Product Cybersecurity Guideline
XV-303-... / XV-313-...

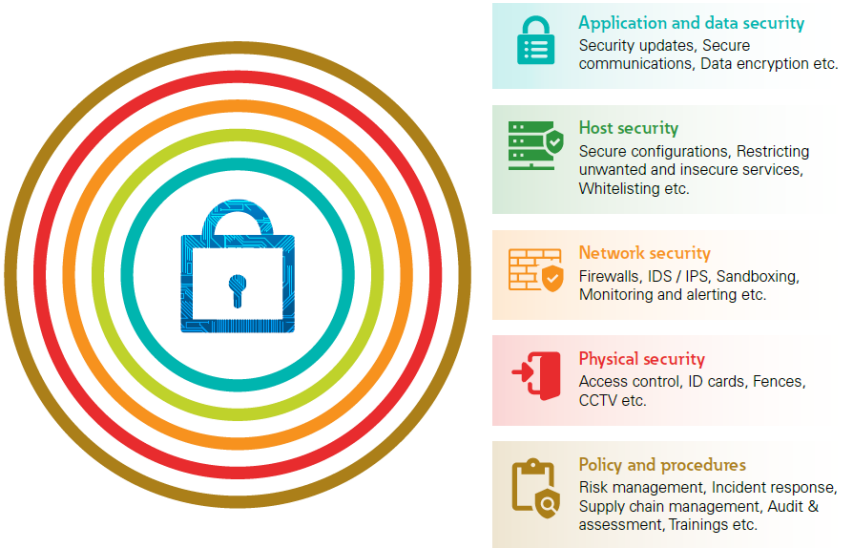
Powering Business Worldwide

EATON PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure Eaton products

XV-303/XV-313 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	Eaton delivers the XV-303 as programmable operator panel with no application. The device function will be defined by the customers application. Typical applications are mid-complex industrial machines, industrial aggregates. There are no functional safety functions or redundancies build in the device. Typically installed at factory floor electrical cabinet or mounted in machine housing. Physical access control mechanism to the rear of the device are needed.
[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, **XV-303/XV-313** supports the following identifying information: • Manufacturing location • Type ID (XV-303-…) • Serial number • Ethernet MAC Address Additionally, the following information about installed software can be gathered from the device' config tool: • Bootloader Version • OS Version For details see the **XV-303/XV-313** manual
[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] 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. **XV-303/XV-313** 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 **XV-303/XV-313** and the associated system. Especially the device's backside and the CTRL button should not be accessible to unauthorized personnel. 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.
	• **XV-303/XV-313** supports the following physical access ports.
	  ○ USB
	  ○ MicroSD card slot
	  ○ RJ-45 (Ethernet)
	  ○ RS485
	  ○ RS232
	  ○ CAN
	
	Access to these ports should be restricted.
	
	• For operations (e.g., firmware upgrades configuration changes or boot application changes) that require the connection of removable media (e.g., USB devices, SD cards, etc.), always make sure that the origin of said media is known and can be trusted.
	• Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.

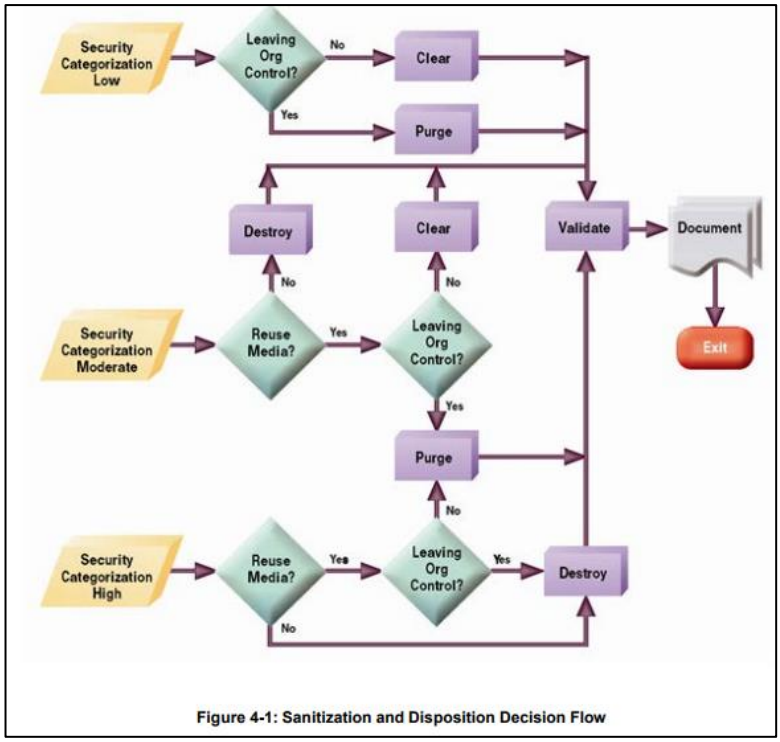
[7] Account Management	Logical access to the system | device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization's written policies: • Ensure default credentials are changed upon first login **XV-303/XV-313** 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.

