

Product Cybersecurity Guideline
for Modular PLCs
XC-104-... XC-204-...

EATON PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure Eaton products

for Modular PLCs XC-104-... XC-204-... 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, competitive for customers.

Category	Description
<p>[1] Intended Use & Deployment Context</p>	<p>New modular, low-cost micro controller to enable customer to design flexible and space efficient automation solutions in combination with our modular XN300 IO slice portfolio. The cost-efficient device provides basic performance & connectivity and is programmable by EATON standard XSOFT-CODESYS. XC104 and XC204 modular controller is part of the EATON automation solution concept to fill the gap of a low-cost micro controller between easyE4 (Nano Controller) and XC300 (Small Controller) for the MOEM segment with Global Applications.</p>
<p>[2] Asset Management</p>	<p>Keeping track of software and hardware assets in your environment is a prerequisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, for Modular PLCs XC-104-... XC-204-... supports the following identifying information:</p> <p>NXP imx7 - MCIMX7S5EVM08S or NXP imx7 - MCIMX7D5EVM10S</p> <p>Software:</p> <ul style="list-style-type: none"> • Overview of each 3rd party open-source SW component • Customers gather relevant information from the systems web configuration.
<p>[3] Defense in Depth</p>	<p>Defense in Depth basically means applying multiple counter-measures for mitigating risks, in a layered or step wise manner. A layered approach to security as shown in the below diagram is what is recommended. Defense in Depth is the responsibility of both the manufacturer and the customer.</p> <div data-bbox="555 1283 1396 1825" style="text-align: center;"> </div>

Category	Description
[4] Risk Assessment	<p>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.</p>
[5] Physical Security	<p>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. for Modular PLCs XC-104-... XC-204-... 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:</p> <ul style="list-style-type: none"> • 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 for Modular PLCs XC-104-... XC-204-... 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. <p>for Modular PLCs XC-104-... XC-204-... supports the following physical access ports. RJ-45, USB, SDIAS. Access to these ports should be restricted.</p> <p>USB port is disabled by default. It can be enabled via system configuration.</p> <ul style="list-style-type: none"> • Do not connect removable media (e.g., USB devices, etc.) for any operation (e.g., firmware upgrade, configuration change, or boot application change) unless the origin of the media is known and trusted. • Before connecting any portable device through a USB port, scan the device for malware and viruses.
[7] Account Management	<p>Logical access to the system device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization's written policies:</p> <ul style="list-style-type: none"> • Ensure default credentials are changed upon first login for Modular PLCs XC-104-... XC-204-... should not be deployed in production environments with default credentials, as default credentials are publicly known. • No account sharing – If possible, each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user

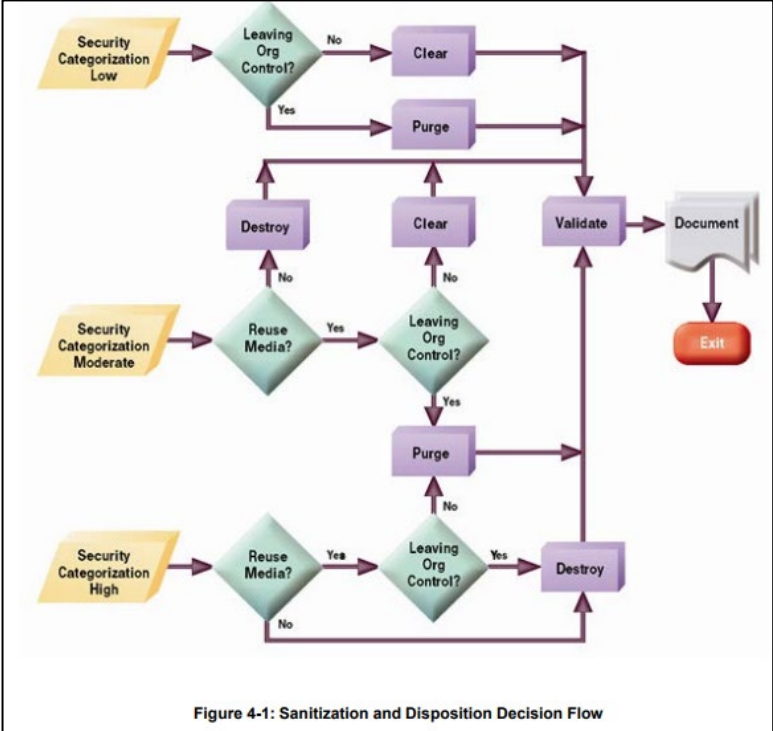
Category	Description
	<p>having a unique account. Allowing users to share credentials weakens security.</p> <ul style="list-style-type: none"> • Restrict administrative privileges - Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be assigned only to accounts specifically designated for administrative duties and not for regular use. • Leverage the roles / access privileges to provide tiered access to the users as per the business /operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role). • Perform periodic account maintenance (remove unused accounts). • Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters, and expire every 90 days, or otherwise in accordance with your organization's policies). • Enforce session time-out after a period of inactivity. <p>System web configuration is protected with a password following the PX Blue password guidelines. Password must be set on first start.</p>
<p>[8] Time Synchronization</p>	<p>Many operations in power grids and IT networks heavily depend on precise timing information.</p> <p>Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588).</p> <p>NTP supported.</p>
<p>[9] Network Security</p>	<p>for Modular PLCs XC-104-... XC-204-... 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 <i>Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]</i>.</p> <p>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.</p> <p>Communication Protection: for Modular PLCs XC-104-... XC-204-... provides the option to encrypt its network communications. Please ensure that encryption options are enabled. You can secure the product's communication capabilities by taking the following steps:</p> <p>HTTPS for system web configuration enabled by default.</p> <p>Eaton recommends opening only those ports that are required for operations and protect the network communication using network protection systems like firewalls and intrusion detection systems / intrusion prevention systems. Use the information below to configure your firewall rules to allow access needed for XC104/204 to operate smoothly</p>

