LISTEN.
THINK.
SOLVE.®

Industrial Security

Protecting networks and facilities against a fast-changing threat landscape

Rockwell Automation

Allen-Bradley • Rockwell Software

Security in The Connected Enterprise

Manufacturing and industrial facilities are operating in ways they scarcely could have imagined a few decades ago.

Greater connectivity and information sharing – enabled by technologies such as smart devices, inspired by concepts like the Internet of Things, and brought to life in The Connected Enterprise – are significantly transforming companies and their operations. They're converging information technology (IT) and operations technology (OT) systems and using new technologies such as mobile, analytics, cloud and virtualization to do more than ever before.

However, just as the nature of manufacturing and industrial operations has changed, so have the security risks. More connected operations can create more potential entrance points for industrial security threats. These threats can come in many forms – physical or digital, internal or external, malicious or unintentional.

Industrial security must address a wide range of concerns, including:

- Safeguarding intellectual property and other valuable information.
- Protecting operations from intrusions that could impact productivity, product quality, worker safety or the environment.
- Maintaining critical systems that populations depend on, such as wastewater treatment systems.
- Achieving network availability and avoiding network-related downtime.
- Enabling, but also properly controlling, remote access to industrial operations.

What is The Connected Enterprise?

By converging historically separate systems and connecting people, processes and technology across an organization, The Connected Enterprise creates new opportunities to access, share and act on data from within your operations.

A 2014 Kaspersky Labs survey revealed **21 percent of manufacturers** suffered an intellectual property loss within a one-year period.[1]

"My biggest security concern is allowing a breach at a customer site that results in loss of safety."

– Engineering manager at an industrial manufacturing company

[1] Kaspersky Lab Survey: One in Every Five Manufacturing Businesses Has Lost Intellectual Property to Security Breaches Within the Past Year, Kaspersky Labs, Aug. 13, 2014.

A Holistic Approach

The growing adoption of smart manufacturing and connected operations combined with today's highly robust threat landscape requires a renewed commitment to industrial security.

First, don't succumb to paralysis from over analysis. It can be overwhelming to think of all the possible threats. Instead, focus on the probable threats. This can help you more quickly and easily begin implementing strong security practices.

Also, avoid approaches that limit security:

- No single security product, technology or methodology is sufficient for today's abundance of threats.
- A security-through-obscurity approach lacks meaningful measures.
- Proprietary networks rely on a single vendor and fall short when they don't take advantage of the plethora of other IT tools, security features and innovations available from the marketplace.

Industrial security must be holistic. It should extend from the enterprise through the plant level and even out to end devices, and address risks across your people, processes and technologies. It also should involve collaboration between IT and OT personnel. Both sides have vital roles to play in establishing a secure network architecture.

Three key considerations for undertaking a holistic approach include:

1. **Security assessment:** Understand your risk areas and potential threats.
2. **Defense-in-depth security:** Deploy a multi-layered security approach that establishes multiple fronts of defense.
3. **Trusted vendors:** Verify that your automation vendors follow core security principles when designing their products.

Basic cybersecurity practices within many industrial organizations continue to be an afterthought or **significantly less than needed**.[1]

[1] ICS Cybersecurity for the C-Level, U.S. Department of Homeland Security, September 2015.

Security Assessment

Developing and implementing an effective industrial security program requires that you first understand the risks and areas of vulnerability that exist within your organization.

A security assessment will help you understand your current security posture regarding your software, networks, control system, policies and procedures, and even employee behaviors. It should be the starting point for any security policy.

A security assessment's deliverables should include at a minimum:

- An inventory of authorized and unauthorized devices and software.
- Detailed observation and documentation of system performance.
- Identification of tolerance thresholds and risk/vulnerability indications.
- Prioritization of each vulnerability, based on impact and exploitation potential.

The final outcome of any security assessment should include the mitigation techniques required to bring an operation to an acceptable risk state.

Executive management should enforce the implementation of **suitable security controls** based on risk assessments, and not tolerate cybersecurity being sacrificed to the **'do not touch it'** attitude.[1]

How Secure is Your Organization?

When it comes to security, there's too much at stake to let your assessment be a guessing game. Whether you're unsure of where to begin or lack in-house security expertise, consider using outside services for help.

The Rockwell Automation Security Assessment Tool is a free, secure and confidential tool that can help you identify your current risk level, benchmark it against other similar facilities, and identify potential mitigation methods.

