Safety through Security

Protecting People, the Environment and Critical Infrastructure against Industrial Security Threats

As industrial operations become more connected, organizations are making significant security investments to help protect their intellectual property, their operations and their brand. However, the inherent safety implications of security risks are too often overlooked. By integrating safety and security programs and following key steps, manufacturers and industrial operators can assess, manage and mitigate the safety implications of security risks in a Connected Enterprise.

LISTEN. THINK. SOLVE.®

Allen-Bradley • Rockwell Software

Rockwell Automation

Introduction

Industrial security is top of mind as organizations implement connected, information-enabled architectures to help improve productivity, efficiency and safety.

Whether it's remote access to production machinery, wireless access to pumping stations, or connecting plant-floor equipment to the IT infrastructure, greater connectivity can provide significant improvements in productivity and safety. But it also increases risks – not only to intellectual property, profits and mission-critical production assets, but also to people and the environment.

Safety systems are designed to detect faults, alert operators and automatically intervene. By altering or attacking safety systems, security breaches can force a standard control system to operate beyond its safety parameters, damage equipment and the environment, or even place workers and the general public in unsafe situations.

Connectivity Brings Opportunity and Risk

A Connected Enterprise connects people, processes and things. It brings together enterprise-level IT and plant-level operations technology (OT) systems into a common network infrastructure. And it harnesses the power of enabling technologies, from data and analytics software to smart devices that make up the Internet of Things (IoT).

"The personnel responsible for operating, securing and maintaining ICS must understand the important link between safety and security. Any security measure that impairs safety is unacceptable."

Guide to Industrial Control Systems (ICS) Security, NIST

What does this mean for manufacturers and industrial operators? It means production intelligence for measuring and improving nearly every aspect of their operations, including quality, productivity, uptime and overall equipment effectiveness (OEE). It means enterprisewide connectivity for instantaneous information sharing and seamless collaboration across an organization. It means remote monitoring of critical production assets and systems dispersed across remote locations.

But for all the opportunities, there are also risks. More connection points can create more entrance points for security threats. These threats can be physical or digital, internal or external, and malicious or unintentional. And they can pose a danger in many ways, including intellectual property loss, disrupted operations and compromised product quality.

Safety is perhaps the least discussed implication of security threats.

When Security Threatens Safety

Breached machine- and process-safety systems can create cascading safety consequences.

For starters, compromised safety systems that don't stop machines when they reach a dangerous state or when a safety device is triggered can expose workers to the very threat from which they were supposed to be protected. Additionally, safety systems that aren't able to stop production beyond certain operating conditions can expose other employees or an entire plant to risks, such as fires, chemical leaks or explosions.

The risks can be especially high in industries where employees work with hazardous or volatile materials, such as in chemical manufacturing. And the risks will only grow as collaborative robotics become more prevalent, with employees and robots working side-by-side on production lines.

Compromised safety systems also could put consumers at risk. Consider the potential impact of a cyberattack that alters processes in a food or pharmaceutical manufacturing operation. It could result in harmful or even deadly contaminations. And even if an attack is discovered before affected product leaves the facility, it could delay the delivery of urgently needed products like life-saving medications.

Likewise, tampered or disrupted processes in critical-infrastructure facilities could impact the critical water and energy supplies on which populations depend.

"Food and beverage manufacturers and distributors use control systems to mix ingredients, package products and transport human-consumed goods. If tampered with, these systems can be abused to contaminate the food supply or cause food shortages."

Critical Control System Vulnerabilities Demonstrated And What to Do About Them, SANS Institute

Dangerous Breaches Already Occurring

Security breaches and vulnerabilities resulting in safety risks aren't just theoretical. They're a reality:

- A cyberattack on a German steel mill resulted in parts of the plant failing and a blast furnace that could not be shut down through normal methods. The plant suffered "massive damage." The incident illustrated the destructive and potentially harmful – effects that security threats can create in industrial operations.[1]
- The FDA put out an alert to medical device manufacturers and health care facilities about certain medical devices being vulnerable to security breaches. One of the vulnerabilities cited was the potential for the devices to be infected or even disabled by malware.[2]
- Verizon reported a likely cybersecurity breach at a facility responsible for supplying and metering water usage. Among Verizon's findings were unexplained valve and duct movements, including manipulation of PLCs that "managed the amount of chemicals used to treat the water to make it safe to drink." [3]
- An oil pipeline explosion in Turkey was publicly blamed on a malfunction, but news reports revealed it was the work of hackers. The explosion resulted in 30,000 barrels of spilled oil. As Bloomberg reported, "Hackers had shut down alarms, cut off communications and super-pressurized the crude oil in the line." [4]

Key Risk Types

Security risks that can result in safety implications can take many forms. Some key risk types include:

Employee Errors: Security risks don't always originate from malicious intent. In fact, one of the most common security risks comes from innocent mistakes. This could include employees or contractors who unwittingly make a network misconnection, download the wrong program to a controller, or plug an infected device into the system. Such seemingly simple mistakes could in fact have major consequences if they lead to systems operating beyond safe parameters.

