Rapid Link 5

Cyber Security Guideline

Profinet

Powering Business Worldwide

Break-Down Service

Please call your local representative:

Eaton.com/aftersales

Eaton.com/us/en-us/support.html

Hotline After Sales Service:

+49 (0) 1805 223822 (de, en)

AfterSalesEGBonn@eaton.com

Original Hardening Documentation is the English version of this document.

All non-English language versions of this document are translations of the original hardening documentation.

1. Edition 2020, publication date 12/2020

Content

1 EATON PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure Eaton products

Rapid Link 5 Profinet has been designed with cybersecurity as an important consideration. A number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable and competitive for customers.

The following whitepapers are available for more information on general cybersecurity best practices and guidelines:

- **Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):**
- **Cybersecurity Best Practices Checklist Reminder (WP910003EN):**
- **Cybersecurity Best Practices for Modern Vehicles - NHTSA**

Category	Description
Intended Use & Deployment Context	Rapid Link 5 is a modern and efficient drive and automation system. The innovative Rapid Link 5 concept focuses on customer and industry-specific requirements for material handling applications. It is suitable for both simple and complex tasks in all areas of conveyor technology. Because the Rapid Link 5 System can be fitted into a power and data bus, it allows electrical drives to be installed and taken into operation much more quickly and cost-efficiently than with conventional methods. Thanks to a power bus and a data bus that are plugged into every Rapid Link 5 module, the system is quick and easy to install. In the Rapid Link 5 variant, the Rapid Link modules are tailor-made solutions as • electronic DOL and reversing starter RAMO, • RASP5 frequency controlled speed control.
Asset Management	Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, [Subject] supports the following identifying information: Manufacturer including location, type ID, serial number, Firmware version number (at time of production) publisher, name, version, and version date. For details see Download Center – Documentation Rapid Link 5 AS-Interface manual, MN034004EN.
Risk Assessment	Eaton recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the system | device and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically.

Physical Security	An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. Rapid Link 5 Profinet is designed to be deployed and operated in a physically secure location. Following are some best practices that Eaton recommends to physically secure your system/device: • Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate. • Restrict physical access to cabinets and/or enclosures containing Rapid Link 5 Profinet and the associated system. Monitor and log the access at all times. • Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. It's a best practice to use metal conduits for the network cabling running between equipment cabinets. • Rapid Link 5 Profinet supports the following physical access ports. - RJ45 - M12 for sensors, actuators and field bus - Forward-/Reverse Switch for manual operation - Power supply plug - Motor plug • Access to these ports should be restricted. • For operations (e.g., firmware upgrades, parameterization changes) that require the connection of removable media (e.g., Keypad, Communication Stick or Eaton Parametrization Software DrivesConnect or Drives Connect Mobile App), always make sure that the origin of said media is known and can be trusted. • Before connecting any portable device via RJ45 or Bluetooth, scan the device for malware and viruses.
Network Security	Rapid Link 5 Profinet supports network communication with other devices in the environment. This capability can present risks if it's not configured securely. Following are Eaton recommended best practices to help secure the network. Additional information about various network protection strategies is available in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host paths (for example, using router ACLs and firewall rules). This helps to protect sensitive information and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82[R3]) for better security control.
Logging and Event Management	• Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities. • Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.). • Ensure that logs are retained for a reasonable and appropriate length of time. • Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system | device and any data it processes.
Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.

Secure Maintenance	**Best Practices** Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and software patches regularly. Eaton publishes patches and updates for its products to protect them against vulnerabilities that are discovered. Eaton encourages customers to maintain a consistent process to promptly monitor for and install new firmware updates. Firmware updates can be installed via drivesConnect. Please see Application Notes Overview document. Link to document in References. Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates
Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** Eaton recommends incorporating Rapid Link 5 Profinet into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system | device data should be backed up and securely stored, including: • Updated firmware for Rapid Link 5 Profinet. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated. • The current configuration. • Documentation of the current permissions / access controls, if not backed up as part of the configuration.
Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by Rapid Link 5 Profinet be adequately protected through the deployment of organizational security practices.

