SANS | Research Program

White Paper

ICS Security and Management of Change: Risks and Resilience

Written by **Jason Dely**

March 2025

HEXAGON

Introduction

The core activities of industrial operations involve the use of physical equipment that is designed and built to meet the specific needs of customers. This equipment is custom-built based on detailed specifications, using a combination of readily available, ready-to-build, and custom-crafted components. The availability and variety of these components can differ significantly across industrial control system (ICS) sectors, directly influencing recovery times after a failure. The operating tolerances built into these physical systems and their components are crucial to the overall quality, integrity, and performance of the final system, as well as the business functions they support. The selection of accompanying cyber components, such as automation, instrumentation, software, and infrastructure components, are designed and implemented to support these tolerances. Considerable implementation, testing, and ongoing management efforts are undertaken to ensure both the cyber and the physical components are aligned with their operational needs. This effort covers the essential functions of ICS operations, including process control, process monitoring, data acquisition, and functional safety.[1] This paper focuses on using management of change to control and monitor changes to the cyber assets within an ICS, highlighting the benefits it offers in enhancing cybersecurity. It emphasizes the importance of understanding ICS risks related to unapproved, unexpected, and unmonitored changes, considering the potential cyber-related impacts and consequences on physical operations.

The notion that changes do not occur within an ICS is not entirely true. What is true is that uncontrolled and unrecoverable changes can be detrimental to running a safe and stable operation. This becomes reasonable when we consider the level of complexities, high dependency on automation, and minimal human interactions and validation of all decisions made by the control systems. When a control system is functioning effectively, the prospect of implementing any change introduces uncertainty. Whether formal or informal, the approach should include first reviewing the justification for the change. In some cases, this step will prevent moving forward, and, as such, the catalyst for change can either become an operational procedure addressed by personnel or be left as-is without intervention. This step is only as good as the information, knowledge, and understanding going into this risk/benefit discussion. The relevance and resistance to justification should not be understated as most operations teams would rather not have to make a change because of the potential issues that can arise.

If justification is determined, the next step is to put together a plan that involves evaluation, testing, and approval. The time and depth of effort for each opportunity of change will vary widely, so an argument can be made for the need for both a formal and informal process. Changes can range from simple adjustments, like modifying a value in a loop control or a valve postion as part of daily operations, to more significant alterations, such as a small modification to a single line of code in a running programmable logic controller (PLC). Changes can also be much larger in scope, such as upgrading firmware or implementing a new function. Knowing where to allow or enforce a formal or informal process is important, but what really matters is being able to actively document, track, and monitor these systems for change with the ability to revert as required.

[1] https://www.tuvsud.com/en-us/services/functional-safety/about

ICS Changes

There is a common trend in the industry where stability of the ICS is directly proportional to time in service. With any new system, in time, operations teams move from supporting the commissioning and working out the bugs to maintaining the system's engineering reliability, resilience, and safety. Figure 1 depicts the trend of the number of changes that occur over time when a new, upgraded ,or expended ICS enters service. Many changes are to be expected when the initial construction stages lead into a Field Acceptance Test (FAT) and Site Acceptance Test (SAT). Once the system enters operational service and begins producing an output, the number of changes reduces significantly over time. There are several factors that determine the length of this time, such as the size and complexities of the process and output. Eventually, after one or two years, the day-to-day activities transition into maintaining the system with few changes that are, ideally, driven by business justifications. During this maintaining phase, processes surrounding change play a pivotal role.

