CONTROL AUTOMATION

Cybersecurity Resources for Control System Engineers

by Steve Blaine

What kind of guidance is available to help you defend your industrial control system (ICS)?

Lately, even the most sophisticated organizations and companies have seen their computer systems attacked and compromised. As control system engineers, we're all on high alert that our systems could be next. This article is written to inform you about some official guidance that is available to help you defend your industrial control system (ICS).

There are many defense and mitigation strategies that should be considered. Some of these actions are administrative and can be done very inexpensively. Others require sophisticated hardware and software, which can be very expensive. A list of these items would include:

- Antivirus software
- Automatic offsite backups
- Disaster recovery plans
- Demilitarized zones
- Data encryption
- Industrial firewalls
- Intrusion detection systems
- Multifactor authentication
- Network monitoring devices
- Network segmentation
- Password management and procedures
- Patch management
- Port configuration
- Redundancy
- Remote management software
- Security incident and event management
- Unidirectional data diodes
- Virtual private networks
- Vulnerability scanning software
- Wireless access point management

How should you decide which strategy is necessary and where it should apply? This can be a daunting task as there is a lot of information to consider. Further complicating things, each control system and the organizations that use them are all different. So, there is no ready answer for choosing how to defend your particular system.

A good place to start is with the knowledge and frameworks available from the organizations dedicated to answering this question. Hopefully, this article will provide an introduction to those resources so you can wrap your arms around the challenges with cybersecurity.

Industrial Control System - Cybersecurity Guidelines and Standards

The knowledge and frameworks mentioned above are available from several organizations as published in their guidelines, standards, and technical reports. Note that each organization has its specific mission and intended audience, which means the focus or even how some things are addressed may not be pertinent to you.

These guidelines are essentially consistent with each other, so there shouldn't be a concern that following only one will lead you astray. Ideally, all of them would be reviewed by anyone tasked with fully understanding industrial cybersecurity.

Most recommended are the two guidelines for industrial cybersecurity available from the National Institute of Standards and Technology (NIST) and a joint standard published by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC).

Both sets of documents are mature but still evolving to keep up with changing technology and newly identified threats. A third recommended resource is the Cybersecurity and Infrastructure Security Agency (CISA), part of the Department of Homeland Security (DHS).

CISA shares guidance, case studies, and many free tools and services as listed on their website. Note that unless you are in the electric power industry, these standards are considered voluntary.