Category	Description
	• Leveraging the roles / access privileges to grant users tiered access in line with business /operational needs, following the principle of least privilege (by allocating users only that level of authority and access to system resources that is required to perform their 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)
[8] Time Synchronization	**XV-303/XV-313** uses its system time for log files and usage in the applications. Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP).
[9] Network Security	**XV-303/XV-313** 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: **XV-303/XV-313** 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: • Eaton recommends opening only those ports that are required for operations and for the protection of the network communication by means of network protection systems, such as firewalls and intrusion detection systems / intrusion prevention systems. Use the information below to configure your firewall rules to allow the access needed for **XV-303/XV-313** to operate smoothly. • VNC remote access is disabled by default. If needed, it can be enabled in the device's config interface. Encryption should always be enabled. To ensure secure communication select a suitable VNC client and configure it to only use TLS 1.2. Misconfiguration of the VNC client might lead to attacker gaining data, which may include VNC credentials. Set a secure password. Port (default): 5900 • SSH server is disabled by default. Currently it is only used for service use cases. Therefore, it is strongly recommended to always keep SSH disabled. Port: 22
[10] 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. • VNC remote access is disabled by default. If needed, it can be enabled in the device's config interface. Encryption should always be enabled. To ensure secure communication select a suitable VNC client and configure it

Category	Description
	to only use TLS 1.2. Misconfiguration of the VNC client might lead to attacker gaining data, which may include VNC credentials. Set a secure password. Port (default): 5900 • SSH server is disabled by default. Currently it is only used for service use cases. Therefore, it is strongly recommended to always keep SSH disabled. Port: 22 • Web Application allows to configure device remotely. The communication is secured using https and authenticated with login credentials. Users need to create the password before first login. Port:8375
[11] 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. • Additionally, to application logs, Eaton HMI PLC offers firmware logs documenting administrative actions, user logons etc. It is recommended to regularly save, review and archive these logs. See the device manual for further instructions regarding firmware logs. • The **XV-303/XV-313** itself automatically logs events such as operating system log, login/logout, easyE4 connections, configuration changes and security related inconsistencies in the communication (hash faults). • Logs are automatically done and can be exported in the log section of the device information page using an external storage device (SD card or USB stick). This includes: Logon, logoff, linux boot sequence, external storage device attachment/detachment, security hash faults, system errors and firmware updates. • Only Admin user group has the rights to view or export logs
[12] Vulnerability Scanning	It is possible to install and use third-party software with **XV-303/XV-313**. 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. • Eaton recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. For COTS components, 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. 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.
[15] Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.

Category	Description
[16] 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. Download Center – Software Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates. Always use secure, hard-to-guess passwords and PINs for Config Tool, VNC and other remote connections. Set a unique PIN for the Config Tool immediately on first boot.
[17] Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** Eaton recommends incorporating **XV-303/XV-313** 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 **XV-303/XV-313**. 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: • To minimize downtime in case of device failure, make sure that you have documented the device configuration; that you have a copy of the application running on the device; and that you have the necessary supplemental application data at hand. If your application generates data, e.g. recipes, make sure that you back them up regularly.
[18] Customer Application Security	**XV-303/XV-313** 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).

Category	Description
	• 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.
[19] Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by **XV-303/XV-313** be adequately protected through the deployment of organizational security practices.
[20] 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: The device should be reset to the original factory settings via the update options. Refer to the device manual for instructions. • Purge: The flash memory can be easily identified by an expert and removed from the board, therefore it may be destroyed independently of the board that contained it. If unsure, the whole board should be destroyed • Destroy: The device should be shred, disintegrated, pulverized or incinerated by burning it 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 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

11/2024 MZ048009EN

Powering Business Worldwide