Product Cybersecurity Guideline

09/2024 MZ049001EN

easyE product family

Powering Business Worldwide

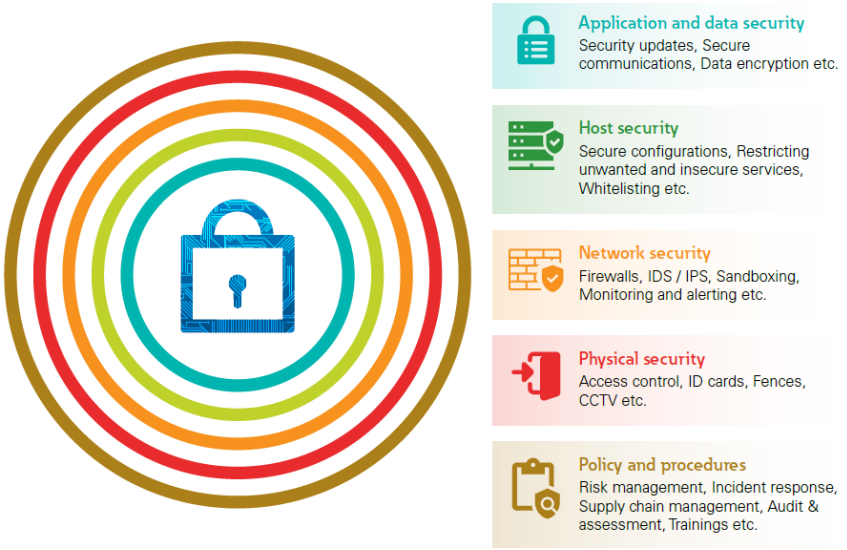
EATON PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure Eaton products

easyE4 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 easyE4 shall be used as a control relay in various industrial and building applications. The easyE4 base unit can be expanded by I/O modules through the easyConnect bus, by a SWD network through the SWD coordinator EASY-COM-SWD-C1 and through the communication module EASY-COM-RTU-M1 by a network of Modbus RTU devices. The easyE4 base unit and I/O devices as well as communication devices EASY-COM-SWD-C1 and EASY-COM-RTU-M1 are typically mounted in control cabinets, control panels, service distribution boards, or control consoles. Before deployment the easyE4 base unit needs to be configured through the easySoft software tool or through a pre-defined easySoft project stored on a SD card. The SWD coordinator EASY-COM-SWD-C1 and Modbus RTU EASY-COM-RTU-M1 can only be configured through the easyE4 base unit. After deployment the easyE4 either has no permanent connection to an Ethernet network or shall be used in protected ethernet network zone only. The SWD coordinator EASY-COM-SWD-C1 and Modbus RTU EASY-COM-RTU-M1 cannot be connected to an Ethernet network but only to the easyE4 base unit through the EASY-E4-CONNECT-COM1 connector and to the SWD network through the standard SWD flat ribbon cable, and to the Modbus network through RS485 serial cable.
[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, easyE4 supports the following identifying information: The printings on the easyE4 enclosure include manufacturer including location, type ID and Ethernet MAC-ID. The QR code of devices manufactured before 04/2024 contains the serial number, firmware version number (at time of production) and a link to product documentation. The QR code of devices manufactured from 04/2024 can be used with the Eaton Asset Manager App for mobile phones for a more convenient asset management. This information can also be retrieved through device display itself, easySoft and web client (if activated). The printing on the EASY-COM-SWD-C1 and EASY-COM-RTU-M1 enclosure include manufacturer including location, type ID, firmware version number (at time of production) as part of the QR code. This information can also be retrieved through the easySoft. For details see device and easySoft manual at Download Center Documentation easyE4 manual, MN050009.

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. 
[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. easyE4 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 easyE4, EASY-COM-SWD-C1, EASY-COM-RTU-M1, attached expansions and the associated system. Monitor and log the access at all times. • Physical access to the communication 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. • Utilize additional physical access restriction mechanisms such as locks, card readers, and/or guards etc. as appropriate. • easyE4 supports the following physical access ports: Ethernet port, SD card slot. Access to these ports should be restricted. • Do not insert a SD card for any operation (e.g., firmware upgrade, configuration change, or user program change) unless the origin of the media is known and trusted.