Decommissioning or Zeroization

It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable.

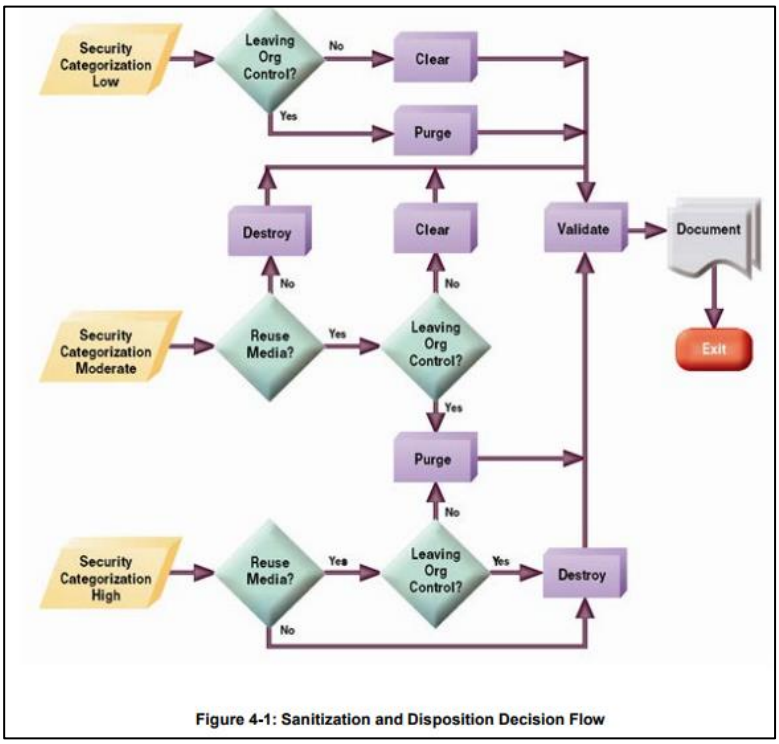

Figure 4-1: Sanitization and Disposition Decision Flow

** Figure and data from NIST SP800-88*

- **Embedded Flash Memory on Boards and Devices**
- Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory.
- **Clear**: If supported by the device, reset the state to original factory settings.
- **Purge**: If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed.
- **Destroy**: Shred, disintegrate, pulverize, or Incinerate by burning the device in a licensed incinerator.

2 References

Documentation		
	Document	**LINK**
Manual Rapid Link 5	MN034004	Link
Overview all Application Notes	Overview	Link
Hardening Documentation Rapid Link ASi	MZ034003EN	Link
NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015		Link
National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009		Link
NIST SP 800-88, Guidelines for Media Sanitization, September 2006		Link
A Summary of Cybersecurity Best Practices - Homeland Security		Link
White Papers		
Cybersecurity Best Practices Checklist Reminder	WP910003EN	Link
Cybersecurity Best Practices for Modern Vehicles - NHTSA		Link
Cybersecurity Considerations for Electrical Distribution Systems	WP152002EN	Link

Eaton is dedicated to ensuring that reliable, efficient and safe power supply is available when it is needed most. With vast of energy management across different industries, experts at Eaton deliver customized, integrated solutions to solve our customer' most critical challenges.

Our focus is on delivering the right solution for the Application. But decision makers demand more than just Innovative products. They turn to Eaton for an unwavering Commitment to personal support that makes customer Success a top priority. For more information, visit **Eaton.com**

Eaton addresses worldwide:
Eaton.com/us/en-us/locate/global-locations.html

Eaton Industries GmbH
Hein-Moeller-Str. 7- 11
D-53115 Bonn/Germany

Publication No. MZ040045EN

Powering Business Worldwide