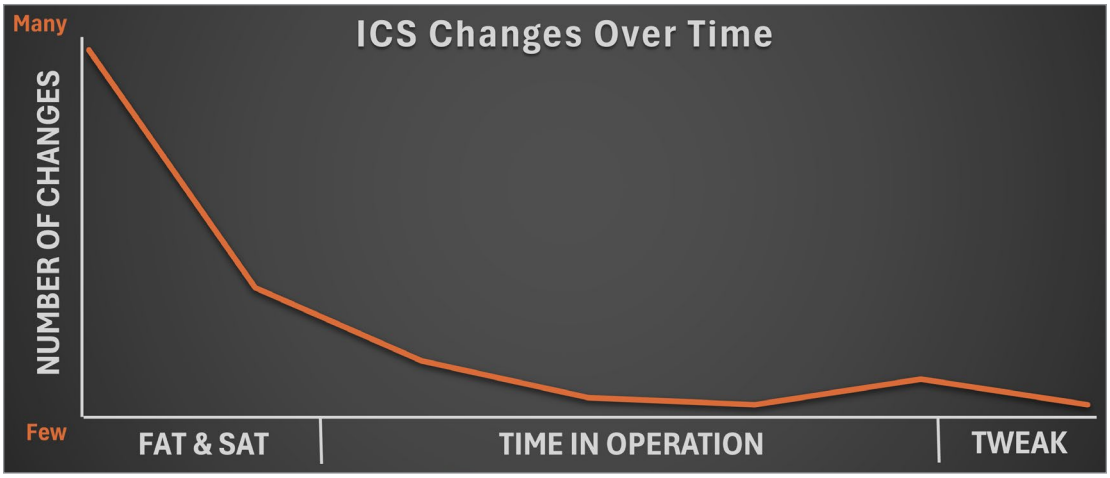

Figure 1. ICS Changes Over Time

There are various types of changes that can be considered with respect to an ICS—some that are easier to specify than others. What is crucial is understanding that each type of change comes with an associated measure of recoverability. This recoverability is determined by what can be performed, provided one or more capabilities exists, to revert that change. Table 1 depicts common types of changes, along with corresponding examples and their recoverability. Understanding how these types of changes can occur on each system is useful when evaluating the readiness of an operations team with respect to how they are equipped to handle impacts and recovery from any form of change.

Table 1. Types of Change and Recoverability

Types of Change	Examples of Change	Recoverability
Expected Change	Operational tweaks, tuning, planned upgrades/projects	Relatively straightforward given changes are appropriately documented and tracked to easily revert change
Unexpected Change	Operational recovery from component break	Difficult without active monitoring and accurate offline backups
Emergency Change	Extended recovery from system failure; Major unplanned event, such as, safety incident or cyber incident	May be straightforward provided documentation and tracking are maintained under duress
Unapproved Change	Invoked, possibly undetected, change that may be a mistake, benevolent, or adversarial	Extremely difficult without active monitoring, tracked changes, and accurate offline backups

Change can introduce various risks to a business's operations. While changes can negatively impact operations, not all changes have consequences significant enough to be considered a business risk. Understanding the full impact of change across the numerous cyber-physical systems can be useful but extremely time-consuming. Many would adopt a macro-level approach to tackle the challenge of determining where and at what level a change process should be implemented. The difficulty arises when changes are not properly tracked, making it challenging to determine if a change contributed to an undesirable process outcome or impact. Care should be taken to ensure that the chosen approach to a change process strikes the right balance in addressing the various types of risks. Table 2 highlights sample impacts and recovery efforts associated with unapproved, unexpected, and unmonitored (tracked) changes categorized by operational and cybersecurity risks. Operationalizing a process around change can help in the prevention, detection, response, and recovery of cyber-related impacts from operational events and cybersecurity events.