Category	Description
	• Before inserting a SD card, ensure that no malicious easyE4 program or unauthorized easyE4 firmware is stored on the SD card.
[6] 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 for 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 & services.
[7] Account Management	Logical access to the 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: • No password sharing – If you activate the webserver users admin, user1 and/or user2 make sure each user group gets its own password instead of sharing the passwords across groups. Security monitoring/logging features in the product are designed based on each user group having a unique password. 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 for the webserver users user1 and user2 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). • Enforce session time-out after a period of inactivity. • Set an easyE4 device password before commissioning. If the easyE4 webserver is activated the easySoft configuration dialog enforce a web administrator password with proper password length and complexity. • In the easyE4 web client the admin user can create API keys with the privileges of either user1 or user2. These keys are useful for the end user to manage the access to the web API. Please ensure that each system, application, or user uses an own API key instead of sharing the key. • Access to the device via easySoft does not provide different user roles. The device password should be used to prevent unauthorized access to the device. Per default no device password is set. It is highly recommended to set a device password in your easySoft project and activate it for all security areas critical to the application. • The webserver offers three different users: admin, user1 and user2. The user management is defined in the easySoft in the project settings. Access privileges for user1/user2 can be defined differently. In this way access to an easyE4 controlling machinery can be organized as follows:

Category	Description
	• admin: access is limited to machine vendor and trained personnel of the end user company. • "user1": access can be limited to maintenance personnel. • "user2": access can be granted for machine operators. • The webserver allows concurrent login with the same user to allow different persons access through one user role. Make sure that the password is limited to authorized personnel only. • The device menu can only be used with one (physical or virtual) device display at a time. In this way concurrent logins cannot be used to read the device password. • When registering easyE4 with AWS IoT Core the following credentials are needed for authentication: • AWS access key ID • AWS secret access key • AWS session token • These AWS credentials need to be valid for the AWS registration process only and are not stored permanently in the easyE4.
[8] 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. The easyE4 offers different options to synchronize system time: SNTP, radio clock (DCF), easyNET and manually through easySoft (for instructions see manuals).
[9] Network Security	easyE4 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. Deploy adequate network protection devices like Firewalls, Intrusion Detection / Protection devices. Communication Protection: easyE4 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: • easyE4 provides the option to encrypt the n/w traffic for the webserver (HTTPS) and for sending e-mails (SMTPS). Deactivation of this encryption is on your own liability. Therefore, please ensure that encryption options are not disabled. • For the webserver use the encryption if your http client supports it and if you are using at least the easyE4 hardware V8 and at least firmware V2.00. Starting with easyE4 hardware V8 easyE4 supports TLS1.2 with a certificate signed by easyE4 itself. It is not part of a chain of trust connected to a CA (on open internet). The root certificate installed by easySoft will ensure that the browser is communicating with a product family easyE4 device, without identifying a dedicated easyE4 device. This authentication is established with levels of certificates inside the device. It is recommended to use https instead

