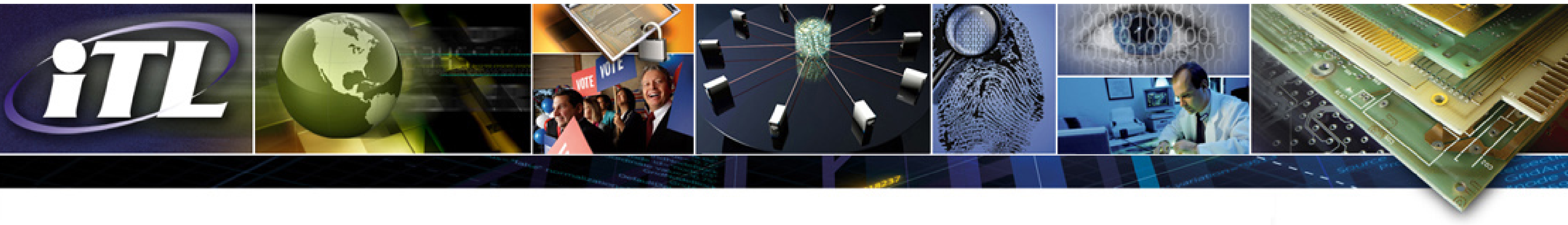


ITL BULLETIN FOR NOVEMBER 2015

TAILORING SECURITY CONTROLS FOR INDUSTRIAL CONTROL SYSTEMS

Victoria Pillitteri, Larry Feldman,[1] and Greg Witte,[1] Editors
Applied Cybersecurity Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

NIST has issued the second revision to Special Publication (SP) 800-82, *Guide to Industrial Control Systems (ICS) Security*. ICS encompass the hardware and software that control equipment and the information technologies that gather and process data that are commonly used in factories and by operators of electric utilities, pipelines, and other major critical infrastructure systems. *Guide to Industrial Control Systems (ICS) Security* includes an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and describes recommended security countermeasures to help mitigate the associated risks. This revision includes new guidance on how to tailor information technology (IT) security controls to accommodate unique ICS performance, reliability, and safety requirements, as well as updates to sections on threats and vulnerabilities, risk management, recommended practices, security architectures, and security capabilities and tools.

Comparing ICS and IT Systems Security

SP 800-82 Revision 2 provides a comparison of ICS and IT, and emphasizes how traditional IT security approaches may have to be tailored to meet the operational needs of ICS. Many of these differences stem from the different goals of each system: IT systems manage data whereas ICS impact elements of the physical world. ICS have different performance and reliability requirements, and also use operating systems and applications that may be considered unconventional in a typical IT network environment. For ICS, security protections must be implemented in a way that maintains system integrity during normal operations as well as during times of cyber attack. As such, the impact of misuse of ICS may result in significant risk to the health and safety of human lives, serious damage to the environment, and financial issues, such as production losses.

Based on this comparison analysis, the publication identifies important considerations when developing security for ICS, including the following:

[1] Larry Feldman and Greg Witte are Guest Researchers at NIST from G2, Inc.

- **Timeliness and Performance Requirements.** ICS are generally more time-critical than IT and require reliable deterministic responses. High throughput is typically not essential to ICS, but automated real-time response to human interaction is often critical.

- **Availability Requirements.** Many ICS processes are continuous in nature, and unexpected outages are unacceptable. Outages must often be planned and scheduled well in advance and depend heavily upon exhaustive testing. Typical IT strategies, such as rebooting a component, are usually not acceptable due to adverse impact on the requirements for high availability, reliability, and maintainability of the ICS.

- **Risk Management Requirements.** In a typical IT system, data confidentiality and integrity are primary concerns. For an ICS, human safety and fault tolerance are the primary concerns. Personnel responsible for operating, securing, and maintaining ICS must understand the important link between safety and security.

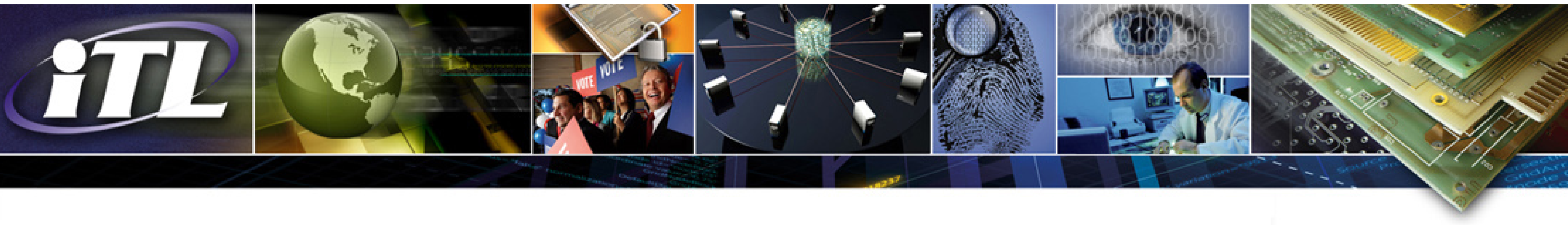
- **Physical Effects.** ICS can have very complex interactions with physical processes. Understanding the potential physical consequences of an adverse ICS event often requires communication among experts in different areas.

- **System Operation.** ICS operating systems and control networks often require different skill sets and levels of expertise from those of traditional IT. Failure to understand those differences can have disastrous consequences on system operations.