Disgruntled Employees: Current or former employees familiar with an organization's control system and industrial network can present security and safety threats. A prime example of this involved a worker in Australia who broke into a sewage-equipment control system installed by his former employer and caused 800,000 liters of raw sewage to spill into local parks and rivers.[5]

Hackers Seeking Political or Financial Gain: A manufacturer's intellectual property can be a lucrative target for hackers. At the same time, hackers also may seek to disrupt a manufacturing or industrial operation for financial, competitive or political reasons.

Corporate Espionage: State-sponsored espionage targeting high-value infrastructure and production assets is a constant threat. U.S. Department of Justice officials have said that thousands of companies have been targeted and that such activities represent a "serious threat" to national security.[6]

Cyberterrorism: Malicious acts could seek to disrupt, infect or cripple critical infrastructure. Potential targets could include nuclear plants, water supplies and oil refineries. One such alleged attack involved hackers attempting to seize control of a small dam in New York. The attack failed because the dam was offline for maintenance.[7]

Addressing Safety through Security

Governments concerned about disruptive and dangerous cybersecurity attacks on plants and critical-infrastructure operations are already working with manufacturers and industrial operators.

"Almost half the security professionals surveyed think it is likely or extremely likely that a successful cyberattack will take down critical infrastructure and cause loss of human life within the next three years."

Critical Infrastructure Readiness Report, The Aspen Institute and Intel Security, 2015

For example, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 295 cybersecurity incidents in 2015 across 16 critical-infrastructure sectors.[8]

The three sectors that garnered the most responses were:

- Critical manufacturing (97 incidents)
- Energy (46 incidents)
- Water and wastewater (25 incidents)

Still, much work remains. Organizations need to be more proactive in addressing safety through security. They should incorporate four key elements into their approach:

- Standards Compliance
- Safety and Security Integration
- Risk Analysis
- Risk Mitigation Measures

A Matter of Compliance

Some requirements do exist within safety standards to help manufacturers and industrial operators address safety through security:

- Section 7.4 of **IEC 61508 ("Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems")** directs companies to conduct a security threat analysis if their hazard analysis identifies a reasonably foreseeable "malevolent or unauthorized action" that constitutes a security threat. Unfortunately, this requirement is rarely followed.
- The second edition of **IEC 61511 ("Functional Safety: Safety Instrumented Systems for the Process Industry Sector")**, which is planned for release in 2016, will require that security risk assessments be conducted for safety instrumented systems (SIS). The SIS design also must deliver the necessary resilience against the identified security risks.

These requirements may not be elaborate, but they do provide formal compliance guidelines for addressing security-based safety risks. They should be followed. Meanwhile, standards bodies are also exploring additional updates that could go further in detailing how industry must identify and address safety through security.

Integrating Safety and Security

Safety and security have traditionally been viewed as separate entities, but there is a commonality between them in the approaches used to analyze and mitigate risks.

For example, the concept of "access control" is common between safety and security. In both cases, policies and procedures are built based on business practices, risk-management approaches, application requirements and industry standards. Both also seek to help protect an organization's assets, including its people, processes, equipment and intellectual property.

Manufacturers and industrial operators that want to reduce the likelihood of security-based safety incidents will need to rethink safety in this way. Specifically, they need to start thinking of safety and security in relation to each other.

To understand how this can happen, organizations should first consider the "three Cs of safety," which is a set of practices that best-in-class manufacturers share:

- **Culture (Behavioral):** Employee and company behaviors – including values, priorities, attitudes, incentives and beliefs – that help define how well a company embraces safety.
- **Compliance (Procedural):** Policies and procedures that help a company achieve compliance with appropriate safety standards.
- **Capital (Technical):** Contemporary safety technologies and techniques that help optimize both safety and productivity.

Next, organizations should consider how security can be engrained into each of these core safety pillars. For example:

Culture: In addition to protecting intellectual property, processes and physical assets, security personnel must make protecting safety systems a core value in everything they do. Greater collaboration between EHS, operations and IT teams also is more important. For example, all three teams should work together to develop co-managed objectives for safety and security, and to identify critical safety data requirements from plant-floor systems. And because a strong safety culture involves every employee, a companywide understanding of the relationship between security and safety is needed.

Compliance: Compliance efforts should meet the security requirements in safety standards, such as IEC 61508 and 61511. Conversely, security efforts should follow a defense-in-depth approach, which is recommended in the IEC 62443 ("Security for Industrial Automation and Control Systems") standard series (formerly ISA-99) and elsewhere, and address safety-related security risks at all levels of an organization.

Capital: Companies should use safety technologies with built-in security features. They also should use security technologies that both help protect against safety-system breaches and enable speedy recoveries should a breach occur.

