Meeting NERC Change Control Requirements for HMI/SCADA and Control Systems

Meeting NERC Change Control Requirements for HMI/SCADA and Control Systems

Overview

There is a lot of attention on NERC and the effect its reliability standards will have on the power industry in North America. In March 2007, the Federal Energy Regulatory Commission (FERC) approved 83 NERC (North American Electric Reliability Corporation) legally enforceable standards for U.S. bulk power systems. Historically, these standards have been voluntary; however, in June 2007, compliance with these standards became mandatory and enforceable. With auditable compliance commencing in 2010, it is necessary for companies to get systems and solutions in place to provide the necessary one year of documentation.

The NERC reliability standards are intended to define the functions needed to ensure that bulk electrical systems operate reliably. These include Resource and Demand Balancing, Communications, Critical Infrastructure Protection, Emergency Preparedness, Facilities Design, Transmission Operations, and more (for a complete list, refer to www.nerc.com). NERC's role is to provide three key activities: compliance monitoring, compliance enforcement and due process.

NERC's standards for Critical Infrastructure Protection (CIP) apply to various critical assets, and this paper aims to demonstrate how Change Control principles can help protect two specific asset types: SCADA (Supervisory, Control and Data Acquisition) and control systems.

Critical Infrastructure Protection

CIP standards focus on identifying, documenting, securing and managing key assets related to the operation of bulk electric systems to ensure reliability. Key sections of CIP include:

- CIP 002 – Critical Cyber Asset Identification. Requires identifying and documenting the critical assets that are associated with the reliable operation of the bulk electric system through risk-based assessments.
- CIP 003 – Security Management Controls. Ensures that minimum security management controls are in place to protect the identified critical assets.
- CIP 004 – Personnel and Training. Requires that personnel have authorized cyber or physical access to the critical assets as well as the appropriate level of training and security.
- CIP 005 – Electronic Security Perimeter(s). Identification and protection of the electronic perimeters for the critical assets.
- CIP 006 – Physical Security of Critical Cyber Assets. Defining, documenting and monitoring security and access to the critical assets.
- CIP 007 – Systems Security Management. Definition of the methods, processes and procedures for securing the critical and non-critical cyber assets.
- CIP 008 – Incident Reporting and Response Planning. Identification, classification, response and reporting of incidents to the critical assets.
- CIP 009 – Recovery Plans for Critical Cyber Assets. Ensures that plans are in place for the recovery of critical assets.

There are certainly many steps involved in meeting these CIP requirements. The obvious starting point is CIP 002—the identification of critical assets, as those assets will be the focus of the subsequent standards.

Cyber Security, SCADA and Control Systems

SCADA and control systems are an essential part of delivering electricity. Control systems such as DCS and PLC systems allow operators to control a power plant, and SCADA systems are widely used to control and monitor the distribution of power. As such, many of these systems would be considered critical assets—falling under the CIP standards.

Modern versions of these systems are typically highly networked and run on Windows® or Unix systems—making them vulnerable to the same threats such as viruses or hackers, as other computer systems. NERC has put forth the CIP standards to protect these systems against such cyber threats.

In addition to cyber threats from external sources, it is also essential to protect from internal threats, which are typically not by malicious intent, but rather from a lack of procedures, human errors, poor documentation and communication. As a result, key elements of CIP 003 are change control and configuration management.

What Is Change Control?

Change control is a process by which changes to an asset are only modified in a controlled manner. Change control can be applied to each of the project lifecycle steps, which have varying levels of importance, and will be discussed later in the paper. Configuration management involves identifying the configuration, establishing change control on it, knowing the status and auditing the resulting changes. In this paper, we'll refer to the entire process as change control.

One way to establish a change control process is by implementing a standardized process along with an automated system, such as GE Change Management software. When evaluating change control software, you want to consider both the core functionality as well as any extended/optional capabilities the software delivers to ensure it fits into your overall process and helps protect your critical automation assets per the NERC CIP standards.

Components of Change Control Software

Typical change control solutions are built in a modular fashion to accommodate progressive inclusion into standard operating procedures and for flexibility across market segments. The core software components required are a data management engine and an end user interface client; these two components deliver the following core functionality:

Security (access control)

Being able to monitor and control who has access to what critical asset is key because it can help reduce errors that occur due to unauthorized access. If something unexpected happens, management can easily determine who made a change and whether or not they were authorized to do so. Your permissions hierarchy should be set up in a role-based fashion. For example, only the engineering staff may modify process system screens; only supervisors may create a new SCADA screen; or technicians may view but not change process screen parameters. Role-based hierarchies are more efficient, eliminating the need to establish permissions for every employee.

