SIEMENS
Ingenuity for life

Siemens EngineeringAdvantage™

Newsletter

Issue 2 — 2019

Introduction

As buildings become smart, there is increasing interest in cloud-based applications for data and IoT devices to help buildings operate more cost effectively and to improve occupant comfort. However, in doing so, we are also increasing exposure to cyber threats, which were not a factor historically with Building Automation Systems.

This newsletter will focus on cybersecurity challenges, current policies, and standards to aid building owners and designers, as well as potential steps to help mitigate the cybersecurity risks associated with modern Building Automation Systems.

In This Issue:

Design Topic

Cybersecurity Concepts

Cybersecurity Overview

Protecting critical infrastructures and sensitive data has become a significant and global concern. This challenge affects public infrastructures just as much as the manufacturing industry and the energy and healthcare sectors. Companies everywhere anticipate that the networking of machines and facilities will not only generate significant financial advantages, but major security challenges as well. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative. Highly-publicized critical infrastructure breaches have revealed that hackers aren't just attacking IT systems, but OT (i.e. BAS systems) as well. Moreover, with ever more products, solutions, and services employing software that is often used in critical infrastructures, the range of cybersecurity risks will continue to grow. As a result, more than eight billion devices, including machines, facilities, sensors, and products, now communicate with one another, representing an increase of about 30 percent since 2016. This number is expected to continue climbing to more than 20 billion devices by 2020.

Figure 1: Credit Cisco 2018

Common types of cybersecurity threats

- **Phishing** is the most common type of cyber-attack and involves sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyber-attack. You can help protect yourself through education or a technology solution that filters malicious emails.
- **Ransomware** is a type of malicious software designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered, or the system restored.
- **Malware** is a type of software designed to gain unauthorized access or to cause damage to a computer.
- **Social Engineering** is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats previously listed to make you more likely to click on links, download malware, or trust a malicious source.
- **Zero-day vulnerability,** at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact,a zero-day exploit leaves NO opportunity for detection ... at first.

continued on next page

	Information Technology	Operational Technology
Purpose	Process transactions, provide information	Control or monitor physical processes and equipment
Architecture	Enterprisewide infrastructure and applications (generic)	Event-driven, real-time embedded hardware and software (custom)
Interfaces	Graphical user interface, Web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, handheld devices
Ownership	Chief information officer, information technology	Engineers, technicians, operators, managers
Connectivity	Corporate network, Internet Protocol – IP-based	Control networks, hardwired twisted pair, IP-based
Role	Supports people	Controls machines

Figure 2: General Differences between IT and OT: Image Credit Michael Chipley, Daryl Haegley and Eric Nickel. "Your Building Control Systems Have Been Hacked. Now What?" HPAC Engineering Nov 10, 2016

Operational Technology vs. Information Technology

Operational Technology (OT) is a category of hardware and software that monitors and controls how physical devices perform. Building Automation Systems (BAS), Industrial Control systems (ICS), SCADA systems, and the like are examples of Operational Technology networks.

Information Technology Networks (IT) are the traditional networks we are familiar with; they're composed of servers, workstations, mobile devices, routers, etc. These networks are usually managed by well-established IT departments with a variety of cybersecurity tools.

As our building automation systems become more complex to meet the data demands of building owners and physical devices are becoming connected and smart, the worlds of IT and OT are merging.

Cloud computing is transforming the way we do business, making IT more efficient and cost effective. However, the convenience also opens companies up to increased risks to cyber-attacks.

While cybersecurity has long been a part of IT, OT has had little need for cybersecurity until the recent move toward converged IP networks. Past BASs had little fear of cybersecurity threats primarily due to limited connectivity outside of simple remote access and obscurity. However, as our modern intelligent buildings are becoming more connected, integrated, and complex, the ability to access the systems has increased.

Defense in Depth

Many organizations have employed Defense-in-Depth (DiD) measures within their information technology (IT) infrastructures but have not applied it to their OT. Until recently, most organizations did not need to as legacy OT systems used obscure or proprietary protocols and were not susceptible to hacking due to their separation from IT and because of having physical protection measures in place. But with the convergence of IT and OT architectures, recent high-profile intrusions have highlighted the potential risk to control systems. DiD takes a holistic approach using specific countermeasures implemented in layers to create an aggregated, risk-based security posture. These layers help defend against cybersecurity threats and vulnerabilities that could affect these systems. DiD provides a flexible and useable framework for improving cybersecurity protection when applied to control systems.