- **Resource Constraints.** ICS are often resource-constrained systems that do not include contemporary IT security capabilities. Many are based upon legacy systems lacking resources and features that are common on modern IT systems (e.g., encryption capabilities, error logging, and password protection.) Because there may be fewer computing resources available on ICS components, retrofitting systems with security capabilities may not be possible.

- **Communications.** Communication protocols and media used by ICS environments for field device control and intra-processor communication are typically different from most IT environments, and may be proprietary.

- **Change Management.** Implementation of change management will vary significantly between IT and ICS systems. For example, while software patches on IT systems are typically applied in a short time frame, perhaps using automated means, software updates on ICS require planning/testing and may not occur as quickly as IT updates. Another example is that many ICS utilize older versions of operating systems that are no longer supported by the vendor, and patches may not be available. The change management process, when applied to ICS, requires careful assessment by ICS experts (e.g., control engineers) working in conjunction with other personnel (e.g., security, IT, operations staff).



- **Component Lifetime and Location.** For ICS, the lifetime of the deployed technology is often on the order of ten to fifteen years (and sometimes longer), in contrast with three to five years for IT components. ICS components may be distributed in isolated and/or remote areas and may not be easily reachable.

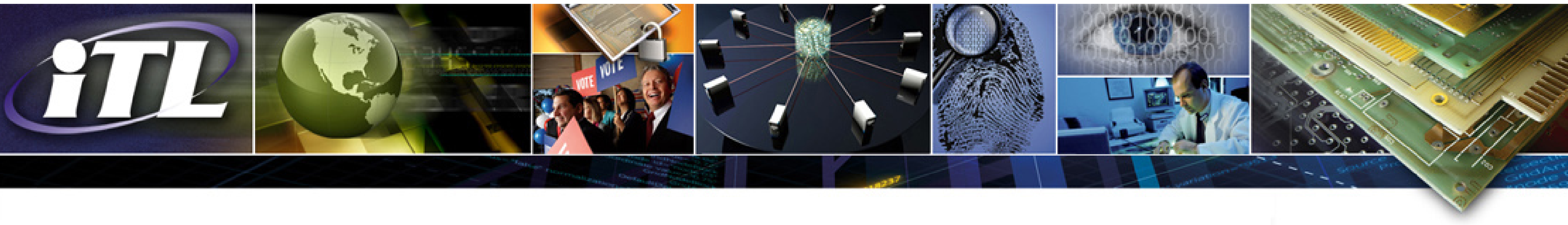
The differences between ICS and IT systems create the need for increased sophistication in applying cybersecurity and operational strategies. A cross-functional team of control engineers, control system operators, and IT security professionals needs to work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation. IT professionals working with ICS need to understand the reliability impacts of IT security methods before deployment.

Applying Security Controls to ICS

SP 800-82 Revision 2 provides ICS-specific recommendations and guidance for each family of security controls described within NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. In particular, SP 800-82 Revision 2, Appendix G includes an ICS-specific overlay of applicable controls that provides tailored baselines for low-impact, moderate-impact, and high-impact ICS. The concept of ***overlays*** is introduced in SP 800-53 Revision 4 to address the need for development of community-wide and specialized sets of security controls. An overlay is a fully specified set of security controls, control enhancements, and supplemental guidance derived through application of tailoring guidance to the security control baselines described in SP 800-53 Revision 4. These tailored baselines can be used as initial specifications and recommendations that can be applied to specific ICS.

For example, SP 800-82 Revision 2 recommends implementing control SI-17, *Fail-Safe Procedures*, which is not selected in the SP 800-53 Revision 4 security control baselines. Mechanical and analog systems can be used to provide mechanisms to ensure fail-safe procedures, which should incorporate potential impacts to human safety, physical systems, and the environment. This is not usually a significant consideration for IT systems.

Overlays benefit the community by reducing the need for organization-specific ad hoc tailoring of baselines. An overlay supports selection of a set of controls and control enhancements that closely corresponds to common conditions, enhancing repeatability and fostering implementation of best practices. In addition to using the ICS-specific overlay, organizations may need to perform further tailoring to add or remove controls and control enhancements for specific needs, assumptions, or constraints. However, all tailoring activity should, as its primary goal, focus on meeting the intent of the original security controls where feasible. For example, there may be situations where the ICS cannot support particular security controls or control enhancements, or where the organization determines it is not advisable to implement those through ICS. In such a situation, the organization provides rationale describing how compensating controls deliver an equivalent security capability or level of protection for the ICS, and why the related baseline security controls could not be employed. If the ICS cannot support



the use of automated mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance in SP 800-53 Revision 4.

Conclusion

SP 800-82 Revision 2 includes new guidance on how to tailor traditional IT security controls to accommodate unique ICS performance, reliability, and safety requirements. It provides updates to sections regarding threats and vulnerabilities, risk management, recommended practices, security architectures, and security capabilities and tools.

Due to unique performance, reliability, and safety requirements, securing ICS often requires adaptations and extensions to NIST-developed security standards and guidelines that are commonly used to secure traditional IT systems.

A significant addition in this revision is a new ICS overlay offering tailored guidance on how to adapt and apply security controls and control enhancements detailed in SP 800-53 Revision 4 to ICS. That document contains a catalog of security controls that can be customized to meet specific needs stemming from an organization's mission, operational environment, or the particular technologies used. Using the ICS overlay, utilities, chemical companies, food manufacturers, automakers, and other ICS users can adapt and refine these security controls to address their specialized security needs.

Resources

NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*

NIST SP 800-53 Revision 4, S*ecurity and Privacy Controls for Federal Information Systems and Organizations*

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.