Category	Description
	<p>Ssh – disabled per default</p> <p>Services can be enabled/disabled via system web configuration.</p>
<p>[10] Remote Access</p>	<p>Remote access to devices/systems creates another entry point into the network. Strict management and validation of termination of such access is vital for maintaining control over overall ICS security.</p> <p>SSH – disabled per default; timeout: 10 minutes</p>
<p>[11] Logging and Event Management</p>	<ul style="list-style-type: none"> • 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. <p>Logging automatically enabled, cannot be disabled. Export via system web configuration.</p>
<p>[12] Vulnerability Scanning</p>	<p>It is possible to install and use third-party software with for Modular PLCs XC-104-... XC-204-... . Any known critical or high severity vulnerabilities on third party component/libraries used to run software /applications should be remediated before putting the device system into production.</p> <ul style="list-style-type: none"> • Eaton recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. For COTS components (e.g., applications running on Windows), vulnerabilities can be tracked on the National Vulnerability Database (NVD), available at https://nvd.nist.gov/. • Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as possible. <p><i>Note: Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.</i></p>
<p>[15] Malware Defenses</p>	<p>Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.</p>
<p>[16] Secure Maintenance</p>	<p>Best Practices</p> <p>Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and software patches regularly.</p> <p>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.</p>

Category	Description
	<ul style="list-style-type: none"> - To update firmware, you have to install the newest CodeSys Version provided by Eaton and update firmware as described in device manual (Chapter 3 Setting up Device) - Eaton also has a robust vulnerability response process. In the event of any security vulnerability getting discovered in its products, Eaton patches the vulnerability and releases information bulletin through its cybersecurity web site - http://eaton.com/cybersecurity <p>Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates.</p>
<p>[17] Business Continuity / Cybersecurity Disaster Recovery</p>	<p>Plan for Business Continuity / Cybersecurity Disaster Recovery</p> <p>Eaton recommends incorporating for Modular PLCs XC-104-... XC-204-... 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:</p> <ul style="list-style-type: none"> • Updated firmware for for Modular PLCs XC-104-... XC-204-... . 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. <p>The following section describes the details of failures states and backup functions:</p> <ul style="list-style-type: none"> • For failure states, status indicators and backup functions see product manual
<p>[18] Customer Application Security</p>	<p>for Modular PLCs XC-104-... XC-204-... provides a platform on which customers can customize and host applications according to their requirements. Security vulnerabilities in these applications may expose the underlying device to attack.</p> <p>Eaton recommends observing best practices for secure system development when customers develop and host an application on the device:</p> <ul style="list-style-type: none"> • Privacy and Security by Design: The application should take security and privacy into consideration from the outset, including at the stage of defining requirements and assessing the associated risks. • Communication Protection: If the application communicates over the network, Eaton recommends encrypting the communications in accordance with the applicable level described by the FIPS 140-2 standard. • Access Enforcement: The application should provide the ability to enforce access controls to protect the application against unauthorized access and to protect accounts against unauthorized authentication attempts (for example, through account lockout). • Least Privilege: Any application developed by the customers should not run with root account privileges. The root account has full control over and access to the operating system. Therefore, if an application that requires root privileges has any security vulnerability, it endangers the entire system.

Category	Description
	<ul style="list-style-type: none"> • Input Checking: All input to the application should be sanitized before storing and processing by the application to protect against malicious code injection. • Output Handling: Data output by the application for user consumption, including error messages, should be appropriately handled to avoid revealing important information about the application and the underlying system. • Password Management: The application should securely store and transmit credentials (for example, encrypting authentication traffic, and salting and hashing passwords in transit and at rest). Password complexity should be implemented, and password should be masked when entered on-screen. • Secure Coding Practices: Follow secure coding practice while developing applications for the device (for example, implementing multiple security layers, verifying authorization for all requests, conducting code reviews, etc.). • Administration Interface: The interface for administering the application should be separated from the end-user interface. • Session Controls: All application sessions should be encrypted, logged and monitored. • Event Log Generation: The application should have the capability to log security related events at a minimum, including the time, date, and user.
<p>[19] Sensitive Information Disclosure</p>	<p>Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by for Modular PLCs XC-104-... XC-204-... be adequately protected through the deployment of organizational security practices.</p> <p>No sensitive information. Log data can only be exported when logged in to the system web configuration</p>
<p>[20] Decommissioning or Zeroization</p>	<p>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.</p>

Category	Description
----------	-------------



* 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. See manual for information how to proceed a factory reset
- **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.

References

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):

http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

[R4] National Institute of Technology (NIST) Interagency “Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41”, October 2009:

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:

http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R6] A Summary of Cybersecurity Best Practices - Homeland Security

<https://www.hsdl.org/?view&did=806518>

Eaton is an intelligent power management company dedicated to improving the quality of life and protecting the environment for people everywhere. We are guided by our commitment to do business right, to operate sustainably and to help our customers manage power – today and well into the future.

By capitalizing on the global growth trends of electrification and digitalization, we're accelerating the planet's transition to renewable energy, helping to solve the world's most urgent power management challenges, and doing what's best for our stakeholders and all of society.

Founded in 1911, Eaton has been listed on the NYSE for nearly a century. We reported revenues of \$19.6 billion in 2021 and serve customers in more than 170 countries.

For more information, visit [Eaton.com](https://www.eaton.com). Follow us on [Twitter](https://twitter.com/eaton) and [LinkedIn](https://www.linkedin.com/company/eaton).

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

© 2023 Eaton Corporation
All rights reserved.
01/2023 MZ050018EN (PMCC)