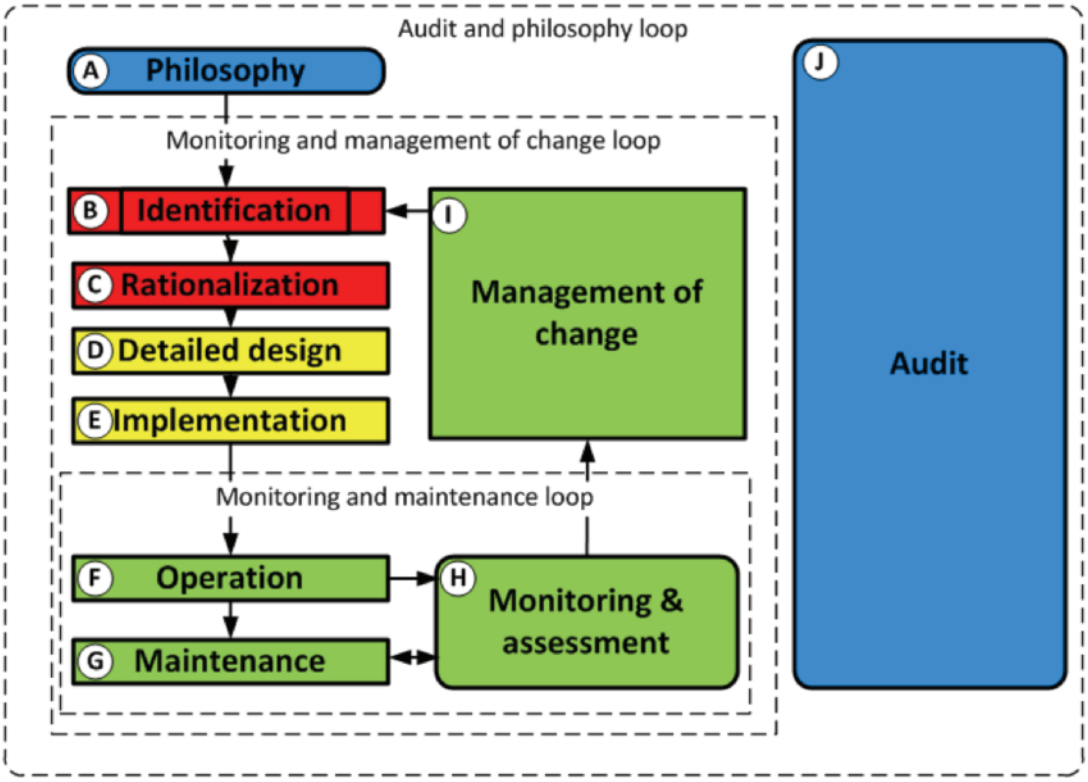

Figure 1. The International Society of Automation 18.2 alarm management life cycle[1]

Rationalization

This step reconciles the identified need for an alarm or alarm system change with the principles in the alarm philosophy and the definition of an alarm. Every alarm is rationalized to determine the consequence of inaction, the response action, the priority, and the class. This information informs training and design. If no consequence is prevented or no action can be taken, the alarm is rejected and not implemented as an alarm, though it may be logged as an event.

The rationalization process only allows for alarms if a timely action is required to prevent an undesired consequence.

Detailed Design and Implementation

In the design phase, alarm attributes are specified and designed based on the requirements determined by rationalization. Implementation puts the alarm or alarm system into operation and includes the key activities of training and testing.

Monitoring and Assessment

The alarm system is monitored while in operation. System performance is assessed by calculating performance metrics and comparing them with target values and action limits. Determining a standardized set of common metrics allows systems to be designed to report those metrics, and the metrics inform the development of appropriate system maintenance practices or the need for modifications.

Management of Change and Audit

Modifications to the alarm system are proposed and approved. The change process should follow each of the alarm management life cycle stages from identification to implementation. In the audit stage, periodic reviews are conducted to maintain the integrity of the alarm system and alarm management processes. The audit can reveal gaps that are not apparent from routine monitoring.

