EATON ASSEMBLIES CYBERSECURITY

SECURE CONFIGURATION AND MAINTENANCE GUIDANCE

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. Cybersecurity risk management throughout the lifecycle of a product requires the consistent application of security management and monitoring practices. Eaton assumes the customer will integrate the recommendations provided into their overall cybersecurity risk management and lifecycle planning.

The cybersecurity configuration and maintenance guidance applies to assembled systems of automation and control components with internal facing and/or external connectivity over wired Ethernet, wireless, or serial communications or with physical ports for USB, serial, or removable media connections for diagnostics, configuration, and maintenance. The guidance is expected to be applied as applicable to the individual components of the assembled system and adjacent components and networks.

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

Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN)

Cybersecurity Best Practices Checklist Reminder (WP910003EN)

Category	Description
Asset identification and configuration	Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cybersecurity. Eaton recommends that an accurate inventory of authorized hardware and software running on the system is maintained. At a minimum, the following information should be included in the hardware inventory: manufacturer, type, serial number, f/w version number, product support contact/location, and function. At a minimum software inventories should include the following information: publisher, name, version, version date, patches/updates/hotfixes applied.
Asset Classification	Evaluate and Identify critical assets in whose loss or compromise, as determined by an engineering evaluation or other assessment method, results in the loss of primary functionality of the system. Classify assets on the basis of the criticality of asset. Also evaluate and identify Cyber Assets in secondary or supporting systems whose Loss, Degradation, or Compromise impacts both operation of Critical Cyber Asset(s) and their associated Critical Asset(s).
Restrict Physical access	Attacker with unauthorized physical access could cause serious disruption to a system. Eaton recommends restricting physical access to networked components where possible and provide physical access controls and monitoring where possible. Eaton assumes the product will be installed in locations not readily accessible (e.g. installed on a light-pole or on the side of a structure). Routine maintenance of the product should include inspection of components for physical intrusion, unauthorized modification, or unauthorized physical media (e.g. SD Card). The Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations. Refer to the individual product manuals for acceptable physical connection, removable media, and physical integrity guidelines.
General Security Hardening	Eaton recommends applying the following security hardening guidelines as they apply and as they do not impact system operations. In general Eaton recommends disabling unused ports and services, changing default credentials, securing network access, using boundary defenses (e.g. firewalls), securing interactive remote access, and maintaining backups to assist in recover in the case of an incident according to the device specific vendor documentation. Additional actions (as applicable) to consider include: • Disable HTTP and use HTTPS • Disable FTP – only use properly configured and secured SFTP when required • Disable Telnet – only use properly configured and secured SSH when required • Disable SNMP by default (use SNMPv3 where possible with strong community strings and read-only access) • Disable any additional ports and services not required for system operation • Apply MAC address or IP whitelisting if available

Category	Description
	• Disable and remove default and unnecessary accounts (including those created during commissioning) • Change default passwords and other authenticators • Apply role-based access control applying least privilege for user accounts • Disable DHCP and use static IP addresses where possible • Disable DNS and routing to external networks • Disable SMTP • Configure logging of administrative events and access attempts For third party Commercial Off the Shelf (COTS) components (e.g. network devices, workstations, servers, Human Machine Interface (HMI) devices) running COTS software (e.g. Microsoft Windows) follow best practice hardening guidelines (e.g. the Center for Internet Security (CIS) benchmarks).
Network Segmentation and Segregation	Physical and logical network segmentation and segregation are effective methods to limit the impact of a network intrusion. These methods can make it significantly more difficult for an attacker to access a system's critical assets. Each system and network should be segmented and segregated, where possible, from the data link layer up to and including the application layer. Use the principles of least privilege and need-to-know. If a system doesn't need to communicate with another system, it should not be allowed to. If a system needs to talk only to another system on a specific port or protocol and nothing else–or it needs to transfer a limited set of labeled or fixed format data, it should be restricted as such.
Configuration Management	Configuration management is used to control modifications to hardware, firmware, software, and documentation to ensure that the system is protected against improper modifications prior to, during, and after system implementation. There should be restricted access to configuration settings, and security settings of products should be set to the most restrictive mode consistent with operational requirements.
Media Protection	All transient cyber assets (including maintenance laptops, removable media, and other tools used for diagnostics, commissioning, or troubleshooting) should be validated and authorized through a sanitization and hygiene program that includes: • Cybersecurity awareness training • Scanning the device for malicious and unauthorized code This includes transient assets used during the validation and commissioning of the system.
System access controls	Eaton recommends using Role Based Access Control (RBAC) and applying the concept of least privilege (use only necessary accounts and with minimal privilege and access to resources to perform proper job function). Eaton also recommends the following:

