TJC and ASSOCIATES, Inc.

spring 2023

The TJCAA Quarterly

www.tjcaa.com

Proactive Alarm Management

TJCAA's Business Certifications

- Alameda County Small, Local Emerging Business
- Bay Area Green Business Program
- California DGS SBE
- City of Colton SBE
- City of Los Angeles SBE
- City of Oakland LBE
- Eastern Municipal Water District SBE
- Inland Empire Utilities Agency SBE
- Metropolitan Water District of Southern California SBE
- Sacramento Municipal Utilities District (SMUD) SEED Vendor
- San Diego County Water Authority SBE
- Port of Long Beach SBE
- Port of Oakland LIABE/SBE/VSBE
- PWC Registration—Dept of Industrial Relations (DIR)
- West Basin Municipal Water District SBE

Proactive Alarm Management

TJCAA's Lead Control Systems Programmer, Michael Erwin, P.E., talks about managing alarms in your SCADA system.

Automation has come a very long way over the course of my 35-year career. When I started in this business, our SCADA human-machine interface systems were developed using rudimentary pixel-based graphics running on MS-DOS based personal computers, and we couldn't trust them enough to abandon our dependance on control room chart recorders, bar graphs, indicating lights, switches, and alarm annunciators. Today, we run redundant servers on fault-tolerant virtual machines, collect terabytes of historical data on redundant solid-state drives, and present high-performance graphics on multi-screen workstations that provide operators with the tools to manage complex control systems more safely and efficiently than ever. I occasionally still see an annunciator, typically with over half the bulbs burned out, or a chart recorder still spinning away underneath a pen that ran out of ink a decade ago, but it's just a matter of time before these are relegated to museum displays.

Just about everything has improved, with the glaring exception of the way many agencies manage their alarms. An alarm is defined as an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response. Yet, I have visited countless facilities where it's considered perfectly normal to be operating with their SCADA graphics filled with red or yellow alarm bars, flashing equipment failure symbols, and alarm summary displays with multiple pages of active alarms.

This raises some interesting questions. If an alarm is supposed to indicate the abnormal, how can we have multiple active alarms when the plant is functioning normally? If an operator is used to operating with active alarm conditions, does it increase the likelihood that they will miss a critical alarm condition and fail to respond accordingly? Does this scenario increase the risk of a public agency failing to meet water quality standards or creating a public health emergency? What steps can be taken to improve alarm management and minimize these risks?

The answers to that last question can be found in the American National Standards Institute (ANSI) / International Society of Automation's (ISA) *Standard 18.2 – Management of Alarm Systems for Process Industries*. ANSI/ISA 18.2 was originally published in 2009 and most recently updated in 2016, and it details the recommended work process for effectively and efficiently managing alarms for a modern SCADA-based control system. Figure 1 shows the 10 stages of the alarm management lifecycle as defined by ANSI/ISA 18.2.

The TJCAA Quarterly
spring 2023
www.tjcaa.com

Proactive Alarm Management

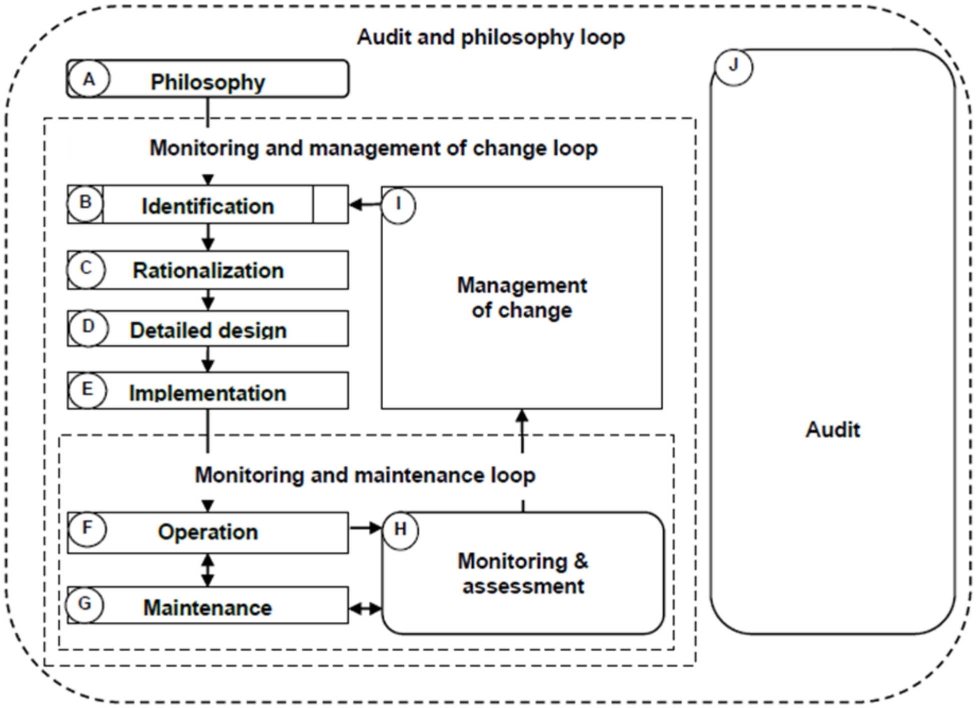

Figure 1: Alarm Management Lifecycle as Defined in ASNI/ISA 18.2-2016

A) Alarm Philosophy documents the objectives of the alarm system and the work processes necessary to meet those objectives.

B) Identification determines what the alarm conditions are for a given treatment process or application.

C) Rationalization ensures that an alarm meets the requirements set forth in the Alarm Philosophy and includes the process of determining prioritization, area classification, allowable setpoint ranges, time delay standards, "latching," and the documentation associated with the alarm and the appropriate response.