Rockwell Automation also offers security assessments through its Network and Security Services. By collaborating with strategic alliance partners, including Cisco, Panduit and Microsoft, Rockwell Automation becomes a one-stop shop for your industrial networking needs.

[1] Cyber Security of Industrial Control Systems, TNO, March 2015.

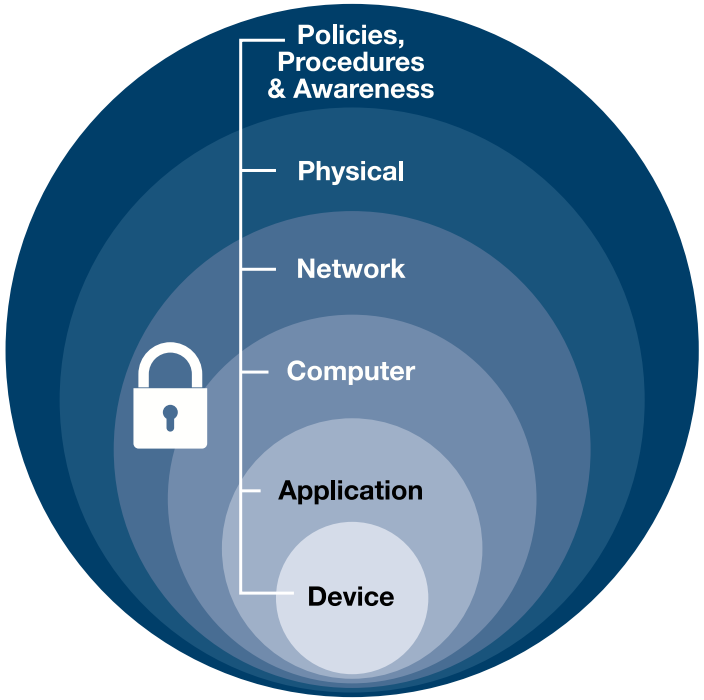
Defense-in-Depth Security

Industrial security is best implemented as a complete system across your operations.

Defense-in-depth (DiD) security supports this approach. Based on the notion that any one point of protection can and likely will be defeated, DiD security establishes multiple layers of protection through a combination of physical, electronic and procedural safeguards. Just like a bank uses multiple security measures – such as video cameras, a security guard and a vault – this helps make sure threats encounter more than one line of defense.

A defense-in-depth security approach consists of six main components:

1. **Policies and Procedures**
2. **Physical**
3. **Network**
4. **Computer**
5. **Application**
6. **Device**



Broad Support for Defense-in-Depth

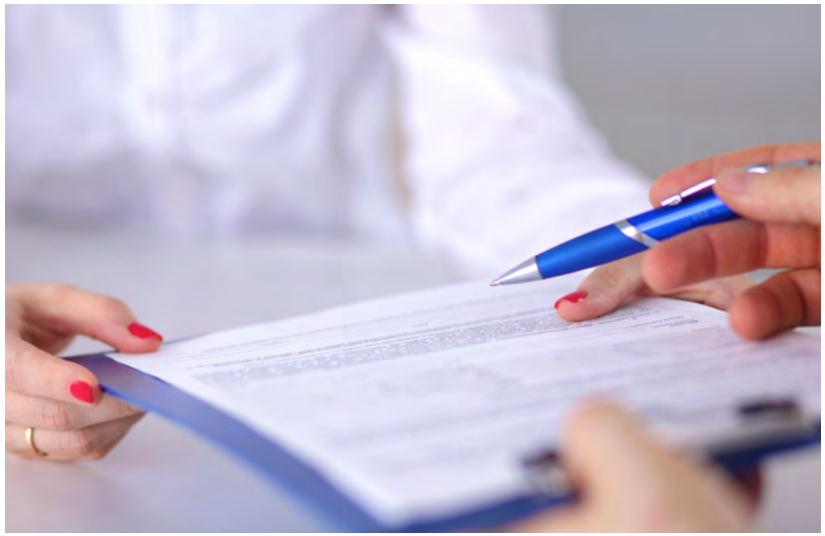
The Defense-in-depth security approach is recommended in:

- IEC 62443 standard series (formerly ISA-99).
- NIST Special Publication 800-82.
- U.S. Department of Homeland Security/Idaho National Laboratory Report INL/EXT-06-11478.

Defense-in-Depth Security

1. Policies and Procedures

Policies and procedures play a critical role in shaping workers' behaviors to follow good security practices and confirming the appropriate security technologies are used. For example, policies that control human interaction with manufacturing and industrial operating systems can help prevent information theft.