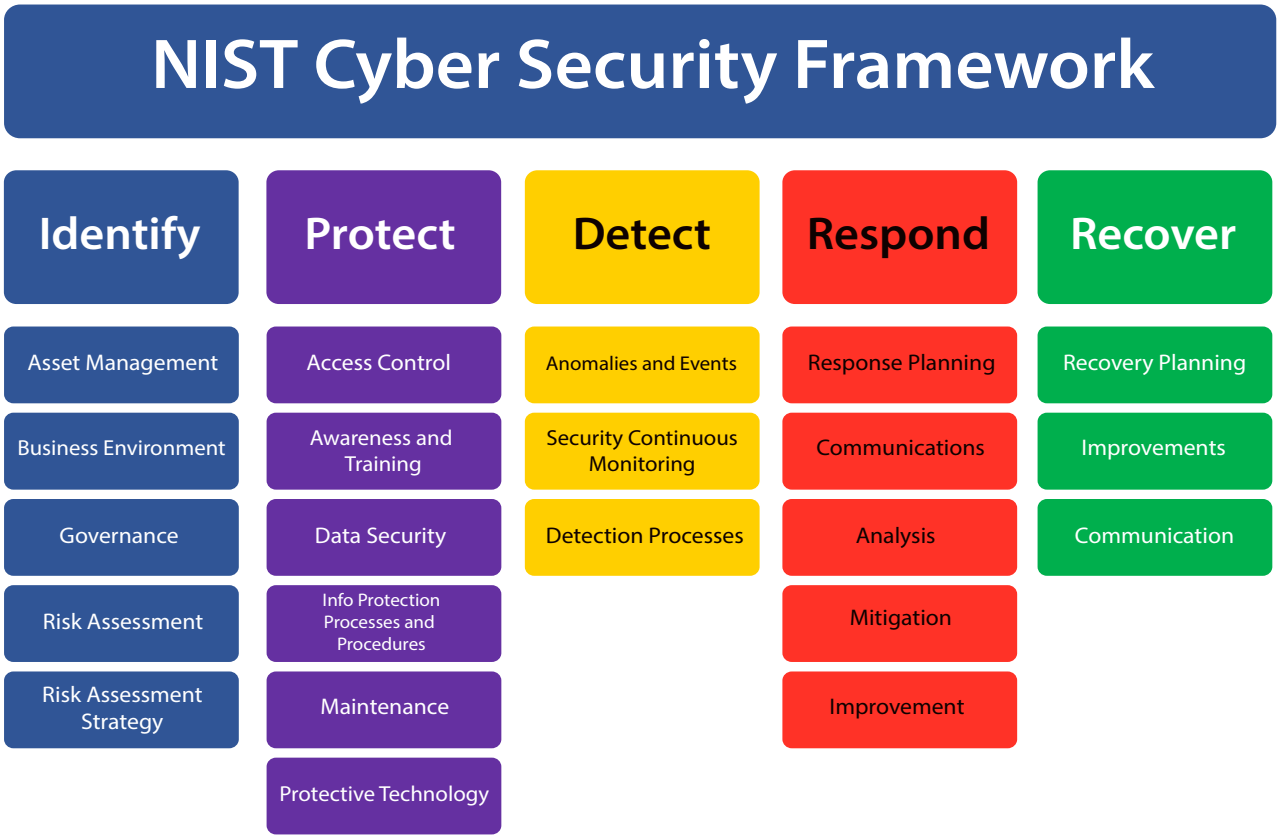
Electrical power control systems have similar concerns, but they must follow North American Electric Reliability Corporation/ Critical Infrastructure Protection (NERC/CIP) regulations that provide similar guidance but are not addressed in this article.

Electrical power control systems have similar concerns, but they must follow North American Electric Reliability Corporation/ Critical Infrastructure Protection (NERC/CIP) regulations that provide similar guidance but are not addressed in this article.

National Institute of Standards and Technology – Special Publication 800-82

The National Institute of Standards and Technology provides specific guidance for industrial control system cybersecurity in NIST SP 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security. This is an important standard to know, but before discussing what's in there, it's helpful to explain how this document fits with other NIST publications and the NIST Cybersecurity Framework.

Cybersecurity recommendations from NIST follow the NIST Cybersecurity Framework – probably the single most referenced source of information for best practices in cybersecurity. The framework applies to computer systems of all sorts, including control systems, and is a comprehensive way to think about cybersecurity.



The framework is organized around five functional areas followed by 22 categories, which are shown above, and 108 subcategories (which are not). The complete framework includes "Informative Resource" references for each subcategory connecting these requirements to specific sections in a variety of other information security standards sort of a cross-reference for all of them.

NIST also provides a "special publication" for organizations that "process, store, or transmit information," NIST Special Publication (SP) 800–53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations. While the information in this publication is not aimed at control systems and may be unfamiliar to you as a control engineer, it's probably well known to your IT colleagues. Following this standard is considered best practice and in fact, is mandatory for federal information systems.

Here's where control systems come in. Because control systems are quite different from other computer systems, a separate NIST document was created to address the special performance, reliability, and safety concerns for control systems.

NIST SP 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security is considered an 'overlay' to SP 800–53 that provides specific guidance for control systems. This highly useful document describes in detail the recommended standards, guidelines, and best practices to protect critical infrastructure.