Category	Description

	of http to protect the http n/w traffic against monitoring password etc., even if you are using an older easyE4 hardware than V8 and therefore facing a web browser warning because of a self-signed certificate.
	• For a faster user experience when using the web-client we recommend using Google Chrome or Microsoft Edge since these browsers support TLS session resumption through TLS tickets.
	• For e-mails (SMTPS) use as encryption options either STARTTLS or TLS/SSL if the e-mail server allows one of these options. If no encryption is used for sending e-mails the device will automatically switch to STARTTLS if the e-mail server supports this.
	• For both options TLS version 1.2 is used.
	• For SMTPS the following TLS cipher suites are supported:
	  • TLS_RSA_WITH_AES_128_CBC_SHA,
	  • TLS_RSA_WITH_AES_256_GCM_SHA384,
	  • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
	  • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
	  • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
	  • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
	  • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
	  • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
	  • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA.
	• Please find detailed information about various Network level protection strategies in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Use the below information for configuring the firewalls to allow needed access for easyE4 to operate smoothly.
	  • https (default port 443): The webserver can be activated and configured in easySoft. The default setting use https (TLS) and port 443. The port can be changed to suit the situation of the local network. Only activate the webserver if needed. The webserver can be started during device boot-up or the user can switch the webserver on/off during execution of the easySoft user program, For the latter option use the function block alarm. Utilizing these options, the webserver can be activated in case of maintenance incidents only.
	  • http (default port 80): The webserver can be configured to be used without encryption. In this case port 80 is the default port. The recommendation is to always use https instead of http.
	  • easySoft (default port 443, 80 or 10001): The communication with easySoft can be established using 3 different options.
	  ○ Option a) Use easyCOM v2 encrypted based on ws/TLS (standard port 443) (default option)
	  ○ Option b) Use easyCOM v2 unencrypted based on ws (standard port 80) (not recommended)
	  ○ Option c) Use easyCOM v1 unencrypted based on TCP (standard port 10001) (not recommended)
	
	The default option a) uses TLS based encryption. The port can be changed to suit the situation of the local network. Since the communication using option b) or c) is not encrypted, the device should in these cases only be used in a secure network environment.
	
	  • Modbus TCP Server (port 502): The Modbus TCP server/slave functionality can be activated in easySoft. The port number cannot be changed. Since every Modbus TCP client can connect to the server the device should only be used in a secure network environment.
	  • easyNET (port range 10100 to 10110): Port range used by the NET protocol dedicated for controller-to-controller between easy devices. easyNET should only be used in a secure network environment.
	  • Discover (UDP port 11111): Discovery service for device identification. The device delivers information about itself on request.
	  • easyE RTD (ports 11112, 11113 and 11119):

Category	Description
	○ port 11112: Used to communicate the easyE4's display content to an easyE RTD and key events in the other direction. The UDP communication is protected by a cryptographic hash. The communication should only be operated in a secure network environment. The usage of this port can be disabled in easySoft by setting the "Remote display configuration" in the Ethernet tab to "No access". It is disabled as default. ○ Port 11113: Used to communicate customized visualization content between easyE4 and easyE RTDs. The UDP communication is protected by a cryptographic hash. The communication should only be operated in a secure network environment. The usage of this port can be disabled in easySoft by unchecking the "Allow visualization" in the Ethernet tab. It is disabled as default. ○ Port 11119: TLS protected service to open a display session and/or visualization communication in easyE4 for easy Remote Touch Display. This can be disabled by disabling both functions (port 11112 and 11113) above. • AWS device registration (standard https port 443): The AWS device registration is required before establishing a connection to AWS IoT Core. • Project download from AWS S3 (https port 443): easyE4 can download a project file from AWS S3 as part of the project update via cloud process. • The connection to the AWS IoT server uses MQTT, where easyE4 acts as the MQTT client. The default ports for AWS IoT Core communication are: ○ ALPN activated: TLS port 443 with ALPN protocol name "x-amzn-mqtt-ca", ○ ALPN deactivated: standard MQTT port 8883. • AWS IoT Core uses mutual certificate authentication. Therefore, MQTT connection to AWS cannot be established when using a proxy server, which exchanges the certificate for the AWS communication. Note: Many compliance frameworks and cybersecurity best practices require an audit of ports and services before and after applying updates and system changes. An end user should be able to refer to the ports and services documentation to determine the expected minimal set of ports and services on a device.
[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. The easy devices should only be used inside a secure network environment. Remote access to the device should only be possible through secure technologies like virtual private networks. Each web session uses a timeout of 30 seconds to determine if a web client is still connected. If no life-signal from the web client is received within this period, the session is closed. The easySoft communication to the device does not use timeout settings since it might be requested to keep a connection open for a longer time to perform debugging of a user application. This should only be used inside a secure network environment. To ensure no malicious access don't leave your workstation unlocked while easySoft is connected to the device. For further recommendations please read Security best practices checklist.
[11] Logging and Event Management	• Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities.

