2016 ISA WWAC Symposium

Alarm Management and Reliable Architecture Needed for Utility-wide SCADA Systems

Achieving Effectiveness, High Availability, Subsystem Autonomy, and Centralized Administration

Alan Hudson[1]*

[1]Trihedral Engineering Limited, Suite 400, 1160 Bedford Hwy, Bedford, NS B4A1C1

Trihedral, Inc., 7380 Sand Lake Rd, Ste 160, Orlando FL 32819
*Email: alan.hudson@trihedral.com; Birmingham AL; cell 205-612-6665

KEYWORDS

Utilities, Water, Wastewater, SCADA, Alarm Management, SCADA Architecture, ISA 18.2, Operations

ABSTRACT

Notifying operations personnel of alarm conditions remains the single most important function of a water and/or wastewater SCADA system; more specifically, SCADA's primary purpose is to facilitate an understanding of alarm condition such that operations personnel can respond efficiently and effectively. In small SCADA implementations with few assets, few alarm conditions and few operations personnel, alarms management is relatively straightforward. Today's SCADA systems, however, are evolving beyond the monitoring of standalone process, plant or remote asset network. The utility-wide SCADA system has emerged as a central administration hub with distributed sub-systems, each responsible for their own assets.

Utility-wide SCADA provides numerous benefits ranging from centralized security management and configuration to operational standardization and large-scale decision-making. However, the importance of alarm management remains paramount. Indeed, the creation of a centralized architecture allows alarms at the sub-systems to be managed from a utility perspective, in regards prioritization, responsibility allocation, consistency, and data analysis. Key industry standards provide important direction in the establishment of alarm policy, and these standards can be applied at a utility-wide level.

While standards help implement best practice, a reliable, scalable and fail-safe SCADA architecture provides the structure required to make utility-wide SCADA systems successful. A solid, client/server architecture and well-designed redundancy scheme allows the alarm system to support real-time alarm synchronization throughout the network, with seamless fail-over and recovery of autonomous sub-system operations.

This paper explores the SCADA functionality required to support large-scale alarms management by applying industry standards and good network architecture techniques in utility-wide SCADA buildouts.

SCADA SYSTEMS: INHERENTLY COMPLEX, CRITICALLY IMPORTANT

Supervisory Control and Data Acquisition (SCADA) Systems are inherently complex. Even the small systems have complexities. We can all accept that fact but they haven't always been that way. The SCADA systems of today have an ever-increasing number of connected PLCs and definite purpose controllers, "smart" instrumentation and electrical components, communication protocols and physical mediums, software-to-software and user interfaces, and most recently, physical and cyber security considerations, all of which have significantly impacted the evolution of SCADA. Additionally, most utilities are tasked with a growing list of monitoring requirements as a result of population growth and environmental regulations. The population growth has led to an increase in demand for public services and municipal accountability while still meeting the needs for increased water availability, distribution, wastewater collections, and the treatment of both. While population gains usually result in increased tax revenues, the geographically expanding infrastructure often exceeds the additional revenues resulting in a greater emphasis on monitoring and controlling the municipality's largest energy assets. Further, the municipality's customers expect a higher level of service than ever before, requiring always-on services and guaranteed availability.

In the past, a municipality simply had to turn on pumps, manage the purification processes necessary, and provide water to their customers. Collections and severe weather events were handled according to procedures. Reports were filled out appropriately and the cycle continued. Today's "media at your fingertips" social environment has placed a lot of pressure on municipalities to manage their assets effectively and "under the radar" of potentially unfair public scrutiny. When combined with every municipality's strained personnel resources, it's easy to see why SCADA Systems have become critically important.

UNDERSTANDING THE PURPOSE OF ALARM SYSTEMS

It wasn't too many years ago that smaller municipalities depended upon the public to keep them informed about the status of their system. Here's how some systems operated before the implemented SCADA or telemetry: If water started running out of the overflow pipe on the elevated tank, the closest neighbor would call and let them know that their garden was sufficiently watered and their driveway was being washed away. If the water had a discoloration or an odor, a customer would call and let them know that it looked terrible or smelled bad. If the lift station pumps failed to start, a passerby would call and let them know that the red light was blinking and if they didn't do something soon, there would be sewage running into the creek. If an operator on his rounds noticed the turbidity reading was high, he would take appropriate action before it affected the output of the clearwell. And periodically, samples were taken, tests were run, and measurements were recorded for the reports that had to be filed.

