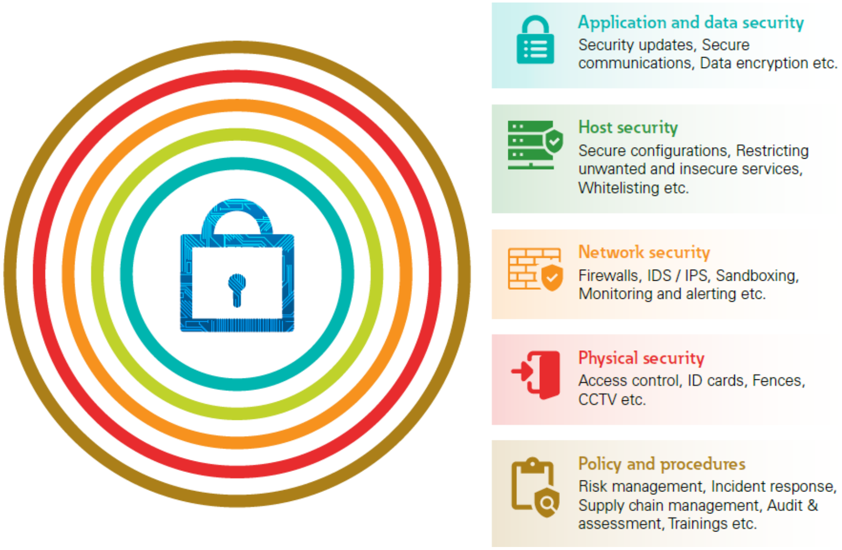
EATON PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure Eaton products

XC-CPU202-EC4M-8DI-6DO-XV 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 modular PLCs are characterized by having a wide spectrum of applications with freely scalable structure to suit. The user thus has the flexibility of designing his automation system precisely to his requirement. A further important attribute is the integration in modern communication concepts and the networking features. The modular PLCs of the XC200 series feature a high performance and excellent communication features. In addition to an RS232 interface and a CAN open fieldbus interface, this in particular is the integrated Ethernet interface. All XC-CPU...-XV feature and integrated WEB server. XC-CPU202-EC4M-8DI-6DO-XV (Y7-134238) equipped with operating system WIN CE 6.0 is controller unit for the modular XIOC system bloc. XIOC system bloc is central controlling unit build of controller, adjusted XIOC IO units and backplane base modules for mounting. The XIOC system bloc is basically to control small and medium automation solutions. The XC-CPU202-EC4M-8DI-6DO-XV is CODESYS programmable and provides ethernet access.
[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-CPU202-EC4M-8DI-6DO-XV** supports the following identifying information: Hardware: • NXP i.mx35 – MCIMX357CJQ5C Software: • To receive device name and serial number use scan in CODESYS and view device information. • To receive communication data like mac addresses and IP settings connect via PLC shell in CODESYS and execute “getipconfig” • To get build number, version and vendor execute “getversion” command in CODESYS PLC Shell

Category	Description
[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.  Application and data security Security updates, Secure communications, Data encryption etc. Host security Secure configurations, Restricting unwanted and insecure services, Whitelisting etc. Network security Firewalls, IDS / IPS, Sandboxing, Monitoring and alerting etc. Physical security Access control, ID cards, Fences, CCTV etc. Policy and procedures Risk management, Incident response, Supply chain management, Audit & assessment, Trainings etc.
[4] 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.
[5] 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-CPU202-EC4M-8DI-6DO-XV** 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-CPU202-EC4M-8DI-6DO-XV** 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.

