SECURITY DEVELOPMENT LIFECYCLE PRODUCT DEVELOPMENT PROCESS

> *We build security into our products with a robust security development lifecycle.*

Manufacturing and industrial operations cannot afford to ignore the paradigm shifts brought about by new technologies. Delivering a fully integrated working environment, where information is available and actionable in real-time, these technologies offer unprecedented opportunities to optimize productivity and minimize unnecessary costs.

However, with the significant benefits of connecting your site and production assets come greater security risks, both internal and external. Therefore, it is our responsibility to build products that can be integrated into industrial control systems to provide a more secure production environment.

Building more secure systems requires the use of products that are developed with security quality over their entire lifecycle. Rockwell Automation uses a robust, structured security lifecycle to help build more secure products.

Educate
Security competency

Building secure products begin with awareness and competency of our people. We provide in-depth and comprehensive training for testers, engineers and software designers, to build and maintain their product and system security skills.

Our teams receive ongoing training on the standards, technologies, and tools needed to implement the latest security policies and practices throughout the product lifecycle.

Additionally, Rockwell Automation collaborates with its partners and learns from other research and development institutions to help develop more robust, secure products for industrial environments.

Design
Design for security

Rockwell Automation has received ISA/IEC 62443-4-1 certification, having adopted specific security development practices into our products and system development processes. These practices help ensure that our products adhere to corporatewide security standards and requirements, using verified, authentic components from an approved supplier network.

ISA/IEC 62443-4-1 is considered the benchmark certification, demanding that we use various review and analysis tools, such as static code reviews, attack surface analysis, threat modeling, and digital signatures, to thoroughly design security in our products.

As part of the design process, we include designated security experts in security architecture and design reviews, and leverage industry expertise in embedded systems and development through our partner ecosystems.

Verify
Test to standards

Comprehensive testing is conducted to verify that the design and implementation meet the security requirements established and to validate conformance to relevant globally recognized standards ISA/IEC 62443.

We verify our products meet necessary security and performance requirements by:

- Validating adherence to global security standards, product requirements and designs

- Conducting security functional and system testing

- Developing methodologies and tools compliant with global security standard ISA/IEC 62443

- Leveraging third-party security firms to validate solutions

Release
Confidence

When the product has been thoroughly verified, it is evaluated for release, including image verification and a series of security reviews.

A final security review is conducted by an independent body to help ensure that the product complies with requirements and specifications. This review is performed by our Product Security Office prior to release.

Maintain

Assess and update

Because standards and technology are constantly evolving, Rockwell Automation takes a continuous improvement approach to managing policies and processes. This allows the organization to assess and update security processes regularly – helping build robust products effectively.

We maintain our processes to reflect best practices and support standards through:

- Corporate-wide governance and risk management

- Risk reduction through continuous improvement

- A designated Product Security Office that assesses and updates security processes regularly

- Ongoing testing and qualification of patches for operating systems and end-point security solutions

Respond
Awareness

We have a plan in place to address vulnerabilities when they are discovered. Using a structured incident response process our product security incident response team evaluates and mitigates issues and communicates with our customers the actions taken throughout the process.

We work with national response organizations, such as ICS-CERT and the Center for the Protection of National Infrastructure (CPNI), to communicate and notify the broader community.

Rockwell Automation also actively works with research communities to identify and resolve vulnerabilities, leverage research, and aid in our future security development efforts.

Learn more about our Network and Security solutions.

Rockwell Automation, Inc. (NYSE:ROK), the world's largest company dedicated to industrial automation, makes its customers more productive and the world more sustainable. Throughout the world, our flagship Allen-Bradley® and Rockwell Software® product brands are recognized for innovation and excellence.

Follow ROKAutomation on Facebook, Twitter and Google Plus. Subscribe to us on Youtube. Connect with us on LinkedIn.

Listen. Think. Solve. and PartnerNetwork are trademarks of Rockwell Automation, Inc. Trademarks not belonging to Rockwell Automation are property of their respective companies.

www.rockwellautomation.com