<table>
<tr><th>Category</th><th>Description</th></tr>
<tr><td></td><td>

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.
easyE4 offers logging of system events on SD card. This functionality can be activated in the system settings of the easySoft project. The log files contain event codes and a time stamp. The following table lists all event codes of the easyE4:

<table>
<tr><td>Event code</td><td>Description</td></tr>
<tr><td>0</td><td>Program download from eS7</td></tr>
<tr><td>1</td><td>Program download from SD</td></tr>
<tr><td>2</td><td>Program deletion</td></tr>
<tr><td>3</td><td>Web API key created</td></tr>
<tr><td>4</td><td>Wrong web API key entered</td></tr>
<tr><td>5</td><td>New device password created</td></tr>
<tr><td>6</td><td>Device password deleted</td></tr>
<tr><td>7</td><td>Wrong device password entered</td></tr>
<tr><td>8</td><td>SWD config. button pressed</td></tr>
<tr><td>9</td><td>Firmware update of easyConnect device</td></tr>
<tr><td>10</td><td>Firmware update of ComBUS device</td></tr>
<tr><td>11</td><td>Firmware update base device</td></tr>
<tr><td>12</td><td>Web user: Invalid user or Password</td></tr>
<tr><td>13</td><td>FW update base device started</td></tr>
<tr><td>14</td><td>FW update base device signature invalid</td></tr>
<tr><td>15</td><td>FW update base device failed (e.g. update for wrong device)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Category</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>16</td><td>Project update via cloud started</td></tr>
<tr><td>17</td><td>Project update via cloud failed</td></tr>
<tr><td>18</td><td>Project update via cloud successful</td></tr>
<tr><td>120</td><td>Modbus TCP Client activated</td></tr>
<tr><td>121</td><td>Modbus TCP Client deactivated</td></tr>
<tr><td>122</td><td>Modbus TCP Client: configuration changed</td></tr>
<tr><td>123</td><td>Modbus TCP Client: invalid data received</td></tr>
</table>
</td></tr>
<tr><td>[12] Vulnerability Scanning</td><td>To utilize easyE4 and easySoft it is needed to install and use third-party software like Windows or web browsers. Any known critical or high severity vulnerabilities on third party component/libraries should be remediated before putting the 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.</td></tr>
<tr><td>[13] Malware Defenses</td><td>Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.</td></tr>
<tr><td>[14] Secure Maintenance</td><td>The device includes a web client to allow a service engineer to retrieve information from an easyE4 device which includes:

• active easyE4 diagnostic IDs,
• easyE4 diagnostic buffer entries,
• network settings,
• SMTP settings.