Version control

It is imperative to ensure that only one person at a time is making changes and that versions are archived as changes are made. For example, if an engineer is making a modification to an existing SCADA screen, a change control system will keep track of all previous versions of that screen as well as the current rendering. To make a change in that screen, the engineer goes through a "check-out" process, which releases the current version of that screen from the server; files, thus, are maintained centrally. The engineer works on the screen, saves the changes, and then checks the file back into the system; the "check-in" process creates a new version and marks it as the current one.

Among the benefits of version control is the ability to revert back to a previous version, if needed. If a change is made inadvertently and the alteration disrupts the application, a record is available of what happened and of the previous version—providing the means for disaster recovery. Additionally, version control includes the core capability to provide an audit trail of who, what, when, where and why the changes were made.

Extended capabilities that go beyond the core functionality are optional and allow users to further automate their change management process. These extension modules can significantly enhance the software system's value but may not be available in all software sets. Therefore, you want to assess which capabilities are critical to you and ensure they are offered in the change control software you select. Typical extension modules are:

Scheduler

Providing the capability to automatically back up on a regularly scheduled basis, this module enables the software to connect and back up the devices code, files and/or settings based on a user-defined frequency such as hourly, daily, weekly, etc. More advanced schedulers can perform incremental backups by reading the automation program, files or code and comparing for differences, and then making a backup if changes are detected.

Automatic Change Detection

This module enables the device to automatically trigger a backup based on any change at any time, independent of the scheduler module. Some devices can trigger a backup once the device is placed in a certain mode (i.e., development/program mode), which will preemptively capture a backup. This functionality is specific to devices, and device support will vary by software provider.

Change Detection Details

Providing an in-depth report on the changes made in the devices code, program or settings, this module will highlight changes down to the rung or line of code and provide the user with a report that captures the previous backup and current code. Device support for this module varies by software provider, as it requires in-depth knowledge of the device's core programming structure; many device manufacturers consider this knowledge proprietary intellectual property. However, with more and more device manufacturers supporting open standards such as IEC 1131, independent software providers can provide such functionality, which ultimately aids in reducing the time required to identify the cause of the problem.

Notification

As changes to critical assets can affect other systems, it is important to appropriately notify users or third-party software that an action has occurred. Actions can be system or user invoked and typically trigger instant emails, text messages and/or pages; or they are simply logged and sent on a predetermined interval such as the end of a shift.

Actions can be simple like a change in a program, a "check in" or "check out" of an asset file, a backup failure, a security breach, etc. They may also be complex actions like a change to a particular element within the program, the presence of a manual force or repeated security breaches. With many of today's notification options now including scripting engines, escalation schemes with on/off shift blocking, users can create fully custom notification rule sets to match their business needs.

Meeting NERC Change Control Requirements for HMI/SCADA and Control Systems

Enhanced Security

Enhanced security options are typically categorized into two sections:

- Electronic Signature – This introduces additional control over changes in your plant by allowing you to enforce authorization to make changes to your devices and projects and prevent runtime changes. Electronic signature is essential in many industries and helps customers meet regulatory compliance requirements such as 21 CFR Part 11 and NERC. Users in unregulated environments are also adopting electronic signature capabilities to improve accountability and meet self-imposed Good Manufacturing Practices.
- Lockout - This introduces the ability to lock out edits on specific devices based on a re-occurring or ad hoc schedule. This is typically used by facilities running a process where slight alterations to the devices could affect the product and/or create an unsafe system.

Graphical Interface(s)

The HTML or graphical plant layout option allows you to customize the end-user interface to match your plant's needs. These point-and-click interfaces can be thick or thin client based, and the main benefit is that it opens the application up to a wider variety of users by enabling easier system access, comparative to surfing the internet. It also allows users to simplify the interface based on end-user roles—giving them access only to what they need—thus reducing user errors, support calls and the learning curve associated with complex interfaces.

Scripting Interface(s)

With open and layered products, this developer-based option is typically offered and can expand the system outside its core functionality. End users may want to customize the existing elements, add another step in a standard function or augment the system's off-the-shelf capabilities. To do this, the option typically exposes an API into the development environment, which enables any type of customization.

Third-Party Support

Enabling the change management system to connect to floor devices, this capability is a must-have component for many of today's facilities and plants that have a wide range of devices built and engineered by different manufacturers such as GE, Siemens, Allen Bradley, Wonderware and others. Some software providers also have advanced third-party support, which allows compatibility with almost any file-based product with pre-configurations—saving setup and deployment time.