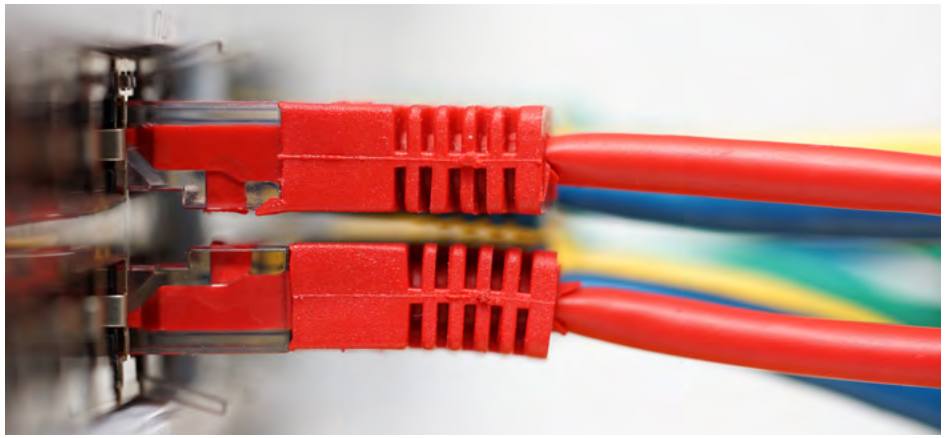
Only 20% of industrial companies surveyed said they have strong physical security policies.[1]

2. Physical

Physical security should limit personnel access to not only areas of a facility but also to entry points on the physical network infrastructure, such as control panels, cabling and devices.

At the facility level, access control technology such as networked key cards can help restrict access to the plant floor, control rooms and other areas to authorized personnel only. Cameras have long been used to monitor facility activities, but advanced video analytics solutions can protect sensitive locations and network access points in new ways, such as through facial recognition, perimeter violations and thermal identification.

The physical infrastructure and components, such as switches, routers and gateways, also must be protected against intrusions, tampering and accidents. Lock-out devices can prevent unauthorized access to USB ports to stop the unwanted removal of data and block potential virus uploads, while lock-in devices can prevent unauthorized cable removals and keep vital connections in place.



[1] TechValidate survey of Rockwell Automation customers, January 2016.

Defense-in-Depth Security

3. Network

A network security framework should be established to help safeguard your network infrastructure against cyberattacks. This requires close cooperation between IT and OT, including a robust discussion between the two groups about the technologies and policies needed to best protect your assets and your ability to innovate.

One of the technologies discussed should be an industrial demilitarized zone (IDMZ), which creates a critical barrier of protection between the enterprise and industrial zones. An IDMZ restricts traffic from directly traveling between the two zones and can help better manage access through authentication enforcement or the monitoring of traffic for known threats.

"My biggest security concern is my company's lack of knowledge and experience in process control network security."

– Plant manager at an industrial manufacturing company

A Network Infrastructure's Role in Security

A unified network infrastructure is built on a physical network fabric and information architecture that uses standard, unmodified Ethernet and IP technology.

Network infrastructures such as EtherNet/IP™ that use the Internet Protocol enable organizations to take advantage of the latest work being done by cybersecurity experts both within and outside of the industrial sector.

Defense-in-Depth Security

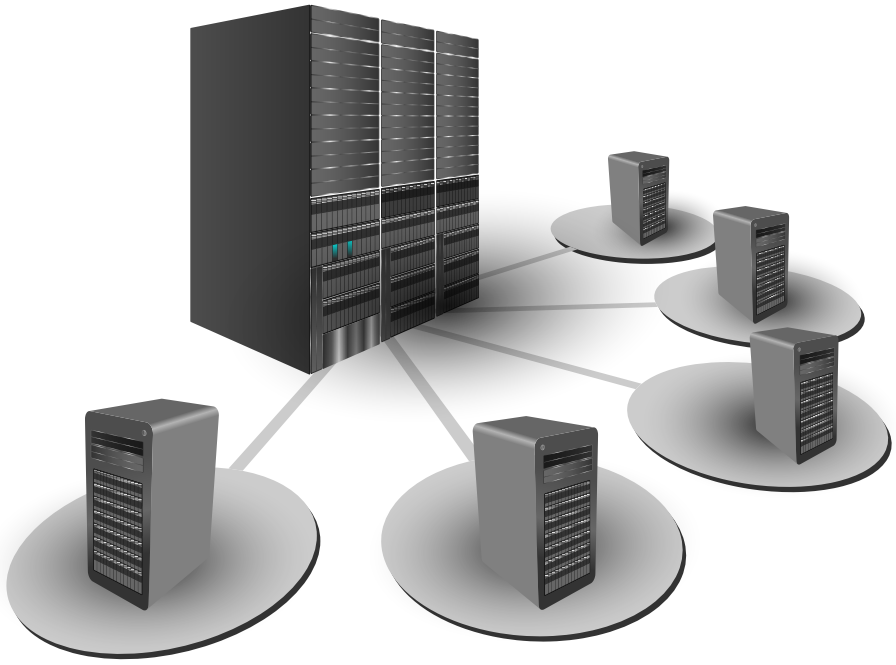
Segmenting areas of the plant floor into virtual local area networks (VLANs) is a good security practice at the network level. VLANs are broadcast domains within a switched network. Smaller VLANs are easier to manage and maintain real-time communications. They can help isolate devices from those that have been compromised, which keeps the negative impact within a single VLAN.

