ARC VIEW

JUNE 10, 2021

Enabling Safe and Secure Industrial Operations

By Sid Snitkin

Keywords

Digital transformation, Industrial cybersecurity, Rockwell Automation

Summary

Industrial companies need security programs that can manage today's increased cyber risks.

The risks of serious industrial cyber incidents have grown significantly. Digital transformation efforts are proliferating new attack pathways with external connections to cloud services, vendors, and remote workers. IoT devices are introducing new vulnerabilities into critical control systems. Industrial companies have become prime targets for ransomware and sophisticated attacks on critical infrastructure.

The risks of serious industrial cyber incidents have grown significantly. Digital transformation and advanced threats demand more active cybersecurity strategies that support rapid detection and response to any suspicious behavior. Companies also need to ensure that trusted partners are dedicated to ensuring the security of critical OT products and services.

While many industrial companies have already invested in OT cyber defenses, most of these programs were built for yesterday's threat environment. Digital transformation and advanced attacks demand more active cybersecurity strategies that include the people, processes, and technologies to support rapid detection and response to any suspicious behavior. Companies also need to ensure that trusted partners are dedicated to ensuring the ongoing security of critical OT products and services.

Recently, ARC Advisory Group discussed these new security challenges with executives from Rockwell Automation. As a leading supplier of automation systems, they have a deep understanding of what is required to ensure the security of critical OT systems and a strong interest in ensuring the security of their customer's systems. A summary of their broad security activities and capabilities is included in this report.

OT Cybersecurity is Under Attack

Sophisticated attacks on manufacturers and critical infrastructure operators are increasing at an alarming rate. Yesterday, most industrial companies only needed to protect operations from general malware floating around the internet. Today, companies need to be concerned about targeted attacks by sophisticated adversaries and compromised software downloads from suppliers. A recent research report also showed that one-third of all ransomware attacks have been against industrial companies.

Digital transformation is occurring at a rapid pace across the industrial landscape. Operators, inspectors, and maintenance personnel are using mobile devices, augmented reality (AR), and digital twins to improve efficiency and effectiveness. Robots and autonomous vehicles are being used to drive higher productivity and process consistency in manufacturing. IoT sensors and analytics are helping managers optimize workflows, improve product quality, and reduce safety incidents. COVID-19 has accelerated many of these efforts by enabling widespread connectivity of remote workers and vendors to critical systems in order to reduce process downtimes and lower service costs.

Every facility should evaluate their OT cybersecurity program to ensure that it provides adequate mitigation for the cyber risks of sophisticated targeted attacks, ransomware, and digital transformation programs.

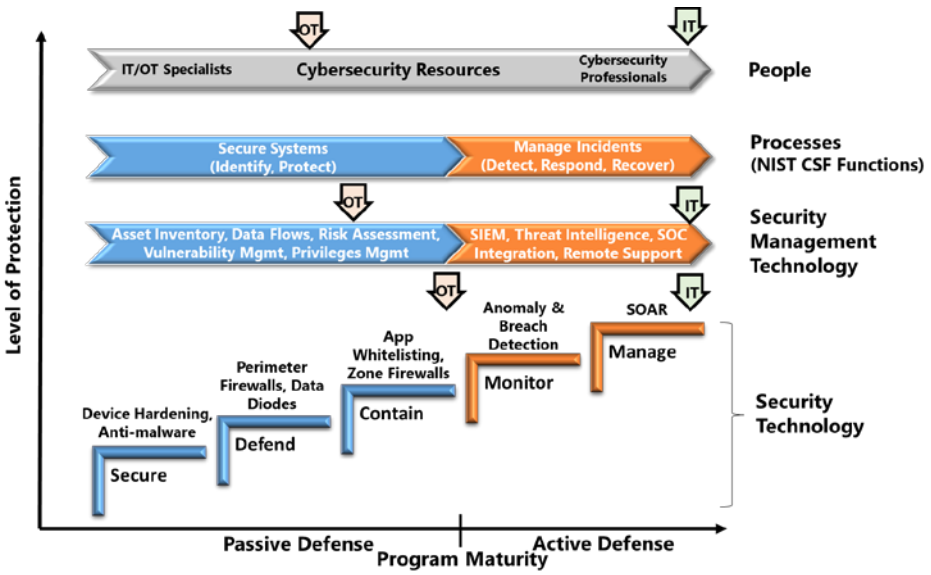
All of these developments have increased the risks of serious cyber events that can impact safety and business continuity. External connections and cloud apps have expanded the pathways for attackers to access critical OT systems. Insecure-by-design IoT devices are providing launchpads for internal system attacks. Mobile devices with unauthorized apps are exfiltrating confidential information and injecting malware into business workflows.