Table 2. Impacts from Change

Risk	Impact Category	Impact	Failures
Operational Risks	Quality of service	Missing, or inaccurate, offline file to recover from failed component	**Prevent:** No active offline copies **Detect:** Immediate or delayed process issues **Response:** Extended evaluation without accurate backups **Recover:** Rebuild code or identify changes made from previous version
	Outage: Extended	Emergency product model change due to availability (end-of-life)	**Prevent:** Not monitoring and/or active planning of product EOL **Detect:** No warning, product failure **Response:** Immediate; no replacement **Recover:** Evaluation with increased future issues
	Outage: Unplanned	Incidental inclusion of minimal, unapproved code triggering event	**Prevent:** No proactive change control **Detect:** Immediate or delayed process issues **Response:** Extended testing and evaluation without accurate backups **Recover:** Rebuild code or identify changes made from previous version
	Outage: Significant	Planned inclusion of code that is inaccurate, unvetted, or unapproved triggering major event	**Prevent:** Not monitoring for change **Detect:** Immediate or delayed process issues **Response:** Extended testing and evaluation without accurate backups; possible physical or environmental impact **Recover:** Rebuild code
Cybersecurity Risks	Insider: Malicious intent	Implementation of code for purpose of fraud (e.g., self-assigned overtime)	**Prevent:** Not monitoring for change **Detect:** Overlooked if not aware **Response:** Root cause unknown **Recover:** Extended without accurate backups, rebuild code
	Insider: Sabotage	Disablement or destruction of physical system or environment driven by vengeance	**Prevent:** Not monitoring for change **Detect:** Overlooked if not aware **Response:** Root cause unknown **Recover:** Extended without accurate backups, rebuild code
	Attacker: Ransomware	Modification to code or infrastructure for purpose of extortion	**Prevent:** Not monitoring for change **Detect:** Only if attacker inadvertently makes a mistake **Response:** Root cause unknown **Recover:** Extended without accurate backups, rebuild code
	Attacker: Prepositioning	Modification or infiltration of extremities of the ICS network to establish a beachhead to recon and planning	**Prevent:** Not monitoring for change **Detect:** Only if attacker inadvertently makes a mistake **Response:** Overlooked if not aware **Recover:** Overlooked if not aware
	Attacker: Delivery	Modification to code or infrastructure in preparation of an attack	**Prevent:** Not monitoring for change **Detect:** Only if attacker inadvertently makes a mistake **Response:** Root cause unknown **Recover:** Extended without accurate backups

Managing Change

Management of Change is common in the industry and found across many disciplines. These and other standards help ensure the formal presence and use of controls that limit or remove impacts from process and operational levels of change with respect to quality, safety, and security. This list demonstrates the benefits and reliance the industry already has using management of change to ensure reliability and safety in these critical systems. Given that many systems rely on managing operational and safety risks, it is logical to apply the same formal process to protect these operations. This approach is further emphasized by its inclusion in ICS security standards, such as the ISA/IEC 62443 Series of Standards and NIST Special Publication 800-82 (see Table 3). Utilizing management of change processes benefits ICS security across many activities including, but not limited to, vulnerability management programs, network security monitoring activities, response activities, and recovery activities.

Table 3. Management of Change Standards

Standards	Description
ISA/IEC 62443 Series of Standards	Standards for industrial automation and control systems security, which include change management requirements[2]
NIST Special Publication 800-82	Guide to Industrial Control Systems Security" highlights change management as part of security practices[3]
ANSI/ISA-84.00.01-2004	Functional Safety standards that incorporate change management processes[4]
API RP 1173	Pipeline Safety Management System Requirements, which includes MOC components[5]
OSHA 1910.119	Process Safety Management standard that requires formal MOC for covered processes[6]
ISA-18.2	Management of Alarm Systems for the Process Industries, which addresses change management for HMI alarm systems[7]
API RP 754	Process Safety Performance Indicators for the Refining and Petrochemical Industries (includes MOC metrics)[8]
IEC 61511-1	Functional Safety for the process industry standard that addresses change management in safety instrumented systems[9]

[2] www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[3] https://csrc.nist.gov/pubs/sp/800/82/r3/final

[4] https://webstore.ansi.org/standards/isa/ansiisa8400012004part

[5] https://pipelinesms.org/rp-1173/

[6] www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.119

[7] www.isa.org/intech-home/2016/may-june/departments/isa18-alarm-management-standard-updated

[8] www.api.org/oil-and-natural-gas/health-and-safety/refinery-and-plant-safety/process-safety/process-safety-standards/rp-754

[9] https://webstore.iec.ch/en/publication/24241

Challenges

Managing change within an ICS environment starts with having an accurate inventory of configurable devices. Building a complete and accurate inventory of the cyber assets within an environment is typically difficult to yield more accurate results than performing the same task in a system that has been running for 15 or more years, where maintaining an accurate inventory may not have been a priority. There are several factors to consider when identifying cyber assets in an environment. While most approaches focus on devices that are accessible from the network, these assets are not always, or exclusively, configured through the network. They can also function within isolated networks and still impact the proper operation of both immediate and downstream processes. There are also assets that are used to manage and monitor the system or other assets. For example, configurable handheld instruments can be used to calibrate instrumentation. Additionally, transient devices, such as operations-owned and contractor-owned laptops, can move between environments and between various security zones.

