Technical Data **TD150026EN** Effective January 2019

Eaton CCOE cybersecurity recommendations

Product team guidelines

Power Xpert multi point meter 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 and competitive for customers.

The following Eaton whitepapers are available for more information on general cybersecurity best practices and guidelines:

Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN): http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

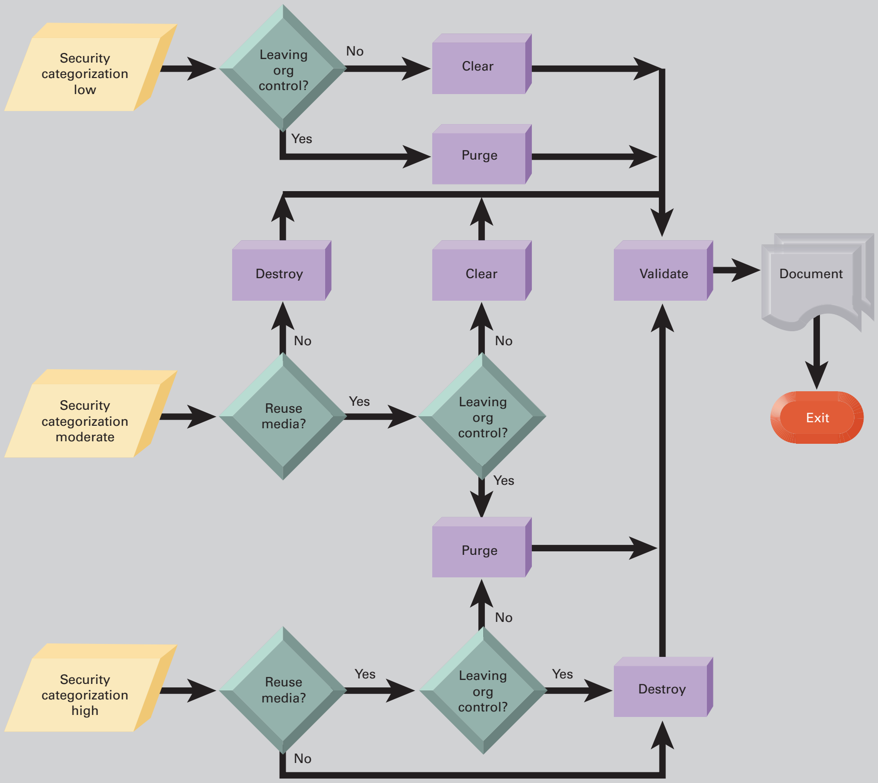
Cybersecurity Best Practices Checklist Reminder (WP910003EN): http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

Powering Business Worldwide

Category	Description
Asset management	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, Power Xpert multi point meter supports the following identifying information: • Part number • Assembly revision • Board revision • Serial number • Firmware version number • UI version number The details above are also available in the web interface under "About" The details about the communication settings are available under "Configuration"
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.
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. Power Xpert multi point meter 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 Power Xpert multi point meter 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 Power Xpert multi point meter supports the following physical access ports: • COM1 & Com2 RS-485 for Modbus_ Slave RTU or optional Display. • LAN Ethernet RJ45 CAT5 10/100Base-T. (optional on energy portal module) • USB config port Access to these ports should be restricted. • 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.
COTS platform security	Eaton recommends that customers harden third-party commercial-off-the-shelf (COTS) operating systems or platforms that are used to run Eaton applications / products (e.g., third-party hardware, operating systems, and hypervisors, such as those made available by Dell®, Microsoft®, VMware®, Cisco®, etc.). • Eaton recommends that customers refer to the COTS vendor's documentation for guidance on how to harden these components. • Vendor-neutral guidance is made available by the Center of Internet Security https://www.cisecurity.org/ Irrespective of the platform, customers should consider the following best practices: • Install all security updates made available by the COTS manufacturer. • Change default credentials upon first login. • Disable or lock unused built-in accounts. • Limit use of privileged generic accounts (e.g., disable interactive login). • Change default SNMP community strings. • Restrict SNMP access using access control lists. • Disable unneeded ports and services.
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. Power Xpert multi point meter 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. • 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).

Category	**Description**
Account management (cont'd)	• Enforce session time-out after a period of inactivity. • The system provides a notification in case a password does not meet the password requirements listed below for a strong password. • Lowercase letter • Uppercase letter • Number • Symbol • 8 or more characters • The product implements and supports password expiry and account lockout feature. The expiry and lockout dates are configurable and should be configured as per your requirement.
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). • Refer to section MN150003EN Clock Setup for details on how to configure the clock.
Network security	Power Xpert multi point meter 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* [1]. 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* [3]) for better security control. Communication protection: Power Xpert multi point meter 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: • Web server: HTTP uses TCP port 80, by default it will be redirected to HTTPs, HTTPs uses TCP port 443. • SFTP service is accessible via TCP port 2222 enabled by defaul.t • SSH Service Enable disabled by default. • Modbus TCP service is accessible via port 502. • SMTP client, disabled by default; if enabled, server TCP port configurable range 1-65535. • SNMP server (agent), disabled by default; if enabled, UDP port 161. • BACnet/IP server disabled by default; if enabled UDP port 47808. • NTP client, disabled by default; server UDP port 123. • The web communication protocol uses TCP port 7693/7694 for communication with the web client. 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 Power Xpert multi point meter to operate smoothly.
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.
Vulnerability scanning	It is possible to install and use third-party software with Power Xpert multi point meter. 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 (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. **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.
Malware defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.

Category	Description
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. • The latest Power Xpert multi point firmware can be acquired from the www.eaton.com/pxmp website. • Eaton customer support: For support on any aspect of the product or installation process contact the Customer Integrity Team by MRsupport@eaton.com or calling 1-844-435-8982. • Only Admin level user can upgrade Power Xpert multi point firmware. Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates.
Business continuity / cybersecurity disaster recovery	**Plan for business continuity / cybersecurity disaster recovery** Eaton recommends incorporating Power Xpert multi point meter 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 Power Xpert multi point meter. 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.
Customer application security	Power Xpert multi point meter 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. • 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.
Sensitive information disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by Power Xpert multi point meter be adequately protected through the deployment of organizational security practices.

Category	Description
Decommissioning or zeroisation	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.  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 1. Sanitization and disposition decision flow** **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. A Factory reset can be done using the settings page. • **Destroy:** Shred, disintegrate, pulverize, or Incinerate by burning the device in a licensed incinerator.

References

[1] *Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):* http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[2] *Cybersecurity Best Practices Checklist Reminder (WP910003EN):* http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

[3] *NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:* https://ics-cert.us-cert.gov/Standards-and-References

[4] *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

[5] *NIST SP 800-88, Guidelines for Media Sanitization, September 2006:* http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. TD150026EN / VCG
January 2019

Powering Business Worldwide