Five Key Security Countermeasures for ICS

Applying these five key steps can pave the way toward a more robust security environment and significantly reduce the risk to operational systems.

1. **Identify,** minimize, and secure all network connections to the ICS.
2. **Harden** the ICS and supporting systems by disabling unnecessary services, ports, and protocols; enable available security features; and implement robust configuration management practices.
3. **Continually monitor and assess** the security of the ICS, networks, and interconnections.
4. **Implement** a risk-based DiD approach to securing ICS systems and networks.
5. **Manage the people** – clearly identify requirements for ICS, establish expectations for performance, hold individuals accountable for their performance, establish policies, and provide ICS security training for all operators and administrators.

(adapted from Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth)

continued on next page

CYBERSECURITY STANDARDS GUIDELINES AND BEST PRACTICES

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Figure 3: FIPS 199 C-I-A Potential Impact Table

FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems

FIPS (Federal Information Processing Standard) 199 is a set of mandatory security standards required by FISMA, and requires Federal agencies to assess their information systems in each of the categories of **confidentiality, integrity, and availability,** (frequently referred as C-I-A) rating each system as **low, moderate, or high** impact in each category. The most severe rating from any category becomes the information system's overall security categorization.

NIST SP 800 – 53r4 – Security and Privacy Controls for Federal information Systems and Organizations

Provides baseline controls from which agencies can satisfy FIPS 199 and 200 to ensure that appropriate security requirements and security controls are applied. Cybersecurity "controls" is defined as a safeguard/countermeasure prescribed for information systems or organizations that are designed to: a) protect the C-I-A of information that is processed, stored, and transmitted by those systems/organizations; and b) satisfy a defined set of security requirements

NIST Cybersecurity Framework (V 1.1)

In response to the 2013 Executive Order 13636, Improving Critical Infrastructure Cybersecurity, NIST was tasked with working with industry and government entities to develop a voluntary frame-work based on existing standards, guidelines and practices to reduce risks to the nations critical infrastructure.

The official title of the document is Framework for Improving Critical Infrastructure Cybersecurity but is usually referred to as the NIST Cybersecurity Framework or just "the framework". It is a comprehensive guide to managing cybersecurity for an entire organization and acts as both a technical reference and management guide.

The framework consists of three main components: (1) The Core, which consists of five functions that collectively provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk (2) Tiers, which consist of four increasing levels of progression and (3) Profile, which represents the cybersecurity outcomes based on business needs that an organization has selected from the Framework Categories.

Although the NIST Framework is a high level, holistic approach to an entire business cybersecurity needs, the Informative References identify guidelines which pertain to Building Automation Systems, such as ISA/IEC 62443, NIST SP 800-53.

Figure 4: The five concurrent and continuous Functions representing the Core of the NIST Cybersecurity Framework