Comprehensive Risk Analysis

Companies should implement a companywide risk-management strategy to manage security threats and vulnerabilities, as well as their potential implications on safety. Two assessments are essential to this strategy:

- A **safety risk assessment** is necessary to confirm compliance with existing safety standards, including the security requirements in IEC 61508 and 61511. The assessment should address not only standard operator functions but all human-machine interactions, including machine setup, maintenance, cleaning and sanitation, and training and administrative requirements. Companies should also expand their existing methods for performing safety risk analysis to analyze risk from cyberattack.
- A **security risk assessment** should describe an organization's overall current security posture regarding software, networks, control system, policies and procedures, and even employee behaviors. It also should outline what steps must be taken to achieve the desired level of security.

While these assessments will be conducted separate from each other, they should work toward the same company-level risk management goals of protecting workers, customers and the environment.

Companies that use a third-party vendor to conduct these assessments should seek out a vendor with expertise in both safety and security. This can help confirm consistency and alignment between the two assessments.

Risk Mitigation Measures

The specific mitigation measures that an organization implements will depend on its unique set of security risks and their potential impacts on safety. However, there are some key mitigation measures that most manufacturers and industrial operators should implement as a best practice:

- **Segmentation into Zones:** This is a core security best practice. It should be used in every plant as part of a holistic defense-in-depth security approach to help limit access to safety systems. An industrial demilitarized zone (IDMZ) with firewalls and data brokers can securely segment the plantwide network from the enterprise network. Also, using virtual LANs (VLAN) and a layer-2 or layer-3 switch hierarchy can create functional sub-zones to establish smaller domains of trust and simplify security policy enforcement.
- **Physical Access:** Many organizations use RFID cards to manage facility access control. But physical-access security should go further than that to protect safety systems. Lock-in, block-out devices should be used to prevent the unauthorized removal of cables and to close unused or unnecessary ports. And control cabinets should be locked to restrict walk-up and plug-in access to the industrial automation and control system devices. More advanced physical-access security also is emerging, such as IP video surveillance systems that can use analytics for facial recognition.
- **Network-Integrated Safety and Security:** CIP Safety™ and CIP Security™ are extensions to the common industrial protocol (CIP), which is the application-layer protocol for EtherNet/IP™. CIP Safety allows safety devices to coexist on the same EtherNet/IP network as standard devices, and enables a safe shut down in the event of a denial-of-service attack. CIP Security incorporates data integrity and confidentiality into EtherNet/IP communications. Working together, devices that incorporate CIP Safety and CIP Security can help protect against data corruption and malicious attacks on safety systems.

- **Safety Products with Built-in Security:** Safety systems and other hardware should include built-in security features. For example, a safety controller that uses keyed software can ensure that firmware is only downloaded from a trusted source, while an access door can restrict physical access to the controller. An industrial managed switch with access control lists (ACL) also can be sure that only authorized devices, users and traffic are accessing a network.
- **Authentication and Authorization:** Security software features can restrict wired and wireless access to the network infrastructure. For example, authentication and authorization security is a key element in human-machine interface software and can limit safety-system access to only authorized individuals. This can help protect against malicious and accidental internal threats. Security personnel can define ***who*** can access the software, ***what*** specific actions they can perform and on which specific hardware, and from ***where*** they can perform those actions.
- **Asset and Change Management:** Asset-management software can automate the discovery of new assets and centrally track and manage configuration changes across an entire facility, including within safety systems. It can detect malicious changes in real time, log those activities and report them to key personnel. If unwanted changes are made, the software can access archived copies of a device program for fast recovery.
- **Vulnerability Management:** Processes and procedures should be developed to help make sure fast action is taken after safety and security advisories are released. This includes having processes in place to immediately review advisories and determine their potential impact. It also includes implementing patch-management procedures for affected products.

Summary

Security isn't only about protecting data and uptime. It's about protecting people and the environment, as well as the critical infrastructures and supplies on which populations depend. Organizations that want to stay ahead of these risks will need to achieve compliance with the latest standards, holistically integrate safety and security, conduct a comprehensive risk analysis, and implement risk mitigation measures using the latest technologies.

Resources

Rockwell Automation has the right mix of safety and security expertise to help organizations address their unique security-based safety issues. We have one of the industry's broadest portfolios of safety solutions, including safety services such as assessments. Our industrial security offerings include network products, free tools and resources, and a full range of industrial security services. We also realize that building more secure systems requires using more secure products. That's why we use a robust security-development process to build security into our products from the beginning.

We're also collaborating with strategic alliance partners, such as Cisco, Panduit and Microsoft, to create a one-stop shop for your industrial security needs. For example, Cisco and Rockwell Automation jointly developed an industrial network security framework as part of the Converged Plantwide Ethernet (CPwE) program. Design guidance, reference architectures and educational resources also are available through the CPwE program.

1) Hack attack causes 'massive damage' at steel works, BBC News, Dec. 22, 2014

2) Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication, FDA, June 13, 2013

3) Data Breach Digest, Verizon, 2016

4) Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar, Bloomberg, Dec. 10, 2014

5) Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia, NIST, July 23, 2008

6) The Great Brain Robbery, 60 Minutes, Jan. 17, 2016

7) U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam, New York Times, March 24, 2016

8) NCCIC/ICS-CERT Year in Review, ICS-CERT, 2015

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication SAFETY-WP035A-EN-P – December 2016