The tools and methods used to identify and catalog discovered assets face additional challenges due to the inconsistent approaches employed in fingerprinting an asset once it's found. Automated mechanisms are only helpful if the service can provide useful information or is available over an extended network. Even the manual approach can be difficult if the label of a device is not visible within the cabinet or if it's inaccurate because a firmware update has been performed at any point. As a result, not all assets are easily discoverable, accurately catalogued, or physically locatable. Multiple approaches and technologies are often required to achieve a comprehensive asset inventory.

For these and other reasons, the inability to identify assets with 100% coverage and accuracy cannot be understated, yet it plays a significant part in identifying, controlling, and tracking change. The approach to asset identification should prioritize the critical systems and process flow, focusing on the components needed to effectively operate each system. Asset identification methods should include physical inspections, online analysis using vendor-approved tools, offline code analysis, and traffic analysis. Extreme caution—or avoidance altogether—should be exercised when selecting and deploying online discovery and identification tools that were not developed by the vendor of the targeted system. It also is important to consider the various indirect supporting assets that can influence reliability, resilience, and safety of the process.

Risks of Change: Impact on Software, Code, and Data

From a cyber perspective on change—aside from the physical change of hardware—the primary elements where change can negatively affect operations include software (including firmware), code (such as programs, configurations, and parameters), and data. An effective operation relies on validating and maintaining current running software and firmware versions. In addition to stable, high-quality hardware, a system that operates reliably and remains free of software bugs, code issues, or cyberattacks will build integrity and foster confidence within the operations team over time. As stated earlier, this integrity is important to the effectiveness of operating physical equipment as the industry operates using a large amount of automation supported by a minimal number of personnel. This is not to argue the integrity benefits of using automation versus personnel, however, if the integrity of an automation system is not established, more personnel costs will need to be incurred to ensure ongoing proper operations. When a system has been operating for many years with the same version of software and firmware, there must be some level of acknowledgement that changing this element may inherently "reset the clock," as it were, on building integrity and confidence of the system over time.

Integrity is important to the effectiveness of operating physical equipment as the industry operates using a large amount of automation supported by a minimal number of personnel.

Although some software may be custom created for a particular environment, code and data are two elements that are most likely unique to a particular operation—even across similar pieces of equipment. Code, as depicted in Figure 2, can be represented in multiple forms and descriptions but is essentially created to serve the intended sequence of operations of a mechanical system. Code that executes incorrectly and data without integrity can cause various types of disruptive or destructive effects to the system. Maintaining integrity in the system requires the ability to track changes between running versions of code and to retain approved offline copies. Offline code is usually associated with a set of initialization data, so this also would need to be tracked and retained with the code version. There are many IT-based solutions that can manage code and data around IT-centric assets such as network infrastructure. However, ICS devices are not built using IT development or configuration tools. These devices also have the greatest influence on healthy operation of physical equipment.