continued on next page

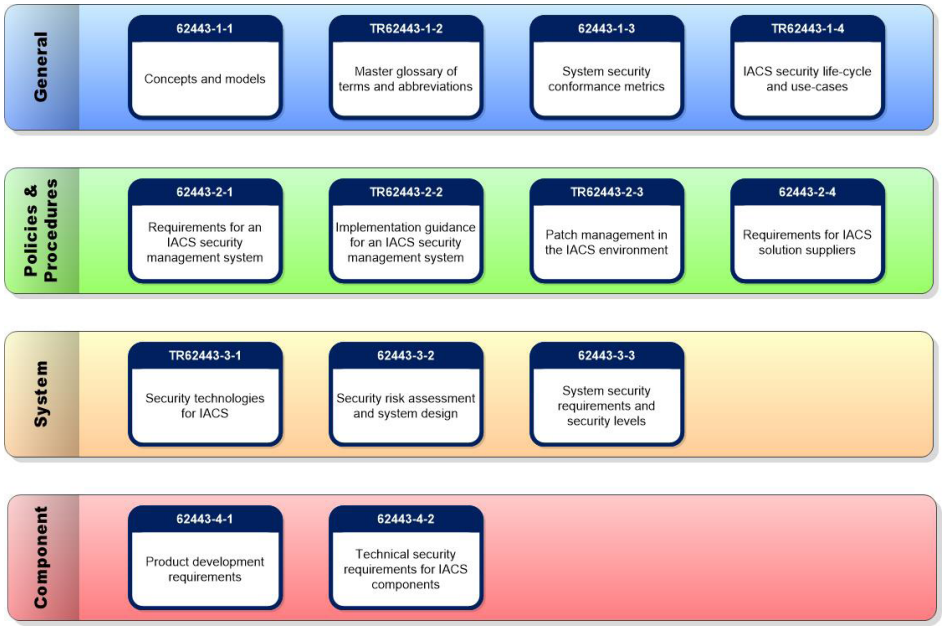


Figure 5: Overview of ISA 62443 Series

INDUSTRIAL CONTROL SYSTEMS

The following paragraphs outline standards/guidelines that address cybersecurity specific to the "control world". As indicated, although there are some similarities to Information Systems, these are meant to help guide the users to address the differences.

NIST SP 800-82r2 – Guide to Industrial Control Systems (ICS) Security

This document contains cybersecurity controls specific to Industrial Control Systems (also referred to as OT in this newsletter) which are a subset of those specified in NIST SP 800-53r4.

DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

The Department of Homeland Security Control Systems Security Program is part of the United States Computer Emergency Readiness Team (US-CERT) and provides tools, standards, training, and publications for ICS.

ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

ISA/IEC 62443 – Security for Industrial Automation and Control Systems

IEC 62443 series (Formerly ISA 99) is a global standard for the Security for Industrial Control System (ICS) networks and helps organizations to reduce both the risk of failure and exposure of ICS networks to cyber threats. The goal of the series is to improve the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, and to provide criteria for procuring and implementing. This standard was originally produced by ISA (International Society of Automation) and adopted by the International Electrotechnical Commission (IEC) to align with American National Standards Institute (ANSI).

The standard is a series of four parts:

General Concepts – these documents are overarching in nature and apply to the entire series of standards and technical reports.

Policy and Procedure – address the organizational aspects of policies and procedures for cybersecurity

System – these documents address the system-level technical aspects of cybersecurity, including system design principles and system capabilities.

Component – these documents address the component-level technical aspects of cybersecurity, including development processes and component capabilities

The key areas for BAS systems would be:

62442-2-4 which specifies requirements for security capabilities for IACS service providers for integration and maintenance

62443-3-3 – detailed technical control system requirements

WHAT YOU CAN DO

Although many of the standards apply to holistic approaches to business practices, as specifiers, you can help customers by stating certain requirements within your BAS designs and specifications such as:

- IBMS (Integrated Building Management System) manufacture must have a Cyber Awareness Emergency Team (CERT). Any product vulnerabilities will be reported in text or email to the owner or via manufacturer CERT website alert.
- Reference cybersecurity standards such as NIST 800-82 and ISA 62443.03.03.
- Increase network and system security with automated device discovery, authentication of devices and users, authorization of traffic flows based on device/user, and isolating network traffic to block and contain threats.
- Secure the network perimeter with the latest firewall, malware detection, and secure remote access technologies.
- Implement BAS role-based access control, password policies, and least privilege.
- Follow BAS manufacturer guidelines for cybersecurity implementation.
- Collaborate with enterprise IT teams and leverage existing IT best practices for OT systems as much as possible.

For facilities/projects requiring an integrated building management system (IBMS) or with a high cyber threat impact, consider a technology partner to bring together a converged IT and OT system. This will require early participation in the design of the project but provides best practices and software tools for cybersecurity to help mitigate risk to an organization.

Product and Solution Focus

Siemens Smart and Secure Building

Protecting your building's OT and IT networks, systems, and components becomes more important as the number of devices, network entry points, and overall system complexity increase. Siemens Smart and Secure Building Connected by Cisco Technology is the only solution of its kind available in the market today. Protect and future-proof your smart building with this unique combination of threat protection, network management, and integrated building management system.

Siemens and Cisco bring together IBMS and network threat defense components to provide automated threat intelligence and security for your smart building. This solution enhances visibility of network traffic and activity so that malicious intruders can be detected, isolated, and contained.