Firewalls with intrusion detection and prevention systems (IDS/IPS) should be deployed within and around the industrial network to manage and limit network traffic. Firewalls also should use deep packet inspection (DPI) to identify, authenticate and re-route data to help improve network performance and reduce security threats.

Lastly, it is important to follow security best practices when using wireless networks. This includes using device-authentication and data-encryption methods that align with IEEE 802.11, which is increasingly becoming the standard for deploying wireless networks in industrial applications.

"Wireless is my biggest security concern because we're using more and more wireless devices and networks in our plant."

– Plant manager at a large chemicals company



Resources Address Security Risks

Rockwell Automation and Cisco jointly developed the Converged Plantwide Ethernet (CPwE) program, which includes best practices, recommendations and reference architectures.

These resources provide the foundation for designing and deploying future-ready network infrastructures, as well as for managing network access security and addressing unknown risks.

Training, education and certification options are available for workers involved in managing network infrastructure.

Defense-in-Depth Security

4. Computer

The top means of intruder entry into automation systems is through software vulnerabilities.

Security patch management should be established to track, evaluate, test and install cybersecurity software patches. Antivirus software, application whitelisting and host intrusion-detection systems can further harden computer assets. Unused Windows® programs, protocols and services should be removed, and infrequently used USB, parallel and serial interfaces also should be protected.

Over half of industrial companies surveyed said **their top security challenge** in the next three years will be **enabling and controlling secure remote access**.[1]

5. Application

Security devices should also be incorporated at the manufacturing or industrial application level as part of a DiD approach.

A role-based access control system can restrict access to critical process functions or require operators to enter log-in information before they access applications. A security lock on the controller can help prevent unwanted physical access, and authentication, authorization and accounting (AAA) software can restrict and monitor application access and changes. Tamper detection capabilities also can detect and record unwanted application modifications.

[1] TechValidate survey of Rockwell Automation customers, January 2016.

Defense-in-Depth Security

6. Device

Device authentication and unauthorized device identification can help make sure only trusted devices are used.

Additionally, changing the out-of-the-box default configurations for embedded devices can help make them more secure in areas such as restrictive access and change management. For example, users can control which tags can be modified from HMIs and external applications, or define tags as constants, which cannot be modified by controller logic.

The default security settings will vary across devices, affecting how much time and effort is required to harden each device.

Trusted Vendors

Your automation vendors are just as integral to helping you meet your security goals as they are your production, quality and safety goals.

Before selecting vendors, request they disclose their security policies and practices. Consider if they follow five core security principles – defined by Rockwell Automation – for designing products used in a control system:

Secure Network Infrastructure

Vendors can help keep information in the automation layer secure and confidential. For example, embedded technology can validate and authenticate devices before they are granted access to a network.

Authentication and Policy Management

Company policies dictate data access levels for employees. Automation products can support these policies using access control lists to manage user access to devices and applications.

Content Protection

Intellectual property is the lifeblood of your operations. Your automation solutions can help protect it by assigning passwords to routines and add-on instructions, and by using digital rights management to limit users' ability to view and edit device data.

Tamper Detection

Built-in tamper detection can detect any unauthorized system activity and alert the right personnel. It also can log key details, such as where the attempted intrusion took place, how it occurred and if anything was modified.

Robustness

A robust vendor security approach includes providing security training to employees; using design-for-security development practices; testing products to global security standards; conducting final security reviews before products are released; verifying processes stay current with standards and technologies; and having a plan in place to address vulnerabilities.