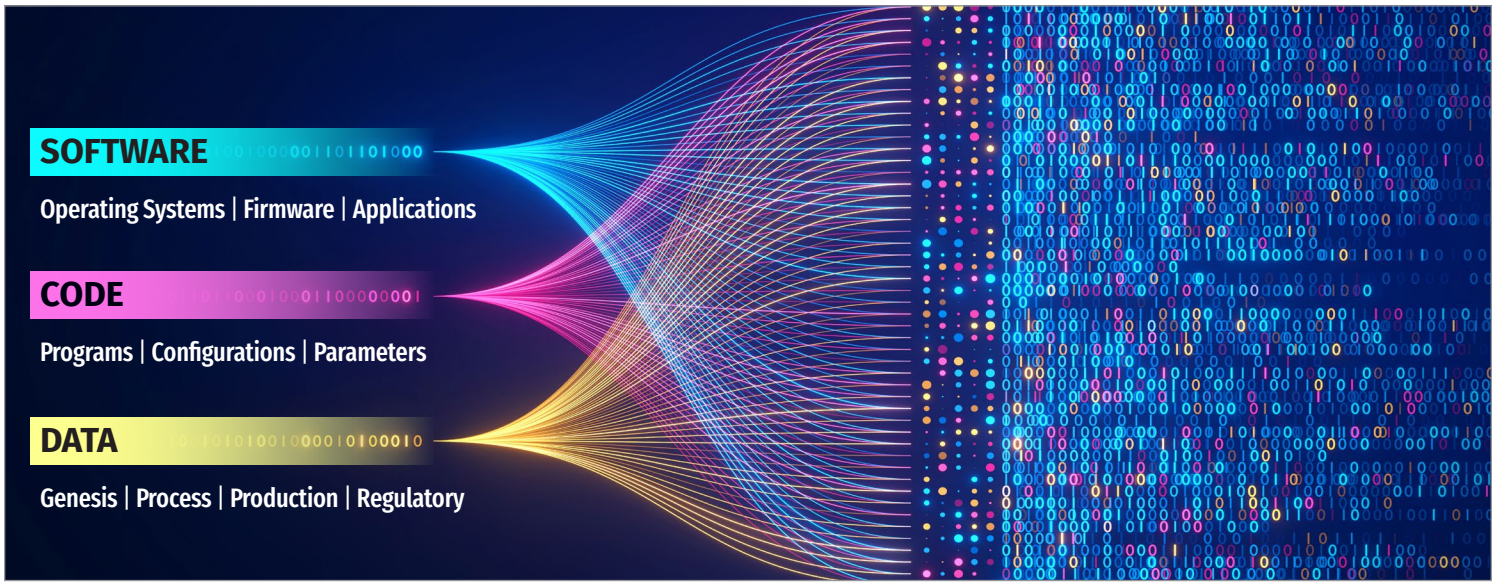

Figure 2. Elements of Change

It will be difficult to find a solution that can support a proactive, online upload and compare style of detection and notification of code version violations across the wide range of ICS component types available across a mix of vendors, products, and solutions. Most vendors operate proprietary protocols that can limit these solutions to be vendor specific. Although beneficial, this can limit the overall coverage because organizations typically rely on multiple vendors, especially when we consider the entire technology stack. There is also the issue around reaching isolated networked or none networked systems. A manual process can be implemented—but with great difficulty—to manage and maintain over time. To truly benefit from having offline copies, they must be adequately protected by access controls, backed up with timely recovery against a disaster, and under a method that can maintain the integrity of all copies knowing that testing is not an easy option. With solutions like these in place, other benefits can be gained, such as change approval processes, accurately tracking date and time of change by personnel, sign-off and approval processes, and the ability to confidently revert changes.

Data Integrity

Managing data changes, separate from code, focuses on overseeing the assets that influence data modification and creation. Data genesis, or the creation of data, occurs across many systems. One example is sensors and instruments attached to physical equipment, which generate data based on their calibration. This data is then fed into automation systems as inputs, where it is processed to solve logic and determine the output that drives the equipment's physical actions. Process data is read, possibly calculated, and displayed to operations personnel for monitoring and appropriate response. Strategic data from the ICS is used to guide decisions on activities and projects for production systems. Some ICS data is specifically captured to meet regulatory requirements. Inaccurate data, whether directly or indirectly, can affect the healthy operation of an ICS and the overall business integrity, impacting costs, service quality, and the safety of people and the environment.