Reading this document, you'll find sections on risk management and assessment, security program development and deployment, and specific guidance targeted for each element, category, and subcategory

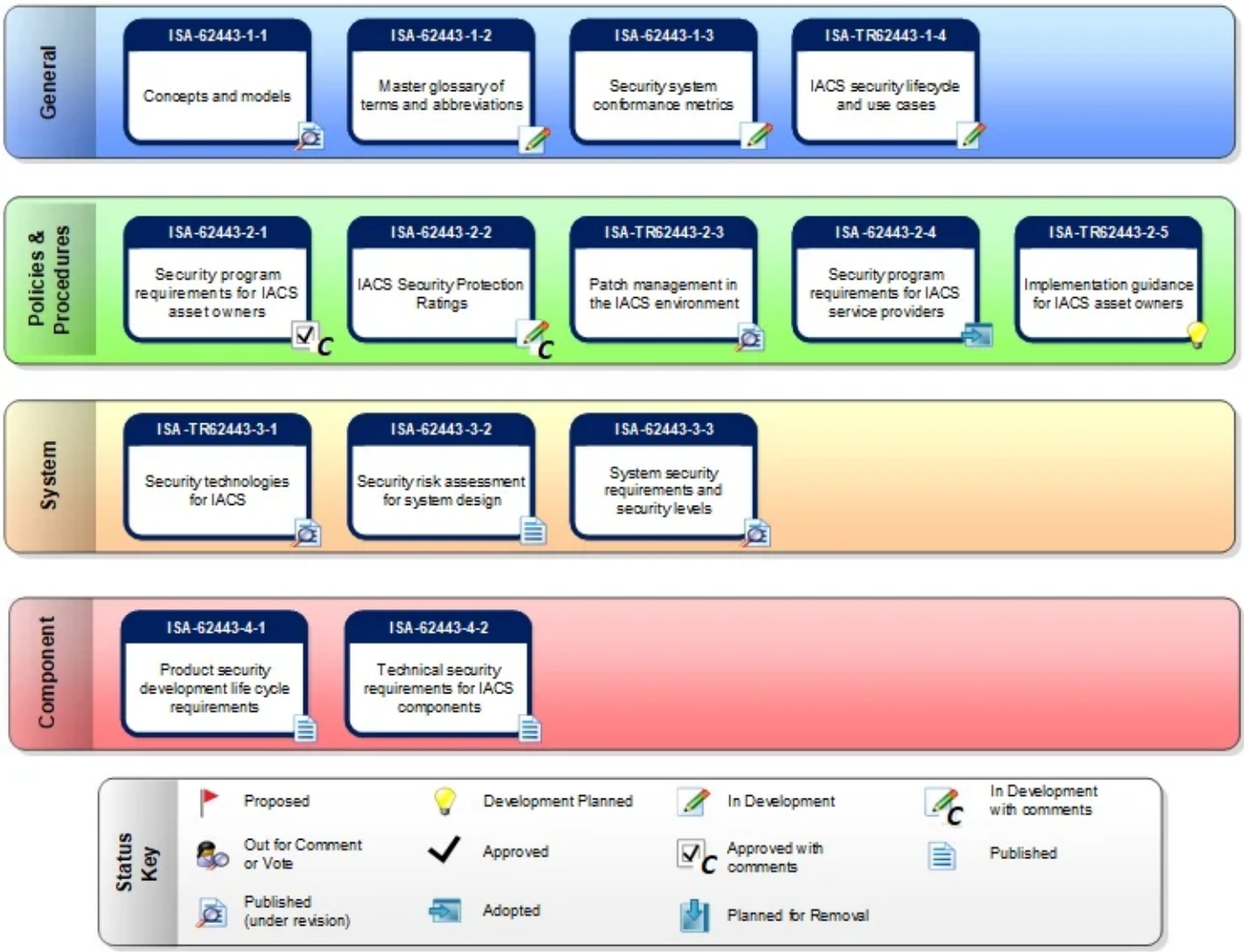
International Electrotechnical Commission - 62443

The second set of standards to reference is IEC 62443 - Industrial communication networks - Network and system security. For control system engineers, IEC 62443 is one of the most comprehensive places to turn because it addresses all aspects of industrial control system cybersecurity in detail.