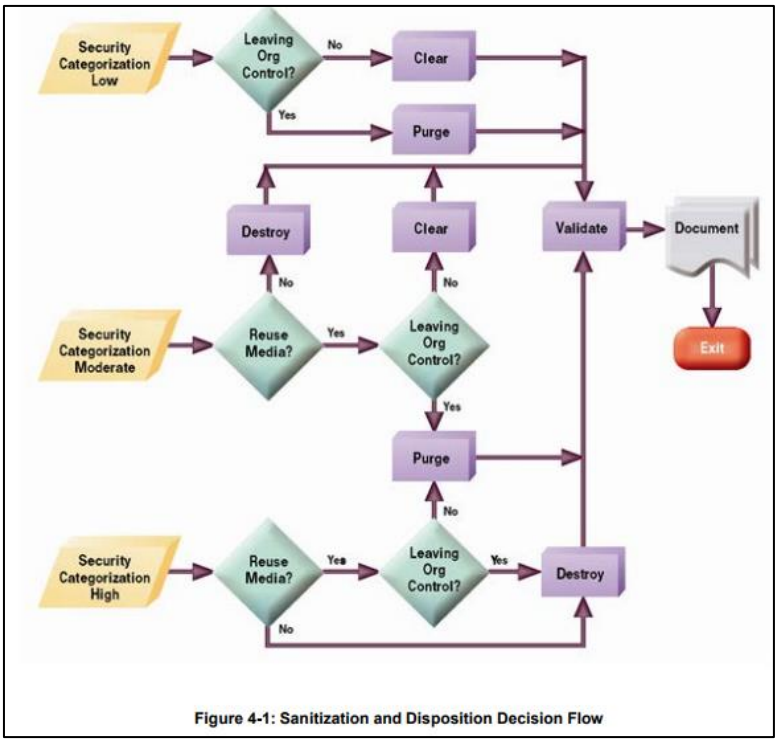
Best Practices

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.</td></tr>
</table>

Category	Description
	• A firmware update file can be downloaded from the Eaton website. This file has to be copied on a SD card and selected in the device menu. The device must be rebooted with the SD card plugged in (see device manual for instructions). Please check Software Download Center for information bulletins about available firmware and software updates.
[15] Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** Eaton recommends incorporating easyE4 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: • Backup of the latest firmware for easyE4. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated. • Backup of the most current easySoft project. • Documentation of the most current user list. The following section describes the details of failures states and backup functions: • If a firmware update of the easyE4 base unit fails, the LCD will show 60 seconds after power-on a red backlight color and the word "error". Solution: Restart the base device with a valid firmware update file on the SD card. If the firmware update fails again, please contact the support. • The ETH LED indicates Ethernet and easyNET status. On devices with LCD these statuses are shown on the start display. For details see device manual. • The power LED of the easyE4 indicates operation mode (STOP/RUN) and communication status to the IO extension modules (if configured). On devices with LCD this information is shown on the start display. • The power LED of the EASY-COM-SWD-C1 and EASY-COM-RTU-M1 indicates operation mode (STOP/RUN) and communication status to the easyE4 base unit. In case the firmware update of the EASY-COM-SWD-C1 or EASY-COM-RTU-M1fails the power LED will blink green with 5Hz. Solution: Try to update the device with a valid firmware again, check if the update file on the SD card is broken. If the firmware update fails again please contact the support. For further details see device manual.
[16] Customer Application Security	easyE4 provides a platform on which customers can customize and host applications according to their requirements. This especially applies to applications using the easyE4 JSON API. 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. ○ easyE4 provides option to protect the interface to easySoft by the device password. This option should be activated always.

Category	Description
	○ easyE4 provides option to encrypt communication to easySoft (easyProtocol V2). It is recommended to always activate this feature. ○ easyE4 provides option to encrypt webserver communication (https). It is recommended to always activate this feature. ○ easyE4 provides option to restrict the access to operands via the webserver. Only the necessary operands shall be exposed via the webserver. • Always secure the easySoft project with a password (as described in easySoft manual). • 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: easyE4 provides option to restrict the webserver access to the users admin, user1 and user2. It is recommended to not allow anonymous access. • 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. The application should generate sufficient error message to diagnose any issue in the application but shouldn't reveal useful information that can be exploited by malicious users. • 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. • When project update via cloud (AWS) is activated/allowed, an Update ID shall be set in easyE4. This Update ID must be set once in device by a special web API call and every time when a project (dedicated for update via cloud) is exported by easySoft. The project will be discarded in case of a mismatch of the update ID in device and in project file. The Update ID has to be kept secret.
[17] Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by easyE4 be adequately protected through the deployment of organizational security practices.

Category	Description
[18] 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.  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. The easyE4 supports a factory reset through a dedicated file on the SD card. The reset will also delete the AWS certificate and the Update ID (used for project updates via cloud). In addition, it is possible to delete the user program in the device menu and through easySoft (see device manual for instructions). • **Purge**: If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed. The SD card of easyE4 can be removed from the device and destroyed separately. The internal flash memory should be destroyed as part of the whole board. • **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):
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