Chart recorders and "tone telemetry" provided tremendous improvements for the recording of historical data and providing a place for conscientious operators to recorders anomalies in their system. Sometimes they recorded outside events that affected the system. Sometimes they recorded equipment failures. Sometimes they were working so diligently to fix the problem that nothing was recorded. If the conditions reached critical conditions, an alarm horn would go off and someone would press the Silence or

Acknowledge button. Maybe it would go off again, and maybe it wouldn't. It wasn't that they were being malicious, it's just that they were busy fixing the problem or taking care of the system.

As alarm systems progressed, especially with the evolution of computer-based systems, a semi-permanent record of alarms was created. As long as there was a good printer ribbon in the dot-matrix printer, the alarms were recorded. If a series of alarms occurred on a Saturday afternoon, the operations managers could come in on Monday and see the progression of events. Then they could meet with the technicians and determine with equipment needed to be checked, verified, calibrated, repaired, or replaced.

By the mid-1990s, however, PC-based SCADA systems had progressed to a point that Alarm Event Historians were considered beneficial to the operations of a system and not a nuisance. Sure, it was still possible to suppress the alarms or acknowledge them with fixing them, but now there was a "software record" that was considered reliable. Although the system was a "flat" record of the alarms, it allowed operations to better understand what happened, how to fix it, and prepare a strategy to minimize it from happening again. These advancements transformed the operations of the system.

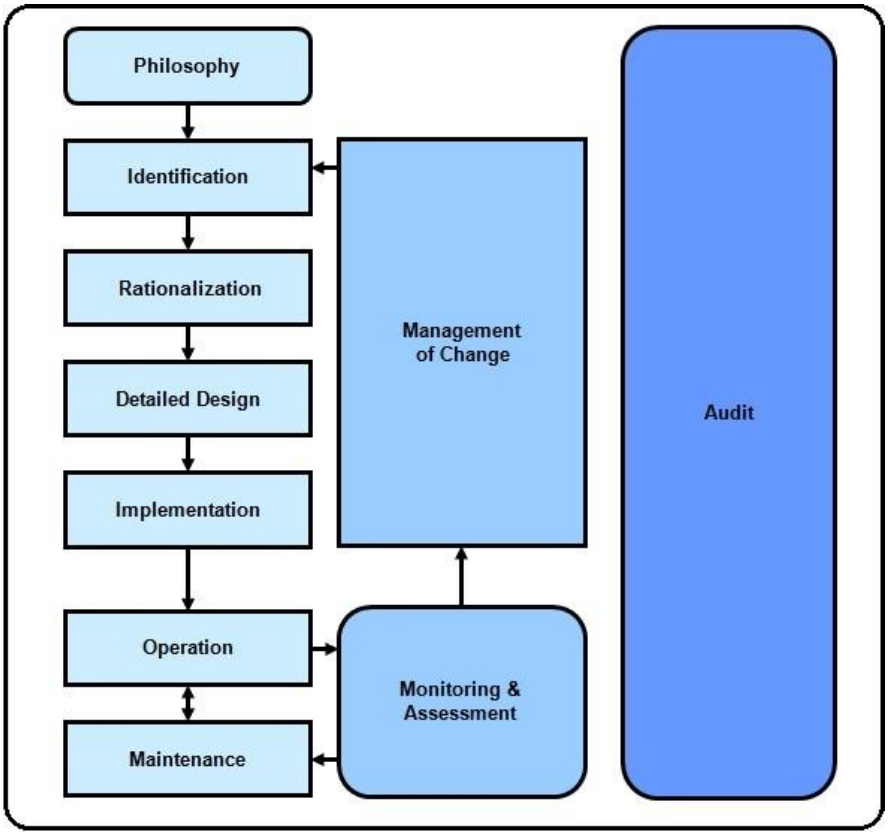
Thankfully, computer technology has continued to improve and software technology has continued to progress. With the help and feedback from operations and management personnel, systems have evolved such that alarm configuration and management developed areas of standardization. Efforts from dedicated professionals resulted in publications like the ISA-18.2 Standard which provides the framework for successful design, implementation, operation, and management of alarm systems. This Standard has become universal for process systems and can be easily applied to water wastewater systems.