Alarm Management in Practice

Applying the alarm management system in ISA-18.2 can produce dramatic results. The activities of monitoring, rationalization, implementation, and management of change substantially affect the overall effectiveness of the alarm system.

Measuring the alarm system's performance quantifies the problem. In addition to performance metrics, diagnostic metrics (e.g., most frequent alarms, chattering alarms, stale alarms) can identify the most problematic alarms. Addressing only the problem alarms may reduce the average alarm rate by two orders of magnitude in some instances.

Dramatic changes are also possible by applying the definition of an alarm through the rationalization process. A general assumption crept into alarm design over the years that if the operator should be aware of a condition, then an alarm is the way to communicate the condition. This assumption led to a proliferation of alarms. The rationalization process only allows for alarms if a timely action is required to prevent an undesired consequence. The alarms are also prioritized based on the urgency for the operator to respond, usually via a matrix of the severity of the consequence and the time to respond. The typical results of rationalization are:

- 50% of alarms eliminated because there is no action or consequence.
- 80% of alarm priorities changed based on the urgency of response.
- 100% of actions in response to the alarm documented.

The purpose of the alarm and the actions to take in response to the alarm are documented during alarm rationalization. This information provides the foundation of the alarm response procedures used to train the operators. Prior to implementation of alarm management, few alarms included documented responses or associated training. Operators were expected to figure out what to do on their own.

Rationalization requires a significant effort. Once completed, the documentation needs to be maintained when alarms are added, modified, or removed. The management of change process updates the rationalization, the alarm response procedures, and the operator training. This is part of keeping the alarm system current over time, year after year.

Conclusion

Differences between the process and healthcare industries will affect the implementation of alarm programs. However, an established process evidenced in the process industry

provides a useful framework for more structured development of clinical alarm management programs. The steps outlined in this article seem reasonably straightforward to translate to the healthcare setting. Such guidelines are a worthwhile next step to help hospitals address alarm-related challenges. ■

Acknowledgments

To Robert Kretschmann (Rockwell Automation) and Jianchao Zeng (CDRH/FDA) for their support and encouragement throughout the preparation process of this article.

References

1. **International Society of Automation.** ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*. Available at: www.isa.org/templates/one-column.aspx?pageid=111294&productId=46961965. Accessed Feb. 1, 2017.
2. **International Electrotechnical Commission.** IEC 62682-2014, *Management of Alarm Systems for the Process Industries*. Available at: https://webstore.iec.ch/publication/7363. Accessed Feb. 1, 2017.
3. **International Electrotechnical Commission.** IEC 60601-1-8:2006+AMD1:2012, *Medical electrical equipment—Part 1-8: General Requirements for Basic Safety and Essential Performance—Collateral Standard: General Requirements, Tests and Guidance for Alarm Systems in Medical Electrical Equipment and Medical Electrical Systems*. Available at: https://webstore.iec.ch/publication/2599. Accessed Feb. 1, 2017.
4. **International Electrotechnical Commission.** IEC 62366-1:2015, *Medical Devices—Part 1: Application of Usability Engineering to Medical Devices*. Available at: https://webstore.iec.ch/publication/21863. Accessed Feb. 1, 2017.
5. **Association for the Advancement of Medical Instrumentation.** ANSI/AAMI HE75:2009/(R)2013, *Human Factors Engineering—Design of Medical Devices*. Available at: http://my.aami.org/store/detail.aspx?id=HE75. Accessed Feb. 1, 2017.
6. **AAMI Foundation.** Clinical Alarm Management Compendium. Available at: www.aami.org/alarm_compendium.pdf. Accessed Feb. 1, 2017.
7. **International Electrotechnical Commission.** IEC TR 80001-2-5:2014, *Application of Risk Management for IT-Networks Incorporating Medical Devices—Part 2-5: Application Guidance—Guidance on Distributed Alarm Systems*. Available at: https://webstore.iec.ch/publication/7487. Accessed Feb. 1, 2017.