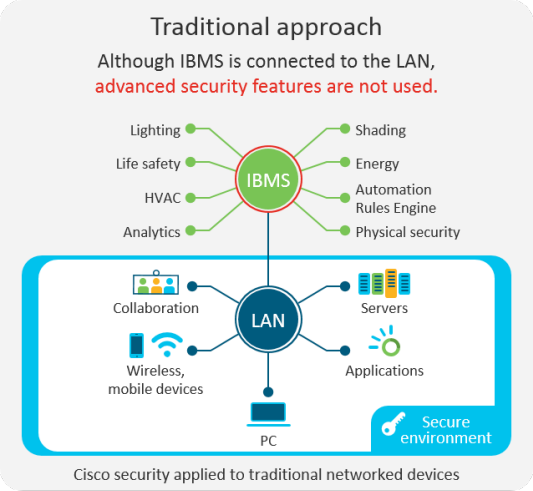
- Cybersecurity solution co-developed with Cisco
- Using off-the-shelf / commercial and proven technologies
- Market-only validated active cybersecurity solution for smart buildings
- Cybersecurity lab commissioned in partnership with Cisco
- Fully tested and validated

Take advantage of the solution provided by these two industry leaders. You can increase the safety and security of your building systems and reduce maintenance effort by installing leading-edge technology that is customized to your environment. Meet today's cybersecurity challenges directly with a best-in-class solution that minimizes risk and prepares your facility to manage the continued growth in technology devices.

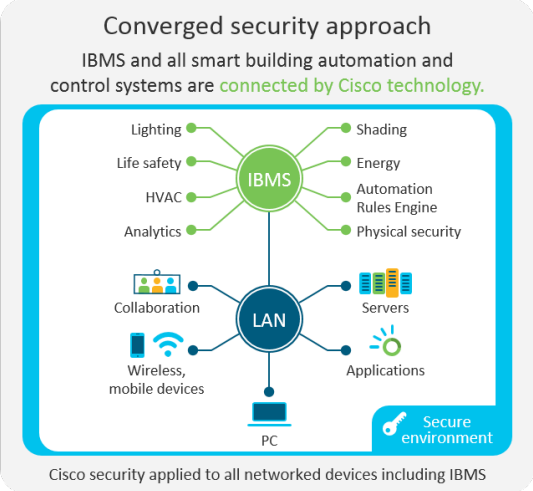
BENEFITS INCLUDE:

- Realize cost savings across the building's life cycle: lower construction costs with ready-to-go solution; lower cybersecurity insurance rates; deliver ongoing efficiencies in OT system maintenance.
- Increase network and system security with automated device discovery, authentication of devices and users, authorization of traffic flows based on device/user, and isolating network traffic to block and contain threats.
- Enable the secure operation of an IBMS designed for the modern smart building to optimize heating, cooling, ventilation, lighting, shading, room automation, energy management, fire safety, and security.

Click here to visit our website to learn more about protecting your smart building's OT and IT systems with the Siemens Smart and Secure Building Connected by Cisco Technology solution.



Cisco security applied to traditional networked devices



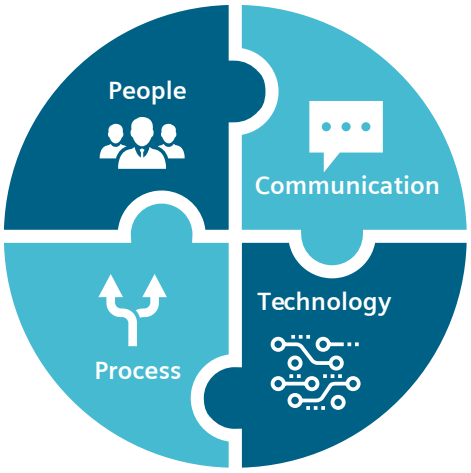
Cisco security applied to all networked devices including IBMS

Use Cases

INDUSTRY	DESCRIPTION
Any	**Authentication** • Establish profiles for every device authorized for the network in order to identify each device as it connects • Protect each network entry point by securely authenticating every device that attempts access • Block access by unauthorized devices
Any	**Authorization** • Build unique device identification profiles • Establish policies that limit network communication to perform a device's function • Limit cyber security risk by controlling areas of network with which a device can communicate • Reduce a potential attacker's mobility within the network and ability to extract data, if a device is compromised
Any	**Visibility and Instruction Detection/Prevention** • Capture meta data and statistics regarding network traffic between devices • Build baseline of normal network traffic for different device types • Detect abnormal or potentially risky network behavior and raise an alert for investigation • Isolate or block risky or malicious devices, denying access to network

Siemens Cybersecurity Model

Siemens Cybersecurity Model applies four key factors into its defense in depth:



1) The People Factor

Ensuring a broad and lasting awareness of the importance of security is a key component of the Siemens security model that is woven into product development and processes.