A Better Way to Build Trucks

During a plant upgrade, Daimler Trucks North America (DTNA) used aspects of the Converged Plantwide Ethernet (CPwE) validated design guides from Cisco and Rockwell Automation to jump start the network architecture design and deployment.

The new network provides secure and reliable Wi-Fi connectivity everywhere on the shop floor and in office areas.

Bringing its IT and OT departments more closely together helps DTNA meet its security and compliance requirements.

Now, one converged plant-to-business network provides secure, reliable connectivity everywhere.

Monitor and Evolve

Security threats aren't relenting. They will only continue to evolve as the industry changes its security practices or implements new defense. Your risk management strategy must keep pace.

Your security program should have no end state. It should be ongoing, evolving with or ahead of the changing threat landscape. Some tips for keeping your security program dynamic and relevant include:

- **Educate your workforce:** Security requires the support of everyone. Workers should be educated in areas such as avoidance techniques for dealing with phishing, USB devices and other security threats.
- **Scrutinize your supply chain:** Your vendors are just as vulnerable to security attacks as you are. Before selecting vendors, request they disclose their security policies and practices.
- **Don't wait for an alert:** Cybersecurity threats are stealthy and designed to defeat a range of defenses. As a result, your security measures should be trusted but also verified. Routinely check audit logs, registry dates and time stamps for unexpected changes.
- **Support security training:** Knowledge is power for IT and security professionals. Provide the necessary investments in education, training and certification to help keep these workers up to date on security challenges and best practices.
- **Evolve with technology:** New technologies can have unique security needs. For example, mobile device management should be used to restrict access and monitor mobile access to the enterprise. Cloud computing services should offer proven security, such as through the Microsoft Azure™ platform.

Symantec reported that more than **317 million new pieces of malware** were created in 2014 – or an average of nearly **1 million per day**.[1]

Cloud Security

M.G. Bryan, a heavy-equipment provider for the oil and gas industry, teamed with Rockwell Automation to develop a scalable solution for remote asset management of fracturing vehicles.

Using Microsoft's Windows Azure cloud-computing platform combined with the FactoryTalk® software suite from Rockwell Automation, M.G. Bryan has enhanced, secure and instant visibility into remote-asset data, which has improved uptime and productivity for its customers.

"It is important not to fall victim to a 'my data needs to be behind a door' mentality," said Josh Rabaduex, director of engineering for M.G. Bryan. "While the cloud can seem like a virtual world, in many cases it can actually provide better security and redundancy than a traditional system."

[1] 2015 Internet Security Threat Report: Attackers are Bigger, Bolder and Faster, Symantec, April 14, 2015.

Summary

The vastness of today's security threats combined with not knowing how, when or where an attack will occur can be daunting. The approaches outlined here will put you in line with best industry practices for securing your intellectual property, while also helping you protect your facilities, assets, employees and competitive advantages.

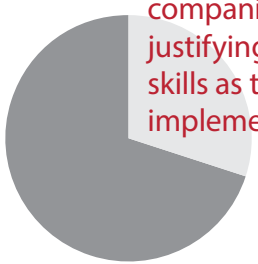
Resources:

Rockwell Automation provides a range of **security solutions and services** to help you manage potential security threats and build more secure industrial control systems and network architectures.

Rockwell Automation Network and Security Services can help you wherever you are in your security life cycle – from assessments and design to implementation and security monitoring.

The **CPwE reference architectures** offer education, design guidance, recommendations and best practices for addressing security risks while navigating the IT/OT convergence process.

Industrial IP Advantage is an online community where best practices and resources are shared for using standard, unmodified Ethernet and Internet Protocol in industrial settings. It also offers e-learning for addressing security and other key aspects of industrial networking.



Nearly **two-thirds** of industrial companies surveyed cite cost justifying and having adequate skills as their biggest fears about implementing security solutions.[1]

The **Rockwell Automation Security Assessment Tool** is a free, secure and confidential tool that can help you identify your current risk level, benchmark it against other similar facilities, and identify potential mitigation methods.

A Shared Commitment to Security

Rockwell Automation has longstanding strategic alliances with industry leaders, such as Cisco, Microsoft, AT&T and Panduit. Our complimentary offerings and combined expertise can help you understand your unique security needs and integrate protection at every level.

[1] TechValidate survey of Rockwell Automation customers, January 2016.

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 SECUR-WP004A-EN-E – July 2016