Trying to deal with each of these security issues on an individual basis is a fool's errand. Rapid detection and response to anomalous behaviors is essential to block such attacks before they wreak serious operational impacts. Companies also need comprehensive, resilient security strategies that can keep up with the digital transformation demands of business leaders.

Current OT Security Programs Can't Deal with Today's Threats

ARC's Industrial/OT Cybersecurity Maturity Model highlights OT cybersecurity requirements and the weaknesses in current programs. This model

provides a roadmap of the steps involved in building a defense-in-depth cybersecurity strategy that aligns with the NIST Cybersecurity Framework. Each step addresses a specific, easily understandable security issue such as **securing** individual devices, **defending** systems from external attacks, **containing** malware spread, **monitoring** for signs of latent compromises, and **managing** active attacks and cyber incidents. Each step adds a layer of protection and has an associated set of technologies that accomplish its goals. Blue and orange colors in the model distinguish basic defensive technologies from advanced technologies that are required to support active defenders.



ARC Cybersecurity Model Shows Current State of Industrial Cybersecurity Programs

Resource requirements grow as programs add layers. Security technologies need periodic updates, alerts need to be analyzed, and compromises need to be addressed. OT personnel with basic tools may have been able to maintain passive defenses, but active defense strategies require cybersecurity professionals and sophisticated tools for forensics and remediation.

The ARC model provides a tool for users to assess maturity individually for people, processes, and technologies. The least mature element determines the maturity and protection level of the overall program. As the figure shows, industrial IT cybersecurity programs are generally more mature than those for OT.

IT security programs generally include advanced solutions for passive and active defense, and they have teams of cybersecurity professionals equipped

with powerful cybersecurity management solutions. This enables timely management of all vulnerabilities and rapid detection and response to all anomalous behaviors.

No industrial company can afford to accept the risks of weak OT cyber defenses. A single incident could jeopardize worker safety, product quality, regulatory compliance, and operational continuity.

Typical OT cybersecurity programs only have passive defenses and many lack the people and tools needed to maintain the effectiveness of these basic security layers. Few companies have invested in the active defense capabilities needed to manage sophisticated attacks. They likewise lack the resources and expertise to ensure secure deployment of new digital transformation efforts.

No industrial company can afford to accept the risks of weak OT cyber defenses. A single incident could jeopardize worker safety, product quality, regulatory compliance, and operational continuity. Every facility needs to evaluate their OT cybersecurity program to ensure that it provides adequate mitigation for the risks of sophisticated targeted attacks, ransomware, and poorly secured digital transformation programs.

Rockwell Automation Security Spans ARC's Model

ARC's discussion with Rockwell Automation executives demonstrated their deep commitment to reducing the risks of OT cyber-attacks. This is reflected in the design of their ICS products as well as the security solutions and services they offer to keep customer sites secure.

Secure-by-Design ICS Products and Systems

Security is a priority in the development of all of Rockwell Automation's products. The company's security development lifecycle (SDL) program has been certified by TÜV Rheinland to meet the requirements of the stringent IEC 62443-4-1 standard. This includes maintaining ongoing security competency on standards, technologies, and tools; collaboration with partners to develop more robust, secure products; and comprehensive testing to verify that products meet established security requirements and conform to relevant standards.

Rockwell Automation's SDL is one of the key capabilities that enable the company to produce products that meet the IEC 62443-4-2 technical requirements for IACS components. Rockwell products developed according to this

Publication SECURE-AR001A-EN-P - June 2021

standard include a variety of features and capabilities to meet critical security requirements like secure boot, firmware signing, and CIP security.

IEC 62443-3, the security requirements for defense of industrial control systems, is used as the basis for the company's reference architectures and technical guidance. Rockwell also offers access to subject matter experts to help users and system integrators meet the intent of 62443-3 in deployed systems.

Security Technology Solutions

Rockwell Automation's product portfolio includes security technology solutions that add additional layers of protection to their secure-by-design control products. These solutions provide perimeter protection, network segmentation, secure communications between control elements, and data protection for users of thin client devices.

Stratix® 5950 Security Appliance

The Stratix 5950 security appliance leverages Cisco ASA Firewall technology to control network traffic according to configured security rules. This enables companies to monitor and control application-level network communications and block malicious traffic. The device's deep packet inspection (DPI) technology provides granular control of allowable network traffic and blocks actions at the application layer, such as CIP Write or CIP Read commands.

CIP Security

CIP Security adds an extra layer of defense against cyber compromises. A self-defending CIP device can reject data that has been altered, reject messages sent by untrusted people or untrusted devices, and reject messages that request actions that are not allowed.

