Product Cybersecurity Guideline

03/2024 MZ050008EN

XN-312-GW-EC EtherCAT Gateway

EATON

Powering Business Worldwide

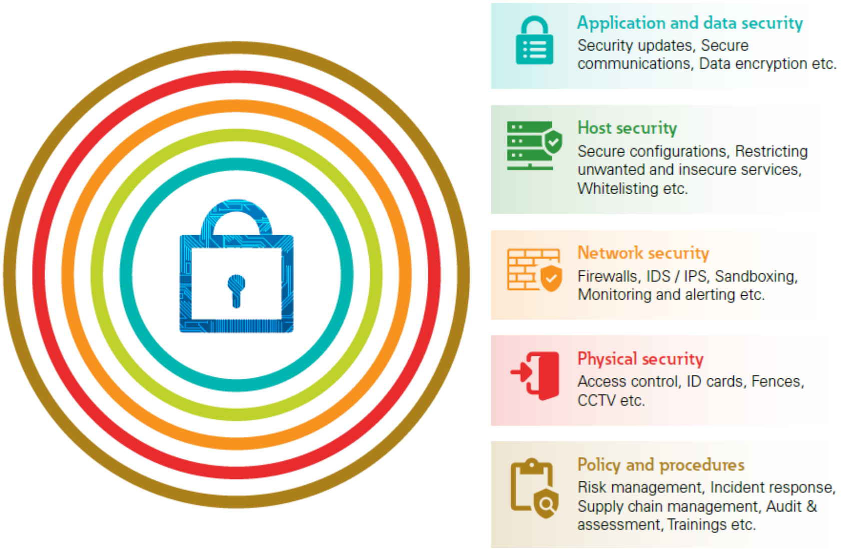
EATON PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure Eaton products

XN-312-GW-EC have 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 XN312-GW-EC gateways are part of the XN300 system. As an IO-Gateway it operates the attached XN322 IO modules. The XN322 IO modules are started and parameterized using parameter-data received from an EtherCAT master. Thereafter IO data and status information is exchanged with the EtherCAT master. It is possible to connect up to 32 XN322 IO modules to the XN312-GW-EC.
[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, **XN-312-GW-EC** supports the following identifying information: Hardware related information of the device can be found in the printing on the side case of the device. It includes: • HW-Version, • Serial number, • Part-number • Manufacturing date (Week / Year) The device name, serial number, hardware version, currently installed FW version and currently installed FPGA version, as well as module name, EtherCAT product code, EtherCAT vendor ID can be read through CAN Over Ethercat (CoE) as defined in the device documentation. For more details about CoE, kindly refer to the user manual. The XN300-Assist software tool supports the planning and commissioning of the XN300 modules. In addition to online features, such as the reading and setting of signal states and parameters, important auxiliary functions, including a validity check, can be performed offline. In online mode connected modules can be verified, the installed firmware version can be read, and a firmware-update can be started.

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. **XN-312-GW-EC** are designed to be deployed and operated in a physically secure location. Followings 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 **XN-312-GW-EC** and the associated system. Monitor and log the access at all times. • **XN-312-GW-EC** supports the following access to XN300-Assist using a Mini-USB Connector. Access to this port should be restricted.
[6] Account Management	The XN-312-GW-EC EtherCAT Gateway is always part of a higher-level controller (PLC and programming system). It does not support or enforce any type user accounts or privileges. Only Timeouts for accesses are governed by EtherCAT standards. Logical access to the higher-level controller should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their

Category	Description
	job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization’s written policies: • 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.
[7] Network Security	**XN-312-GW-EC** supports only Ethercat protocol. 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. 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 XN-312-GW-EC to operate smoothly.
[8] 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. The XN-312-GW-EC EtherCAT Gateway logs any updates and update attempts. It logs success and failure to verify update files as well as success and failure of the update itself. This log holds up to 50 entries. It can be read by reading file “log” through File over Ethernet (FoE). More details about FoE are available in user manual.
[9] Secure Maintenance	To effectively maintain this device you should make yourself familiar with this product.

Category	Description
	The latest informations, including manuals specifications and certifications, can be found on our webpage: XN300 I/O system | Eaton **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. Please use the configuration tool XN300-Assist to read out and update the Firmware of **XN-312-GW-EC**. Firmware-Update files for **XN-312-GW-EC** can be downloaded from the Eaton Download Center at: https://applications.eaton.eu/ XN-312-GW-EC Firmware can be found at • Category: “OS Updates” • Product Group: “XN300” • Product: “XN-312-GW-EC” The Configuration Tool XN300-Assist can be downloaded at • Category: “Wizard” • Assistant: “XN300 Assist” • Version: → Select and install the newest version available**.**
[10] Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** Eaton recommends incorporating **XN-312-GW-EC** 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 XN-312-GW-EC. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated.

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):
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/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