Examples of How Change Control Addresses CIP

In the NERC standards, CIP 003 clearly calls for change control and configuration management. Considering that all of the elements have a documentation aspect, a change control process or system can help you manage the documentation that is created as a result.

For example, when you identify and document the critical assets for CIP 002, the documentation should be managed by establishing a change control process; this is beneficial because as critical assets are added, removed or modified, an evidence of change is tracked. CIP 007 also requires that changes resulting from the modifications to the security system and control be documented.

CIP 009, which is geared toward recovery plans for critical assets, requires documentation as well. As most control systems and SCADA are running logic that needs to be reloaded in those systems, it is important to maintain a version control system to keep track of the versions of logic in a central location—enabling recovery of the running logic in the event of an emergency, large or small. Change control software ensures that the approved version of that configuration is always available.

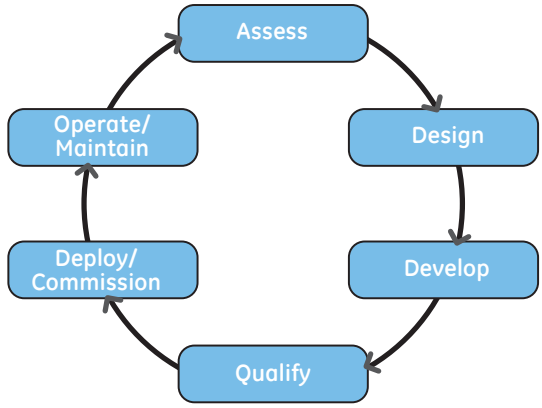
It's important to note that not all aspects of change control need to be automated by a software system, and since change control software is typically modular, many companies choose to phase it in over a period of time—ensuring that the new process becomes part of standard operating procedures and allowing personnel to absorb and embrace the changes progressively.

Making It Happen

Implementing change control software is the best way to ensure a change control process is followed, but will only be successful if integrated with your standard operating procedures and supported from the organization top down. Implementation has to involve many facets of the organization and is successful only if the project is led by an operations management group that is focused on floor level ownership, else the software will be ineffective and usage will degrade over time, resulting in NERC non-compliance.

Some industries such as life sciences already have this organizational culture in place, having been regulated by the FDA for a significant time, which makes implementing a change control process and software a more natural extension. But many companies—for example, those in industries such as energy where regulations are still very new—have not established such a culture.

Regardless of organizational culture, companies can start by mapping out existing manual or informal processes to identify areas for improvement. By assessing, adapting and automating those, you can begin to establish the type of change control culture necessary for success. The following describes the typical project life cycle phases and how change control software fits in each step:



Assess

Change control software in this phase provides the ability to manage your project documents, code, configuration and programs. This results in traceability on your design decisions and a better way to collaborate using a central storage location.

Design/Develop

During these stages, the software provides version control to ensure work is being done on the current plan and that only one person at a time is making changes. With some more advanced change control software packages, a single project can be shared between developers by allowing checkouts at the screen/element level—saving time and avoiding duplication of effort or even deconstruction of effort.

Qualify/Deploy/Commission

In this phase, as a system is being installed, the software captures changes and ensures careful control of modifications—recording details for future recall—resulting in reduced development and deployment times. To fully understand the benefit in this phase, one has to experience a rework or data loss situation.

Operate & Maintain

This component is where adopters will see the most value in change control software, as it ensures the storage of the latest information and backups in a central location with change history and audit records—an area NERC auditors will focus. Maintenance personnel can more easily troubleshoot issues and keep the systems running efficiently. In addition to meeting NERC compliance, using the software in this phase helps reduce downtime and delivers soft benefits like accountability, process adherence and secured access.

Business Benefits

When deploying a change control process or system for NERC, consider the advantages it can bring to your overall operations, including your personnel and processes. Implementing change control makes sense from a business perspective by enabling reduced cost of ownership and shorter time to solution. It offers an automated way to help your organization assess, monitor, manage, control—and lower—project costs as well as ongoing maintenance costs. In addition, by providing traceability and notification of changes, it drives increased efficiency of your personnel, and as a result, your productivity.

Conclusion

There are no magic bullets to meeting NERC standards, and we can expect the standards to change over time. As companies establish methods to meet evolving standards, new best practices will emerge, and the bar by which compliance is measured will be raised. Establishing a strong process and improving it over time will help you meet these standards today and in the future while increasing the efficiency of your personnel and overall operations—providing your business with a sustainable competitive advantage for long-term success.

About GE
GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry. www.ge.com

Contact information
Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

www.ge.com/digital