FactoryTalk Security

FactoryTalk Security provides access control and policy management that prevents access by unauthorized users and minimizes exposure to internal threats.

ThinManager

ThinManager securely enables use of applications (e.g., HMI) on thin clients and mobile devices without storing data on those devices. In addition, location resolvers (WiFi, Bluetooth, QR code) capabilities allow users to limit locations where applications can operate. For example, a Bluetooth beacon

can be used to limit mobile applications to operators who are in visual proximity to machine(s) being controlled.

Security Management Technology

Rockwell Automation recognizes that security requires periodic updates of software to address new vulnerabilities. The company offers various capabilities and technologies to help customers perform these essential tasks.

Vulnerability Monitoring and Patches

Rockwell accepts responsibility to proactively test their products for security vulnerabilities on an ongoing basis. Customers are informed of new vulnerabilities and patches and updates required to mitigate these new risks.

Source Protection

Source protection limits users' ability to view and edit control programs, like equipment phase state routines, without the associated source key or license.

FactoryTalk AssetCentre

FactoryTalk AssetCentre software helps users track system changes for compliance and troubleshooting purposes. This product secures system access, monitors user actions, tracks firmware versions, manages historical versioning, provides automatic backups, and compares operations on supported devices.

ARC's discussions with Rockwell Automation executives demonstrated their deep commitment to reducing the risks of OT cyber-attacks.

FactoryTalk Network Manager

FactoryTalk Network Manager software provides visibility and insight into the performance of automation networks. It allows users to view network topology and manage switch-level alarms.

Industrial Security Services

Rockwell Automation leverages their deep knowledge of industrial processes, control systems, and IT to offer a range of cybersecurity support services. These services help users perform the two major cybersecurity management processes outlined in ARC's model - Secure Systems and Manage Threats. As noted in the model, these processes encapsulate the five key functions described in the NIST CSF.

Secure Systems (NIST Identify and Protect)

Assessments are an essential part of every cybersecurity strategy. Initial assessments provide the information to build a proper security program. Ongoing assessments provide compliance data and ensure that systems are meeting security goals. Rockwell Automation service personnel have the skills and resources to safely perform these assessments in industrial environments. The company also offers assessments to achieve compliance with various standards including NERC CIP, NIST 800-53, and NIST 800-82.

Rockwell also has the resources and expertise to design and implement a security program to address security deficiencies. This includes recommendations for product updates, compensating controls, security technologies, and security maintenance solutions needed to meet user passive and active defense goals.

Rockwell has the resources and expertise to safely perform assessments, as well as design and implement a program to address security deficiencies.

Manage Threats (NIST Detect, Respond, and Recover)

Even robust security programs can be compromised by sophisticated attacks. So smart companies enable rapid detection and response to minimize the impact of these events. Rockwell Automation's threat detection services can help companies implement these capabilities. These services include use of anomaly and breach detection technology to establish normal operation baselines and alert defenders to investigate situations that do not conform to expected patterns.

Rockwell's industrial security services team can also help companies develop incident response plans. Rockwell's back-up and recovery services ensure that companies always have near real-time records of production and application data to rapidly restore operations after any cyber incident.

IT/OT Convergence Guidance

Rockwell Automation maintains close partnerships with industry-leading partners in IT and security, including Cisco, Claroty, Microsoft, and others. They co-developed the Converged Plantwide Ethernet (CPwE) architecture with Cisco to give users a set of tested and validated architectures that span IT and OT networks. This includes documented architectures, best practices, guidance, and configuration settings that enable scalable, reliable, secure, and future-ready industrial network infrastructures. Rockwell Automation

can also help companies implement a robust network, confirming that it meets installation, security, and performance requirements.

Conclusions and Recommendations

The risks of serious cyber incidents are clearly growing for industrial companies. Every industrial company should:

- Review OT cybersecurity strategies to ensure that facilities have the maturity needed to deal with sophisticated attacks, ransomware, and compromises in key supplier products and services.
- Review OT cybersecurity strategies to ensure that current and future digital transformation programs include the security controls needed to mitigate the risks of insecure IoT devices and broad-based connectivity with cloud services, vendor systems, and remote workers.
- Consider IT-OT cybersecurity convergence and third parties to fill gaps in the availability of experienced cybersecurity professionals.

Existing gaps in OT security strategies and policies add urgency to the need for every company to address these issues. Don't let the lack of resources delay action. As our review of Rockwell Automation illustrates, there are companies that can help you avoid a security event with devastating impact on personnel safety and operational performance. The only roadblock to a secure future is the decision to act.

For further information or to provide feedback on this article, please contact your account manager or the author at srsnitkin@arcweb.com*. ARCViews are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.*