XC-303-C11-000
XC-303-C21-001
XC-303-C32-002

Powering Business Worldwide

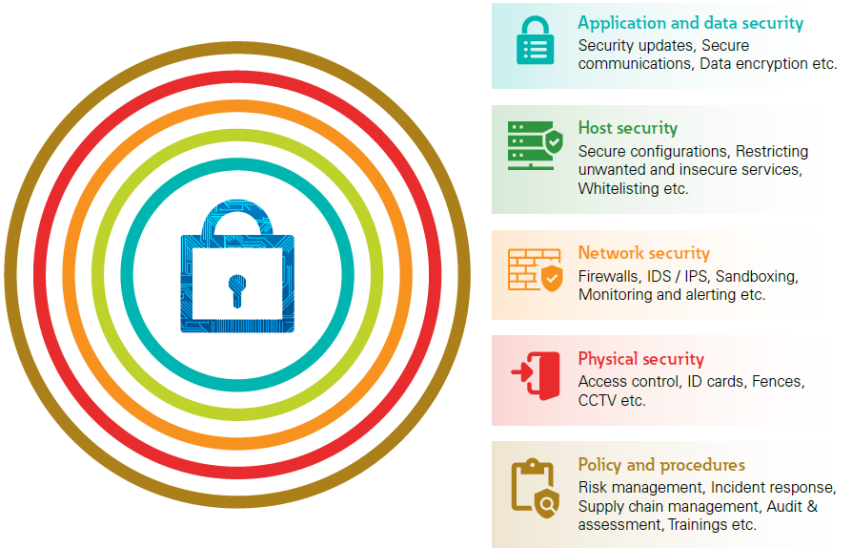
EATON PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure Eaton products

XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 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
[1] Intended Use & Deployment Context	The XC300 Modular control is Eaton's powerful and flexible control system, allowing machine and plant builders to achieve a slim and modern automation concept in combination with the compact I/O system XN300. Thanks to the large number of interfaces, the PLC is suitable for use as a universal and flexible data node for a wide range of applications. The integrated OPC server allows for standardized data transfer in machine-to-machine (M2M) communication, and the web server supports visualization in HTML5 format. This PLC can be programmed using the XSoft-Codesys programming tool. Unboxing this device it might run an outdated firmware. It is strongly recommended to update the device-firmware before starting to use this device.
[2] 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, XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 supports the following identifying information: <u>Serial-number of the device:</u> • Printed on the left side of the housing • Read via XSoft-CODESYS using the PLC-Shell command 'gethwinfo' or 'getserial' <u>MAC-Address:</u> • Printed on the left side of the housing • Read via XSoft-CODESYS using the PLC-Shell command 'gethwinfo' or 'getipconfig' <u>Firmware-Version:</u> • Read via XSoft-CODESYS using the PLC-Shell command 'getversion'
[3] Defense in Depth	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.

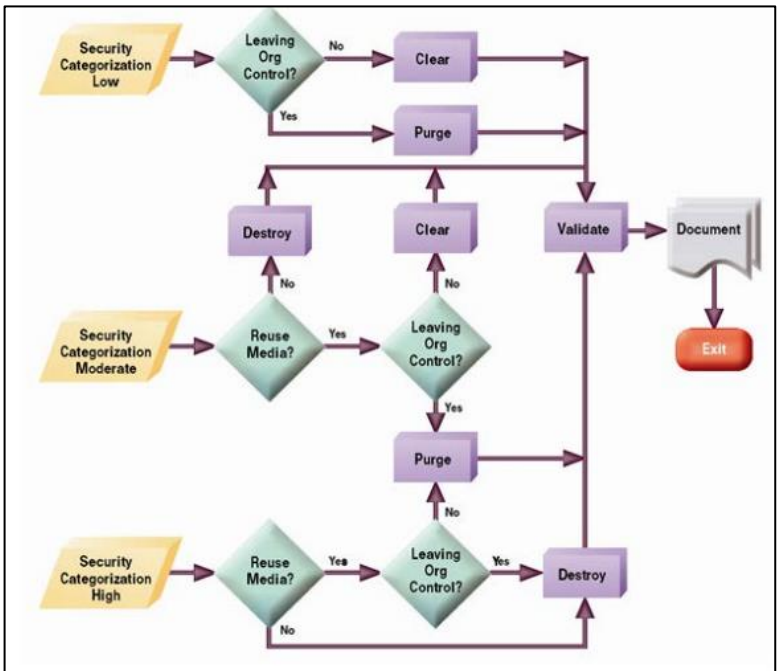
Category	Description
	
[4] Physical Security	An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 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 XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 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. • XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 supports the following physical access ports. - Ethernet Interface 'eth0' - Ethernet Interface 'eth1' - Ethernet Interface 'eth2' - USB-Host Inferface - SD-Card Interface - CAN-Bus Interface 'CAN1' - CAN-Bus Interface 'CAN2' - RS485 Interface Do not connect removable media (e.g., USB devices, SD cards, 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 or SD card slot, scan the device for malware and viruses.