So, while the alarm "horn and light" systems of the past decades were needed make quick control changes, and the purpose of legacy computer-based alarm systems was to add "alarm history recording" functionality, today's alarm systems now provide valuable insight into the health of individual autonomous systems as well as the system as a whole. Therefore, considering the alarm system as an operational component will provide for effective and efficient analysis and decision making.

KEY INDUSTRY STANDARDS

In 2009, an alarm system framework was released that was the culmination of over six years of hard work by a group of alarm and process experts. This framework, referred to as ISA-18.2, is built on the work of other standards and guidelines that included EEMUA 191, NAMUR NA 102, and ASM. The conclusion was that alarm management is a continual life-cycle process. Consequently, ISA-18.2 is an RAGAGEP – a Recognized and Generally Accepted Good Engineering Practice – that should be considered a foundation of an alarm system for most process industries. It is interesting to note that while Water Wastewater was not one of the expressed target industries, Water Wastewater has been deliberate in adopting this standard and realizing the importance of these alarm management principles.

While this paper is not intended to be a discussion of the ISA-18.2 standard, we must consider these standards when contemplating alarm management in a utility-wide system. There is an abundance of ISA-18.2 information available on public forums including the ISA website.



Source: International Society of Automation. (2009). ANSI/ISA-18.2-2009 - Management of Alarm Systems for the Process Industries; Research Triangle Park: ISA

One of the benefits of this standard are the philosophies regarding alarms. Some of the key alarm issues addressed in the ISA-18.2 standard are:

Alarm Definitions	Alarm Priority definitions
Alarm Requirements	Alarm Shelving and suppression rules
Alarm Roles	Alarm System monitoring requirements
Alarm Rationalizations	Alarm Change management
Alarm Class definition / design	Alarm Training

CENTRALIZED ARCHITECTURE, LOCAL AUTONOMY

Perhaps the most difficult concept to grasp and implement is that of a central administration hub with distributed sub-systems, each responsible for their own assets. While the industry seems to do this today, what it often lacks is a centralized architecture which allows alarms at the sub-systems level to be managed from a utility perspective in regards to prioritization, responsibility allocation, consistency, and data analysis. What this really highlights is the critically important planning and preparation phase of design where the key partners and beneficiaries meet to discuss priorities, interconnectivities, and cause/effect.

These discussions must go far beyond the "status quo, industry norm" of alarm and operations management and reach for excellence by examining "industry best practices" throughout all industries, not just water wastewater.

- Involve the appropriate stakeholders so that the system will be solid at all levels.
- Seek outside assistance so everyone is clear on the fundamentals of alarm management and how it applies to water wastewater.
- Define performance expectations and metrics, potential difficulties and obstacles. Draft, edit, and review as necessary.
- After conditions occur and performance has been tested, review the process and make necessary adjustments.

THE US MILITARY

In some ways, this idea of Centralized Architecture with Local Autonomy is similar to the US military. The US military is divided appropriately between different, independent branches with unique intentions, ambitions, and leadership structures with a centralized governance, coordination, and unified mission. While it's true that our military is incredibly and increasingly advanced technologically, the real success of the US military is that the Army, Navy, Air Force, Marines, and Coast Guard have a clear mission. This mission is true whether the lines of communication are intact or whether they are temporarily interrupted.

During times of peace, the centralized leadership spends a lot of time exploring many various scenarios based on many different possibilities. Even if the scenarios seem far-fetched and improbable, they consider them anyway. Along with Branch leadership, they develop detailed plans with built-in contingencies. The plans are often cross-functional with the other branches and depend upon their implementation and execution in order to be completely successful. The plans always include distributed leadership so that plans can be carried out autonomously. The plans are put in place and practiced accordingly so that once an issue occurs, they can respond.

When in a situation of heightened security, each Branch goes into action. And quickly. If centralized communication is available, the plan can be carried out with optimal execution. But what about when communications are severed? The plan continues as designed but without constant reporting or oversight. And when conditions occur that were "outside the plan", there is complete confidence in the Branch (or unit, platoon, crew, or individual) that they will perform in accordance in the directives and objectives indicated in the "Plan". When normal conditions resume, the Branches report back and shares its information, actions, difficulties, revisions, etc. The newly synchronized content allows for a complete record to be determined and for the leadership to address obstacles, overcome difficulties, and make necessary revisions.