2) The Communication Factor

Clear, consistent, and friction-free communication helps establish a culture of security among the people in an organization.

3) The Process Factor

Organization processes are just as important to security as the technology that is used to protect a company from cyber threats.

3) The Technology Factor

Knowing which security technologies and building blocks are suitable for a given organization is important.

Highlights of Siemens Approach to Security

Employee know how	Customers security objectives and requirements	Secure product architecture and design	Pre-deployment assistant	Security testing	Deployment and maintenance	Incident and vulnerability management
Specialist cybersecurity skills and consistency	Specify security requirements	Security design measures aligned to EC62443	Threat and risk assessment	Product security verification and validation	Product hardening	Established incident handling process: Siemens Product CERT
Company-wide cybersecuity initiative	Detect customer protection goals	Provide solid product foundation	Anticipate and integrate foreseeable cyber threats	Regular manual protection testing	Secure installation and commissioning	Continuous vulnerability and threat monitoring
	Focus on intended operational environment			Automated testing tools and methods	Software maintenance progress	

Siemens Charter of Trust

At the Munich Security Conference 2018, Siemens and eight partners from industry signed the first joint charter for greater cybersecurity. Initiated by Siemens, the Charter of Trust calls for binding rules and standards to build trust in cybersecurity and further advance digitalization. Since 2018, the Charter of Trust has grown to 16 members. In addition to Siemens and the Munich Security Conference, the signatories include AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, IBM, NXP, SGS, Total and TÜV Süd.

In addition, the German Federal Office for Information Security, the CCN National Cryptologic Center of Spain and the Graz University of Technology in Austria have joined the charter as associate members. On February 19, 2019, Mitsubishi Heavy Industries (MHI) signed a letter of intent to join the Charter of Trust for cybersecurity in Tokyo, expanding the Charter's reach into Asia. The company's membership is expected to be finalized by the end of September 2019. MHI will be the first Asian company to join the global cybersecurity initiative.

For More Information

NIST (National Institute of Standards and Technology):
Framework for Improving Critical Infrastructure Cybersecurity

Cyber-Physical Systems (CPS) Framework

NIST IR 8183 - Cybersecurity Framework Manufacturing Profile

NIST SP 800-82r2 - Guide to Industrial Control Systems Security

NIST SP 800-53r4 - Security & Privacy Controls for Federal Information System

DHS (Dept of Homeland Security):
Cybersecurity and Infrastructure Security Agency (CISA)

National Cybersecurity and Communication Integration Center's (NCCIC)

National Infrastructure Coordinating Center (NICC)

Critical Infrastructure Cyber Community Voluntary Program (C3VP)

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

ISA (International Society of Automation):
ISA/IEC 62443 Series
International Society of Automation (ISA) Security Compliance Institute

Whole Building Design Guide (WBDG)
WBDG - Cybersecurity

DoD:
UFC 04-10-06 - Cybersecurity of Facility Related Control Systems

Siemens:
Visit our Smart and Secure website

Go to the Siemens Desigo CC page for more information.
Click here to visit Siemens Charter of Trust.

Go to the Siemens Smart Buildings page

Cisco:
Click here to visit Cisco Digital Building Solution.

Click here to visit Cisco Network Intuitive.

Simple Select

SpecWriter

CONTACTS

Mark Halbur
Siemens USA
Senior Manager
(847) 274-0532
mark.halbur@siemens.com

William Coyle
Siemens USA
Business Development Manager
(224) 900-0993
william.coyle@siemens.com

Valerie Klengson
Siemens USA
Business Development Manager
(678) 446-9375
valerie.klengson@siemens.com

About the Siemens EngineeringAdvantage™ Program

The EngineeringAdvantage Program features the tools and information consulting engineer firms need to stay on top of the latest trends and technologies in building design and operation—from specifying the right field device to earning continuing education credits. Let the EngineeringAdvantage Program help you deliver high-performing facilities that exceed owners' expectations. You'll get:

- A dedicated and experienced team of professionals with extensive, real-word experience
- Educational programs and presentations that are AIA registered and may qualify for a range of credits for continuing education
- Technical tools and resources, including specification and product selection programs
- Interactive support at your fingertips

If you have questions about the EngineeringAdvantage Program, would like to be added to the distribution list or have a story idea for an upcoming issue, please contact: **william.coyle@siemens.com**.