D) Detailed Design determines the methods used to notify the operator of alarm conditions and ensures that the alarm meets the conditions determined in the alarm Rationalization and Alarm Philosophy. This would include symbols and colors used on the HMI, how audible or visible notifications are made, how alarms are acknowledged and cleared, and how alarm logs are saved for long-term data storage.

E) Implementation is the programming and configuration work done to make the alarm management plan operational.

F) Operation is when the alarm system is functioning on an active process.

G) Maintenance is the work required to keep the alarm system functioning.

TJC and ASSOCIATES, Inc.

Proactive Alarm Management

H) Monitoring and Assessment is the process of continuously monitoring the alarm system and ensuring it meets the goals defined in the Alarm Philosophy. This is the stage that allows for evaluation of alarms and identification of problems such as alarm storms, nuisance alarms, chattering, and faulty design logic.

I) Management of Change defines the process for correcting issues found during Monitoring and Assessment.

J) Audit is a periodic review of the performance of the alarm system and the alarm management process. Audits include an intentional review of alarm logs and operator responses to ensure that the alarm management system is meeting the goals of the agency.

As part of the rationalization process, we typically define four levels of alarm priorities:

1) Critical – Alarms that require immediate operator response (within 5 minutes) due to personnel life-safety, impending water quality violation, or impending serious equipment damage.

2) High – Alarms that require a rapid operator response (within 30 minutes) due to treatment process upsets that may lead to eventual water quality violations, major process equipment or systems failure, or equipment failure with no available redundancy.

3) Medium – Alarms that require a moderate operator or maintenance technician response (within 2 hours) due to equipment failure, diagnostic alarms, or process conditions that are outside of normal conditions but are not causing impending water quality issues.

4) Low – Alarms or diagnostic warnings that can be addressed after 2 or more hours without causing process disruption, water quality issues, or potential equipment damage.

If an operator is used to operating with active alarm conditions, does it increase the likelihood that they will miss a critical alarm condition and fail to respond accordingly?

In a typical system, 5–10% of alarms are Critical, 15–25% are High priority, 30–40% are Medium priority, and 20–30% are Low priority. Many agencies tend to over-prioritize alarms. While this may seem like the more conservative approach, the result can be operator complacency, which may slow their response to a truly critical situation.

Another important part of rationalization that isn’t always well thought out is designed suppression. Most modern SCADA packages include alarm generation functions, such as when a value exceeds a setpoint or when two Boolean values are in a specific state, but I always recommend that alarms be generated in the process control logic (programmable logic controller or programmable automation controller). This allows the programmer to include alarm suppression logic that prevents an alarm from becoming

Proactive Alarm Management

active if monitoring of that point isn't necessary due to other operating factors. For example, if a filter is offline, operators don't need to be notified if the filter's effluent turbidimeter rises above the high alarm setpoint.

I recently visited a water treatment facility that was only staffed for 8 hours per day. Intrusion switches were installed on all the exterior doors and the intrusion alarms were assigned critical priority at the SCADA system. That would have made sense to prevent unauthorized access to the facility, except that their normal operating procedure was to open all the doors when they arrived in the morning and close them when they left for the evening. By suppressing the intrusion alarms except for off hours, they could have eliminated seven critical alarms from their normal operating conditions.

Designed suppression can also be used to prevent alarm storms, which occur when a single event triggers multiple alarm conditions. A good illustration of this is when a SCADA system loses communication to a remote PLC. This could cause every point that is monitored from that PLC to go into a communication failure alarm condition. A well-designed system will issue a single PLC communication failure alarm and suppress the communication failure alarms for the individual points.

Manual maintenance suppression is another feature that should be included in alarm management process. This allows maintenance technicians to either take equipment out of service while it is under repair, or temporarily (for a limited time) disable alarms while an instrument is being calibrated or replaced.

The assessment and audit portions of the alarm management plan are almost always neglected. Once a project is completed, most agencies stick with whatever was designed by the engineer and implemented by the integrator and never look back. This is a crucial mistake. Monitoring and assessment should be an integral part of the startup and commissioning process and it should continue during the months after a new process is installed. For new systems, an alarm management audit should be performed at least quarterly. For well-established systems, a yearly audit is sufficient.

The alarm system audit process should review alarm logs and responses, eliminate nuisance alarms and alarm storms, determine where additional designed suppression is necessary, and streamline the alarm and response procedures so that the alarm management system becomes a useful tool instead of a continual annoyance.

The goal of the alarm management system must be to provide operators and maintenance personnel with clear and actionable information to respond to process upsets and equipment

The TJCAA Quarterly

spring 2023

www.tjcaa.com

Proactive Alarm Management

failures. If the assessment and audit of the alarm management system become part of the culture and process, that goal can be attained. Displays full of abnormal conditions should not be a normal operating mode.

As consultants, TJCAA engineers focus on philosophy, identification, and rationalization. In our role as programmers, we focus on detailed design and implementation. Unfortunately, we rarely have the opportunity to participate in the assessment and audit process. Because this is where alarm management is optimized, we would like to change that. If your SCADA system has an overly colorful alarm summary display, give us a call. We can help!

Michael Erwin, P.E. who heads up TJCAA's Control Systems Programming group, has been building valuable experience since 1986 in the design, implementation, and management of electrical power, control, automation, and instrumentation systems. He performs electrical design engineering for water and wastewater treatment facilities, collection and distribution systems, and industrial facilities, focusing on instrumentation and control system design and programming. His specific experience includes development of power calculations, protective device coordination, equipment specification, instrument selection, and control panel fabrication design; design of SCADA systems for in-plant and telemetry-based systems; and PLC programming.

p: 925.357.2676

www.tjcaa.com