Some sections are still being developed but the information already available is quite complete. Note that the IEC standards use the acronym "IACS" for Industrial Automation & Control System instead of "ICS" or Industrial Control System which is used in the NIST documents. They should be considered the same thing.

This standard was developed by the ISA99 committee in 2002 to improve control system security. The series has grown and evolved and has now been adopted by the International Electrotechnical Commission as IEC 62443 - which is how it will be referenced here.

Just like the NIST standard relies on its predecessors, the NIST Framework and SP800-53, IEC 62443 relies on its predecessor, IEC 27001 – Information Security Management, the international standard that outlines best practices for implementing information security controls. That document is not focused on control systems but can also be an important reference for cybersecurity.



The 62443 series is organized into 4 groups and 14 subgroups. Image courtesy of International Society of Automation (ISA).

These documents are not available for free. Hopefully, that does not prevent you from accessing this comprehensive resource.

As you can see, the subgroup standards are in various stages of development and acceptance. Each section is also targeted at specific parties - Asset Owners, System Integrators, Product Developers, or combinations of each. All of them are informative but key sections that control system engineers should know are listed below.

62443-2-1 - Security Program Requirements for IACS Asset Owners

This section describes the elements that make up a cybersecurity program. The section starts by describing the ideas of security and maturity levels, two concepts that help tailor a security plan to your particular control system requirements.

The core of the section follows with a description of eight Security Plan Elements (SPE):

SECURITY PLAN ELEMENT	DESCRIPTION
SPE 1 – Organizational security measures	Details required for how organization and policies such as security awareness training, physical access, and other programs should be implemented.
SPE 2 – Configuration management	Requirements for Inventory management of system hardware/software components and network communications, including Infrastructure drawings/ documentation, Configuration settings, and Change control.
SPE 3 – Network and communications security	Describes rationale and requirements for system segmentation, wireless access, and remote access. These requirements may be the most essential part of the security plan.
SPE 4 – Component security	Describes requirements for device hardening, portable media, malware protection, patch management.
SPE 5 – Protection of data	Describes data retention, and purging, cryptography, and key management.
SPE 6 – User access control	Identification and authentication, multifactor and otherwise, password protection, administrative rights, and so on.
SPE 7 – Event and incident management	Event detection, reporting, logging, event analysis, incident handling and response, vulnerability handling.
SPE 8 – System integrity and availability	Continuity management, resource management, DoS attacks, Backup/restore/archive.

Table 1 – IEC 62443-2-1: Security Plan Elements.

Understanding these elements will help you to comprehend the cybersecurity concepts which are part of the standard. Subsequent IEC 62433 sections elaborate on these concepts and help determine where each element described above is required and how to implement them.

62443-3-2: Security Risk Assessment for System Design

This document describes how to assess the security risks faced by a particular control system. There are four Security Levels (SLs) defined in the standard: from SL 1 (mistake resistant) to SL 4 (resistant against nation-state attacks). A summary of each level coupled with a characterization of the type of attacker the security level is designed to address is presented in the table below:

SECURITY LEVEL	TARGET	SKILLS	MOTIVATION	MEANS	RESOURCES
SL1	Casual or Coincidental Violations	No attack skills	Mistakes	Nonintentional	Individual
SL2	Cybercrime, Hacker	Generic	Low	Simple	Low (Isolated Individual)
SL3	Hacktivist, Terrorist	ICS Specific	Moderate	Sophisticated (Attack)	Moderate (Hacker Group)
SL4	Nation State	ICS Specific	High	Sophisticated (Campaign)	Extended (Multi-Disciplinary Teams)

Table 2 – IEC 62443-2-1: Security Plan Elements.