Category	Description
[5] Account Management	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: • Ensure default credentials are changed upon first login XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 should not be deployed in production environments with default credentials, as default credentials are publicly known. • No account sharing – 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 having a unique account. Allowing users to share credentials weakens security. • 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. • 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. On XC-303 devices, running Firmware V3.5.20 or higher, the initial use of XSoft-CODESYS User Management is mandatory. The customer is asked to create a user account on first login. SSH, SFPT access is disabled by default and must be enabled by the customer setting customer owned credentials SD-Card access and USB-Host access are enabled, but autostart actions to these devices are disabled and must be enabled by the customer on demand. Documentation and Guidelines regarding CODESYS Security / User Management can be found here: CODESYS_HELP_SECURITY
[6] Time Synchronization	Many operations in power grids and IT networks heavily depend on precise timing information. Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588). A valid date is required to ensure correct handling of certificates. System Time of XC303 devices can be modified in various ways. • Read and modify System Time using XSoft-Codesys PlcShell functions "rtc-get" and "rtc-set" • Read and modify System Time using library functions "SysTimeRtcGet" and "SysTimeRtcSet" from within the user-application • Configure and activate the use of an NTP-Server to keep the system time synchronized using XSoft-Codesys PlcShell functions "ntpsetserver" / "ntpstart"

Category	Description
[7] Network Security	XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 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. Communication Protection: XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 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: How to establish encrypted communication can be found in CODESYS_HELP_SECURITY 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 XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 to operate smoothly Ports used by XC303: • Port 11740 is always enabled to ensure programming capability it is important to secure this port by way of restricting its access using a firewall, proper authentication and encryption on port 11740 (CodeSys Programming Port) as described in CODESYS-ONLINE-HELP. Also port 1217 hpss-ndapi is used by the codesys application for efficient application transfer to the device. • Port 4840 is used to run the OPC-UA protocol from XSoft-Codesys application. If no OPC-UA server should be hosted by your XSoft-Codesys application this port should be closed. This port can be disabled in the configuration file CODESYSControl.cfg. • Port 22 (SSH Connections) is disabled by default. To enable SSH/SFTP the XSoft-Codesys PlcShell command "setsshstate" may be used. An 'admin' user can be enabled by providing a customer specific password. • Ports 443/8080: (Webserver) This port can be disabled in the configuration file CODESYSControl.cfg • To get a list of open ports and services connect via SSH and run command "netstat -tulnp"
[8] Remote Access	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. Information how to establish an secure an online connection can be found here CODESYS Online Help - Communication
[9] Logging and Event Management	• Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities.

Category	Description
	• 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. The XSoft-Codesys Log can be read using the XSoft-Codesys Programming tool. This log-file can be filtered and uploaded.
[10] Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.
[11] 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. • To update firmware you have to install the newest XSoft-Codesys Version provided by Eaton and update the device firmware included in this installation. • 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 Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates. Eaton Products & Services - Download-Center - Eaton Europe • Category: Software • Software: XSOFT-CODESYS • Product-Version: <latest version>
[12] Business Continuity / Cybersecurity Disaster Recovery	Plan for Business Continuity / Cybersecurity Disaster Recovery Eaton recommends incorporating XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 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 XC-303-C32-002; XC-303-C21-001; XC-303-C11-000. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated. • User-application stored as a boot-application • The current configuration. • Documentation of the current permissions / access controls, if not backed up as part of the configuration

Category	Description
[13] Customer Application Security	XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 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. Eaton recommends observing best practices for secure system development when customers develop and host an application on the device: • 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: -XC303 provides option to host any type of application which may need over the network communication. If application is using over the network communication, then it should be hashed and encrypted as per FIPS 140-2. We highly recommend using https and TLS encryption, description about how to activate TLS can be found in CODESYS Online Help - Communication. • 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. • 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.
[14] Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by XC-303-C32-002; XC-303-C21-001; XC-303-C11-000 be adequately protected through the deployment of organizational security practices.
[15] 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.

Category	Description
	 **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. • XC303 running Firmware-Version >= 3.5.20 supports factory-reset functionality. . The factory-reset can be activated by XSoft-CODESYS using the PLC-Shell command 'factoryreset <serialnumber of the device>' • 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. • Check if SD-Cards are used on XC303 that need to be removed • Destroy: Shred, disintegrate, pulverize, or incinerate by burning the device in a licensed incinerator.

References

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):
https://www.eaton.com/content/dam/eaton/markets/machinebuilding/optimize-machine-and-system-performance/documents/eaton-white-paper-cyber-security-WP182004-en-us.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 3, Guide to Industrial Control Systems (ICS) Security, May 2015:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.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

Eaton is an intelligent power management company dedicated to protecting the environment and improving the quality of life for people everywhere. We make products for the data center, utility, industrial, commercial, machine building, residential, aerospace and mobility markets. 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 sources, helping to solve the world's most urgent power management challenges, and building a more sustainable society for people today and generations to come.

For more information, visit Eaton.com.

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

10/2025 MZ050007EN

Powering Business Worldwide