While we are not the United States military, we are responsible for delivering the world's most precious resource in a safe and reliable manner. Uninterrupted service is imperative. The same is true for wastewater. Safe, reliable, uninterrupted service is expected. In a small system, this process may seem

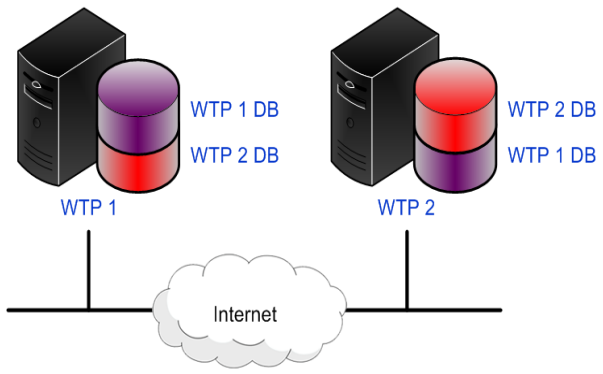
straightforward. In larger, more complex systems, the comparison is even more appropriate. The Water Wastewater industry must approach this with the same attention, importance, and passion that the US approaches its military.

SCADA SYSTEM HISTORIAN AND ALARM ARCHITECTURE

A reliable, scalable and fail-safe SCADA architecture is what makes a utility-wide SCADA system successful. The system must include a solid, client/server architecture and a well-designed redundancy scheme. The data historian needs to be distributed with central connectivity and synchronization. The more difficult aspect is having an alarm system that supports real-time alarm synchronization throughout the network, with seamless fail-over and recovery of autonomous sub-system operations. Some systems share redundancy responsibilities while others have multiple backup schemes. The key is to have one that is reliable, scalable and fail-safe. If communication is interrupted, the re-synchronization ability must be solid.

Here are a few examples of actual systems and their architecture.

Example 1:

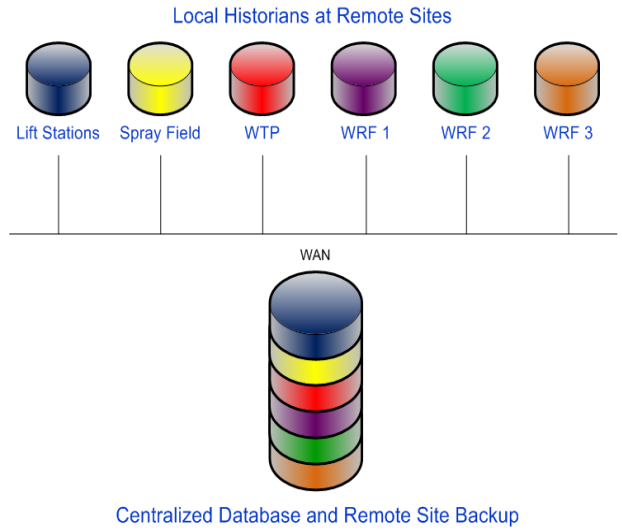


Example 1: Single SCADA application with distributed alarms / historians filtered by function and centralized backup.

WTP1 includes a historical database, which is used for primary storage of local data and backup storage of data from WTP2. Conversely, WTP2 includes a 2nd historical database, which is used for primary storage of local data and backup storage of data from WTP2.

Both databases are synchronized in real-time across an Internet connection using a secure VPN tunnel. If either database is unavailable, the historian still continues to store all data in the remaining database. When the 'outage' database is returned to service, a comparison is done on the database to determine if any data is missing and this data is backfilled.