62443-3-2: Security Risk Assessment for System Design

A feature of the standards is guidance on segmenting the system under consideration into "security zones and conduits." The components and devices within each zone or conduit are then assigned an individual target security level (SL-T). The key concept is that the defense strategy should match the security level needed for the risks faced.

Knowing the target Security Level, the necessary System Requirements (SRs) and Requirement Enhancements (REs) can be proposed. This section includes a detailed list of requirements necessary to comply with each of the security levels. For Security Level 1 (SL1), there are 37 individual requirements. For SL2, the specification includes all the SL1 requirements and adds 23 more. And so on through level 4.

As an example, here is what the standard says about the System Requirement (SR) and Requirement Enhancements (REs) for a single security measure, Control System Backups:

Requirement	SL1	SL2	SL3	SL4
SR 7.3 – Control system backup	x	x	x	x
SR 7.3 RE 1 – Backup verification		x	x	x
SR 7.3 RE 2 – Backup automation			x	x

Table 3 – IEC 62443-3-3: Example - Security Requirements & Enhancements.

62443-4-2: Technical Security Requirements for IACS Components

This section lists SRs and REs for Product Suppliers to follow to provide built-in security that matches the four Security Levels listed previously. These requirements are applicable to components, embedded devices, software applications, host devices, and network devices.

This is the start of an effort to provide "built-in" security for control system equipment, even including things like PLCs and communication modules. Not all equipment vendors have begun to meet this standard yet, but some already have. As it develops, it will provide a common baseline functionality for all types of devices going forward.Formerly known as "Achilles Certification," the lab providing certification for this standard has been acquired by GE. A list of certified products is available on their website.

Cybersecurity and Infrastructure Security Agency (CISA)

Finally, the Cybersecurity and Infrastructure Security Agency (CISA) also has a vast assortment of resources available to help identify threats, protect your system, respond to and recover from attacks. The CISA also offers a range of assessment services that evaluate an organization's cybersecurity practices and resilience.

For example, CISA offers a self-assessment tool called the Cyber Resilience Review, which is useful as a starting point for you to complete yourself. They also offer a free Validated Architecture Design Review (VADR), which evaluates your systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner.

They even offer free on-site visits from their experts to conduct cybersecurity reviews at your facility. If you participate in the CISA assessment process, they will provide confidential recommendations and plans. The entire range of services available on their website.

A comprehensive and consistent set of resources is available to help control system engineers respond to the cybersecurity challenge. A good first step for anyone trying to safeguard their system is to become familiar with the guidance and standards published by NIST, IEC, and CISA.

Following the guidance available from the sources in this article may help select and implement the most effective security measures to provide the defense-in-depth strategy that experts recommend for your system.

About Us

Control Automation is an online community for control and automation engineers in the broader industrial field. The Control Automation forum is a place for users to offer their expertise and seek the help of their peers. The forum allows members to ask specific questions and establish connections with others who share similar knowledge in the industry.

It also provides a strong sense of community for those solving similar types of problems. Control Automation's editorial section is dedicated to developing useful, relevant news and insights from all corners of the industry and the engineers who run them.

The articles highlight new trends, challenges, and solutions, so users have all the skills they need to succeed in the industry. For more information, please visit https://control.com/, or contact the editors at pr@control.com.

Author Bio

Steve is an Automation Technologist with Jacobs Engineering. He holds a BS in electrical engineering from the University of Pennsylvania and an MS in Engineering Management from Portland State University. In his almost 40 years of instrumentation and controls experience, he has taken projects through all phases from conceptual design to final commissioning. He has designed controls for machines, facilities, and systems using PLCs, PCs, operator interfaces, and SCADA systems – even push buttons and relays. He has completed industrial control projects all over the world with a focus on the semiconductor, metals, water, and wastewater sectors.

Cybersecurity Resources for Control System Engineers

BY STEVE BLAINE

CONTROL AUTOMATION