Category	Description
	• Ensure default credentials are changed upon first login. Eaton recommends verifying all default credentials are changed during commissioning This includes default usernames, passwords, and certificates. • No account or password sharing • Restrict administrative privileges - Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Limit privileges to only those needed for a user's duties • Perform periodic account maintenance (remove unused accounts). • Change passwords and other system access credentials no longer than every 90 days, or per the organizational policy • Enforce complex passwords and session time-outs • Secure centralized authentication (e.g. via RADIUS or LDAP) according to industry best practices and manufacturer guidelines Refer to the individual component manuals for information on how to configure the system access controls and additional guidelines.
Secure Architecture and Network Access	Eaton assumes these systems will not be connected directly to the internet or les trusted networks. Physical, logical, and network access are assumed to be limited to authorized users and assets (user responsibility to implement). Each system and network should be segmented and segregated, where possible, from the data link layer up to and including the application layer. Use the principles of least privilege and need-to-know. If a system doesn't need to communicate with another system, it should not be allowed to. If a system needs to talk only to another system on a specific port or protocol and nothing else–or it needs to transfer a limited set of labeled or fixed format data, it should be restricted as such. To help secure network access Eaton recommends applying the following natively on the individual network facing components (as supported) or on external networking devices: • Using IP whitelisting • Applying default deny access (firewall) rules • Apply Network Access Control (NAC) mechanism (e.g. MAC filtering) • Limiting exposure to the internet • Limiting access to the local network • Using more secure protocols over less secure alternatives (e.g. HTTPS not HTTP) • Disabling SSH and other remote shell services Additional network deployment and hardening best practices can be found in Eaton Cybersecurity Considerations for Electrical Distribution Systems.
Remote Access	Interactive remote access (i.e. for system administration) should follow the following guidelines: • Limit access to authorized users

Category	Description
	• Use secure connections using FIPS140-2 cryptography • Configure session timeout and lockout policies • Enable logging (at a minimum login and logout) • Whitelist authorized endpoints where possible (via a firewall) • Use device authentication and Virtual Private Networks (VPN's) where possible
Logging and Event Management	Eaton recommends that that all event and session logs are logged, including all administrative and maintenance activities. Perform log review at minimum every 15 days. Centralized logging solutions can be used with the product if desired. Refer to the product user manuals for information on log configuration and management.
Vulnerability Management	Eaton recommends monitoring individual vendor sites, the Department of Homeland Security (DHS) Industrial Control System (ICS) Computer Emergency Readiness Team (CERT), and NIST National Vulnerability Database (NVD) for known vulnerabilities in products and mitigating or remediating the vulnerabilities as recommended though patches, updates, or compensating controls. ***The customer is responsible for downloading and verifying the integrity (e.g. cryptographic hash) and validating the compatibility and operation of all firmware and software applied to the system. The customer is also responsible for contacting the individual device vendors to vulnerability and other cybersecurity related information.*** Eaton publishes cybersecurity notifications and known vulnerabilities for its products on www.eaton.com/cybersecurity. Users are also able to report cybersecurity issues and receive automated cybersecurity notifications on this site. Eaton also has a vulnerability disclosure policy that is documented at this link: https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/vulnerabilitydisclosure.html The asset inventory should identify a vulnerability reporting source (typically the product vendor). Users are encouraged to keep a track of the security patches released by the COTS vendors and apply them to their environment as appropriate. 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.
Cybersecurity Awareness and Transient Asset Hygiene	Eaton assumes system access will be restricted to authorized personnel and devices. Eaton assumes all personnel have attended cybersecurity awareness training (per the individual organizational standards) and all transient assets (e.g. maintenance laptops, USB drives, DVD's) are authorized and have been scanned for malicious code.