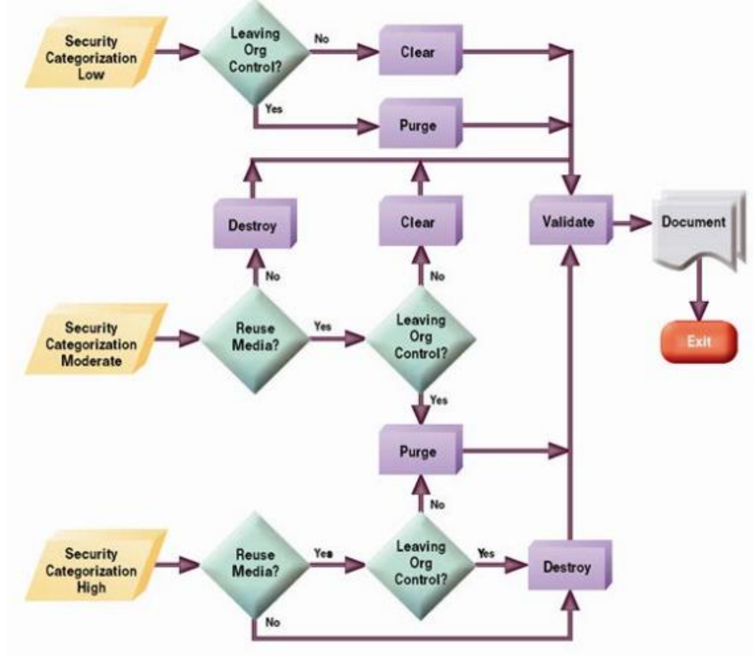
Category	Description
	XC-CPU202-EC4M-8DI-6DO-XV supports the following physical access ports: FTP (Port 21); CODESYS (Port 11740); Webserver http (Port 8080) FTP is disabled by default and can be enabled via INI file; External interfaces: USB; RJ-45; Mini SD • Do not connect removable media (e.g., USB 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.
[6] 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-CPU202-EC4M-8DI-6DO-XV** 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. Documentation and Guidelines regarding CODESYS User Management can be found in CODESYS Help Please review Chapter: "Protecting and Saving Projects": CODESYS Online Help

Category	Description
[7] 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). System Time 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 • Configuration and activation the use of an NTP-Server to keep the system time synchronized using XSoft-CODESYS PlcShell functions “ntpsetserver” / “ntpstart”
[8] Network Security	**XC-CPU202-EC4M-8DI-6DO-XV** 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. • How to establish encrypted communication can be found in CODESYS Help • Chapter “Encrypting Communication, Changing Security Settings” : CODESYS Online Help 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-CPU202-EC4M-8DI-6DO-XV** to operate smoothly • 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 Help. Also port 1217 hpss-ndapi is used by the CODESYS application for efficient application transfer to the device. • Services can be disabled via CODESYS (Webserver: ports 443/8080) and via the INIT_PLC file, as described in Manual Chapter 7

Category	Description
	• To disable Ethernet ports please read device manual Chapter 7 System parameter • For IP whitelisting for MODBUS/TCP use CODESYS MODBUS Configuration
[9] 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. • To log data use the standard CODESYS logging features as described in their help file. This includes logging of startup, shutdown and application downloads.
[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 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 Please check Eaton’s cybersecurity website for information bulletins about available firmware and software updates.

Category	Description
[12] Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** Eaton recommends incorporating **XC-CPU202-EC4M-8DI-6DO-XV** 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-CPU202-EC4M-8DI-6DO-XV**. 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. The following section describes the details of failures states and backup functions: • For failure states, status indicators and backup functions see product manual
[13] Customer Application Security	**XC-CPU202-EC4M-8DI-6DO-XV** 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: 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. • 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.

Category	Description
	• 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-CPU202-EC4M-8DI-6DO-XV** be adequately protected through the deployment of organizational security practices. No personal information is stored automatically by **XC-CPU202-EC4M-8DI-6DO-XV**
[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
	 Security Categorization Low Leaving Org Control? No Yes Clear Purge Destroy Clear Validate Document Exit No No Security Categorization Moderate Reuse Media? Yes Leaving Org Control? Yes Purge No Security Categorization High Reuse Media? Yes Leaving Org Control? Yes Destroy No **Figure 4-1: Sanitization and Disposition Decision Flow** ** Figure and data from NIST SP800-88* **<u>Embedded Flash Memory on Boards and Devices</u>** 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 • **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