The end solution will ultimately entail both automated and manual efforts following enforceable processes and procedures to ensure staff and contractors comply. Managing and monitoring change in an ICS depends heavily on the effectiveness of adoption by personnel and adjusting to new ways of doing things. The success of adoption is dependent on the culture of the operations team. For some organizations, that can vary among facilities in different locations across the world. For others, it can vary between operational areas within the same facility. There are numerous well-documented options to onboard a culture for change that will not be covered here. Many can understand the cybersecurity benefits that can be gained regarding monitoring, tracking, and controlling change. However, for some operations personnel, this may not be a compelling argument. In such cases, an effective approach might include clearly emphasizing the operational benefits that would directly impact the operations team's overall effectiveness (e.g., minimization of unplanned downtime events and/or shortened recovery times).

Operationalization

To best understand the business drivers for management of change, it can be helpful to analyze and understand the cyber-related impacts to physical equipment as it relates to operational requirements around reliability, resilience, and safety. The first step is to identify which cyber assets have the greatest influence within each operation and analyze how each driver of change can influence operation, including the existence and effectiveness of recoverability. There can be many business drivers for managing change as change does support multiple areas of business functions. As shown in Figure 3, management of change supports operational and cybersecurity functions of an organization. Knowing how the elements of change correlate with each support area can ensure the correct solutions are in place.

Figure 3. Change Support Areas

Conclusion

Many organizations are working to understand how to manage the ever-increasing number of vulnerabilities within an ICS environment. Managing a vulnerability typically means making a change. Those changes can include patching, code changes, or the introduction or revocation of an asset. Any change to a system can create a positive or negative operational response. Regardless of the details of the vulnerability, organizations should prioritize studying its effects on the process, being sure to consider and balance the impacts of both making or not making a change. Documentation of this study can be used to determine what issues, if any, were predicted, and used to select the course of action. If an action was taken, this study would outline how to prevent foreseen issues and could be revisited for unforeseen issues. For reasons already discussed, not all identifiable cybersecurity vulnerabilities will be directly mitigated. When direct action is not taken, this study becomes useful in selecting appropriate cyber-related preventative detection and response activities.

There are many operational benefits to detecting and tracking changes within an ICS. Many people think managing changes in ICS is as simple as tracking PLC code: What change has been made, when, and by whom and was it approved? These are reasonable and quite useful questions. As covered earlier in this paper, change can come in all forms, not just the PLC, but the significance of their role does deserve inclusion. Enforcing change implies there is a formal process and procedure coupled with a method to detect when change occurs. Some organizations implement a formal Change Advisory Board as it ensures due care prior to implementing significant changes. These mechanisms are worth investigating, but it's important to note that even small, seemingly insignificant changes can lead to consequential impacts. For network security monitoring benefits, detection methods must consider rapid detection of unapproved changes across the scope of asset types—such as computers, ICS devices, and network devices—that are impactful to the operation. This can range from detection over the network, such as a partial download to a PLC, to periodically comparing online and offline files. Both methods are complementary approaches to achieve comprehensive visibility.

Operations personnel typically first consider what has changed in response to any operational events. This is reasonable when considering an operation that has been largely functional and without issue for multiple months or years. During a cybersecurity event or incident, the question remains the same, but the focus should shift to understanding if there is evidence of benevolence that can help the operations team determine if a system can continue to operate safely. Much of this depends on effective detection practices but instead of driving forward momentum, the response typically focuses on assessing whether that momentum can continue and looking backward to determine what led to this point. The other consideration during response is when continuing operation requires an emergency change, including but not limited to isolating a system or moving to manual operation that may require code changes to automation equipment or configuration changes to network equipment. The expediency of the decision may require circumventing some aspect of a change process, but effective tracking, in some method, should be retained. This may include bypassing networked, in-band change management systems and connecting directly to a PLC to make a change.

The improvement or recovery process used depends on the path from current state to future state of an operation. However, when changes are involved, the activities should have measurable results. An evaluation of what needs to be done can be helpful to clarify and agree upon what changes need to be made. On execution of a plan, it would be helpful to know where a change was made, by whom, and when if questions need to be asked or tools need to be examined. The significance of validation should never be undervalued. Some changes may require an informal verbal approval, others may need a performance-driven metric to gain certainty the objective has been met. A well-planned revocation process that includes its own testing and validation should also be written into any planned formal or informal change.

Sponsor

SANS would like to thank this paper's sponsor: