GE
Industrial Solutions

Cyber Security: PACSystems RX3i

Availability and Security for Industrial Internet Applications

Cyber Security in the Age of the Industrial Internet

GE is leading the development of the Industrial Internet, which helps companies to achieve new levels of performance and productivity by connecting machines, data, insight, and people.

GE recognizes that this vision of the Industrial Internet requires products and systems with comprehensive cyber security capabilities, and is committed to developing secure and reliable products for companies within the industries it serves.

As technology innovates and evolves, cyber security issues and concerns will grow right along with it. When everything is connected, every business is affected and therefore every business is vulnerable. This means we have to change the way we think about cyber risk. GE deploys a Secure Development Lifecycle process which incorporates security considerations in all phases of product development, from initial planning through release.

For our customers, secure control solutions boost productivity, maintain system availability, and protect valuable operational information and customer data. Industry looks to GE to help protect their system investments, reduce operational risk, protect the environment, and maintain their customers' trust.

GE's Approach to Cyber Security

Security is a top priority for GE. We're working hard to protect our company, our assets, our employees and our customers – using a risk-based approach to balance the benefits of open connectivity, productivity enhancements, and Operational Technology (OT) security. As technology and the nature of threats and risks are changing, GE is evolving to address the ever-changing threat landscape.

GE's approach to cyber security begins with a robust cyber-hardened platform that forms the core of the industrial automation control system, which is then augmented through application of multiple layers of defense at the plant, network and system levels. Product features can be enabled to manage all aspects of remote access and external communications. GE's cyber-hardened platforms are designed to meet industrial security certification standards. Firewalls help protect networks from intrusion. These and other physical, mechanical, and electronic barriers and processes help to defend critical processes and operations.

GE works with customers, industry working groups and standards bodies, government agencies, and the security research community to continually improve the security of industrial control systems and global infrastructure. We are committed to maintaining the integrity, availability, and confidentiality of customer systems and data.

PACSystems RX3i

Availability and Security for Industrial Internet Applications

The PACSystems* RX3i controller provides the foundation for Industrial Internet connectivity. It is a powerful, modular Programmable Automation Controller that improves productivity through higher performance and system availability. The RX3i is built on open standards for easy upgrades without application interruption or rework.

In the world of the Industrial Internet, no longer can a system assume that there is no need for self-protection on a plant floor or in a remote location. The RX3i is not only designed to meet the security requirements of today's connected industry, but it also provides more information, more securely. To this end, the RX3i includes the latest security features to help protect data and processes from attacks and unauthorized access.

Achilles Level 2 Certification

RX3i has achieved Achilles Communications Level 2 Certification, meaning it has been independently verified to meet rigorous industry-recognized standards for reliability and communications robustness.

Role-Based Access Control

User access to the RX3i PLC platform is accomplished through Proficy Machine Edition integrated deployment environment (IDE). At logon, privileges are assigned to the user based on pre-defined levels of authorization. Each level of authorization enables a specific set of user rights according to the role assigned to the user account, enhancing system security.

Signed Firmware Updates

All Rx3i CPUs are updated using firmware digitally signed by GE. This helps ensure that only core operating system software supplied by GE will run on the PLC and that it is has not been tampered with since it left the factory.

Cyber-Hardened Platform

The RX3i platform has undergone extensive testing to ensure that it will perform under the most extreme network conditions, such as "man in the middle" and denial of service attacks. The controller passes all tests specified to meet Achilles certification, indicating the robustness and stability of the system design.

Secure User Authentication

GE uses an industry standard method of password generation that does not require the actual password to be transmitted across the network without encryption, preventing any possibility of a "man in the middle" attack.

Option to Require Physical Presence to Change Application

The Rx3i is equipped with a switch on the front panel that prevents any update to the application code and PLC firmware. The user can set this switch to enable or disable network downloads. This feature helps to prevent an unauthorized user with remote access from downloading contents to the PLC, adding an extra layer of security to the system.

Secure Development Lifecycle

The Rx3i PLC is engineered to GE's high standards of quality and reliability. It is designed to optimize the total cost of ownership by minimizing maintenance cost and delivering maximum reliability. This is accomplished through meticulous attention to detail in the software development process with the objective of delivering a PLC platform that is free of all known security vulnerabilities.

Secure-by-Design Communications with OPC UA

A "man in the middle" attack, executed between a controller and another device it communicates with, is a legitimate concern in any industrial automation application. The RX3i controller offers more secure communications across the network through use of the OPC UA protocol. OPC UA provides encryption and certificate management, making it difficult for an attacker to impersonate a legitimate device and insert itself into the communication path between devices.

Continuous Evolution

As cyber security threats continue to evolve, GE will continue to enhance the security features of the RX3i to help ensure it remains the most advanced controller for Industrial Internet applications.

GE
Industrial Solutions
2500 Austin Dr
Charlottesville, VA, 22911
1-800-433-2682 or 1-434-978-5100
www.geautomation.com

02.16 GFA2106