Example 2

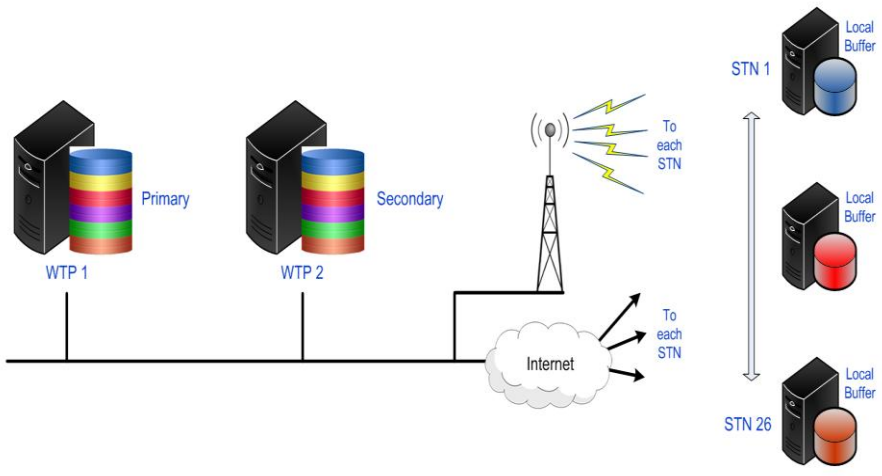


Example 2: Single SCADA application with distributed alarms / historians filtered by function and centralized backup.

This application includes six functionally separate SCADA systems combined into a single, unified SCADA application connected via a self-healing fiber ring network. A unified SCADA approach allows each functional area has its own local historian which only logs data and alarms from the local process. In this application, the lift station SCADA server, geographically separated in a different part of the utility complex, is oversized to provide a backup storage location for all six historical and alarm databases.

In the event the backup storage is unavailable, the Historian can still service all data requests by dividing the requests into subparts and requesting the subparts from each of the geographically separated databases.

Example 3



Example 3: Centralized redundancy with local data buffering at remote stations.

This application uses a report-by-exception scheme to report data and alarms from 26 remote sites and record it to a pair of collocated historical databases located in the central control room. The Historian directs data storage, synchronization services and bi-directional data backfill between the databases.

PLAN & PREPARE, IMPLEMENT & EXECUTE, REVIEW & REPEAT

While some SCADA architectures may be complex, elaborate, and widely-differing, every SCADA system's "Alarm Mission" is the same: Provide for efficient and effective alarm management by applying industry standards and solid network architecture techniques in utility-wide SCADA build-outs.

Defining "the Mission" sounds simple but is actually difficult because it takes a lot of planning and preparation. The design and implementation of most alarm management systems is left up to the consultant engineers to design an alarm system and the system integrators to implement what has been specified. It's not that the design or implementation is bad, but all too often it doesn't meet the ultimate needs. The needs are only uncovered and addressed when the appropriate stakeholders are involved in the process and take ownership of the results.

Here is the process:

Plan & Prepare

- Plan and Prepare for success by focusing on the desired results
- Take the time necessary to plan properly
- Involve key stakeholders and outside resources
- Determine differences between Central Administration and Local Autonomy, and their respective actions, and the consequences

Implement & Execute

- Invest in technologies and the necessary infrastructure to make the plan succeed
- Publish "The Mission" and include key metrics, success factors, and acceptable behaviors
- Train personnel to analyze and execute with local autonomy through the viewpoint of central administration responsibility

Review & Repeat

- Review and simulate while conditions are normal
- Review after conditions have been upset and the procedure tested
- Develop a mindset of continual improvement

SUMMARY

The utility-wide SCADA systems continue to emerge and develop as centralized administration hubs with distributed sub-systems where each sub-system is responsible for their own assets and for the actions taken as process disruptions occur. The single most important function of a Water Wastewater SCADA system is to notify operations personnel of alarm conditions so that operations personnel can respond efficiently and effectively.

Further, the creation of a centralized architecture allows alarms at the sub-systems to be managed from a utility perspective in regards to prioritization, responsibility allocation, consistency, and data analysis. Key industry standards provide important direction in the establishment of alarm policy, and these standards can be applied at a utility-wide level.

While standards help implement best practice, a reliable, scalable and fail-safe SCADA architecture provides the structure required to make utility-wide SCADA systems successful. A solid, client/server architecture and well-designed redundancy scheme allows the alarm system to support real-time alarm synchronization throughout the network, with seamless fail-over and recovery of autonomous sub-system operations.

The keys to a successful Alarm Management System can be summed up in three steps: Planning & Preparation, Implementation & Execution, and Continual Review & Improvement. If proper attention is given to these three steps, Alarm Management Success can be achieved.

ABOUT THE AUTHOR

Alan Hudson is US Sales Manager for Trihedral Engineering. Alan holds degrees in Mathematics from Samford University and Electrical Engineering from Auburn University and has been in the water wastewater segment for 26 years with experience in engineering, consultative design, programming, and system integration.

Contact: alan.hudson@trihedral.com