Product Cybersecurity Guideline
easyE4

Powering Business Worldwide

Break-Down Service
Please call your local representative:
http://eaton.eu/aftersales
or
Hotline After Sales Service:
+49 (0) 1805 223822 (de, en)
AfterSalesEGBonn@eaton.com

Original Hardening documentation

The English-language edition of this document is the original Hardening documentation.

Translation of the original Hardening documentation

All editions of this document other than those in English language are translations of the original Hardening documentation.

1st Edition 2018, publication date 11/18
2n Edition 2019, publication date 05/19

Author: M.Suing
Editor: Bettina Ewoti

Contents

1 Introduction

easyE4 has been designed with Cybersecurity as an important consideration.

As such, the product offers a number of features for addressing cybersecurity risks. The Cybersecurity Recommendations below have been devised to help users deploy and maintain the product in a manner that minimizes cybersecurity risks. These recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

This section "Secure Hardening Guidelines" provide information to the users to securely deploy and maintain their product to adequately minimize the cybersecurity risks to their system.

Eaton is committed to minimizing the Cybersecurity risk in its products and deploys cybersecurity best practices with latest cybersecurity technologies in its products and solutions; making them more secure, reliable and competitive for the customers.

Several Eaton white papers provide additional information on general cybersecurity best practices and guidelines referenced at

www.eaton.com/cybersecurity

2 easyE4 – Secure Hardening Guidelines

2.1 Categories to consider

Category	Description
Asset identification and configuration	Keeping track of all the devices in the system is a pre-requisite for effective management of Cybersecurity of a system. Ensure you maintain an inventory of all the components in your system in a manner in which you uniquely identify each component. To facilitate this easyE4 supports the following identifying information printed on the enclosure: • Manufacturer including location • Type ID • Ethernet MAC-ID This information and the serial number is also available through: • the device display itself • the software easySoft • the web client (if activated) For details see device enclosure, easySoft online help and at Download Center – Documentation easyE4 manual , MN050009.
Restrict Physical access	Attacker with unauthorized physical access could cause serious disruption to device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections at protocol level leaving the devices / systems relying on these protocols, exposed to Cybersecurity risk. Physical security is an important layer of defense in such cases. easyE4 is designed with the consideration that it would be deployed and operated in a physically secure location. Following are some best practices that Eaton recommends to ensure adequate security. • Restrict physical access to cabinets and/or enclosures containing easyE4 and the associated system. Monitor and log the access at all times as applicable. • Physical access to the communication lines should be restricted to prevent any attempts of wiretapping, sabotage. It's a best practice to use metal conduits for the communication lines running between one cabinet to another cabinet as applicable. • 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 them need to be restricted. • Only insert SD cards with known/valid content for any operation (e.g. firmware upgrade, configuration change and boot application change). • Before inserting a SD card, ensure that no malicious easyE4 program or unauthorized easyE4 firmware is stored on the SD card. Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations.

2 easyE4 – Secure Hardening Guidelines

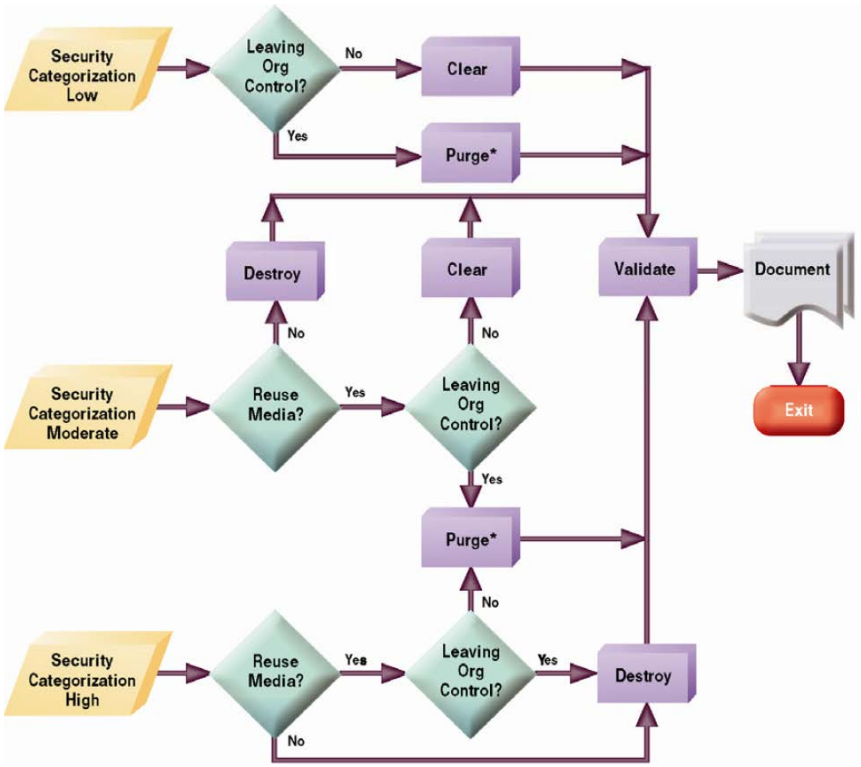
2.1 Categories to consider

Category	Description
System access controls	Securely configure the logical access mechanisms provided in easyE4 to safeguard the device from unauthorized access. Eaton recommends proper use of the access controls provided in the device to restrict system access only to legitimate users. And, such users are restricted to privilege levels necessary to complete their job roles/functions. • Set an easyE4 device password before commissioning the device for production. • If you activate the easyE4 webserver the configuration dialog will force you to set a web administrator password. • No password sharing – If you activate the webserver users admin, user1 and/or user2 make sure each user gets his/her own password vs. sharing the passwords. Security monitoring features in the product are designed with the view of each user having his/her own unique password. Security controls will be weakened as soon as the users start sharing their credentials. • Leverage the roles / access privileges for the webserver users user1 and user2 to provide tiered access to the users as per the operational need. Follow principle of least privilege (minimal authority level required) and least access (minimize unnecessary access to system resources). • In the easyE4 web client the admin user can create API keys with the privileges of either user 1 or user 2. 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. • Change passwords, API keys and other system access credentials no longer than every 90 days, or as per the organizational policy. • Enforce complex passwords. **easyE4 user roles** • Access to the device via easySoft does not have 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 a easyE4 controlling machinery can be organized as follows: – 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.

Category	Description
Secure Network Access	easyE4 provides network access to facilitate communication with other devices in the system. But this capability could open up a security loophole if it's not configured securely. Following are Eaton recommended best practices for securely configuring the network access. Eaton recommends segmentation of networks into logical enclaves and restrict the communication to host-to-host paths. This helps to protect sensitive information, critical services and limits damage from network perimeter breaches. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP800-82[R3]) for better security control. Deploy adequate network protection devices like firewalls, intrusion detection / protection devices. Communication Protection: easyE4 provides the option to encrypt the n/w traffic for the webserver (https) and for sending e-mails (SMTPS), Deactivation of this encryption is on your own liability. Therefor please ensure that encryption options are not disabled. For the webserver use the encryption if your http client supports it. easyE4 support TLS1.2 with a self-signed certificate. Common web browsers issue a security warning because of the self-signed certificate. Nevertheless, it is recommended to acknowledge these warnings and use https instead of http to protect the http n/w traffic against monitoring passwords etc. For e-mails (SMTP) use as encryption option 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. 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 settings 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 (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 (port 10001): Used to communicate with easySoft. This interface cannot be deactivated but can be protected by the device password. Since the communication is not encrypted, the device should 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. • NET (port range 10100 to 10110): Port range used by the NET protocol dedicated for controller-to-controller between easy devices. NET should only be used in a secure network environment. 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.
Remote Access	Remote access to devices/systems represents a provision of control to an external party. Strict management and validation of termination of such access is vital for maintaining control over the 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 15 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.

2 easyE4 – Secure Hardening Guidelines

2.1 Categories to consider

Category	Description
3rd Party / COTS Security	Any third-party component/libraries used to run software /application should not have any publicly known Critical/High vulnerabilities. • Users are recommended to keep update the Commercial-off-the-shelf [COTS] components (e.g. an application running on Windows). It is recommended to contact the vendors for security related patches. Vulnerabilities affecting the COTS components can be tracked on National Vulnerability Database (NVD) https://nvd.nist.gov/. • 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.
Decommissioning or Zeroisation	It is a best practice to purge the data before disposing any device containing data. Proper decommissioning is described in NIST SP800-88. Eaton recommends that products containing embedded flash memory be destroyed to ensure any secure data is unrecoverable.  Figure 4-1: Sanitization and Disposition Decision Flow; Source: NIST SP800-88 **Embedded Flash Memory on Boards and Devices** This includes motherboards and 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. 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 from the disposal 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.

Category	Description
Secure Maintenance	**Best Practices** Apply Firmware updates and patches regularly Due to increasing Cyber Attacks on Industrial Control Systems by malicious actors, Eaton implements a comprehensive patch and update process for its products in the event of new methods of compromising security of Eaton products get discovered. Users are encouraged to maintain a consistent process to promptly monitor for fresh firmware updates, implement patching and updates as and when required or released. A firmware update file can be downloaded from the Eaton Download Center – Software. This file has to be placed on a SD card and the device has to be rebooted with the SD card plugged in (see device manual for instructions). Eaton also has a robust vulnerability response process. In the event of any security vulnerability getting discovered in its products, Eaton patches the vulnerability and releases information bulletin through its cybersecurity web site http://www.eaton.com/us/en-us/company/news-insights/cybersecurity.html. Conduct regular Cybersecurity risk analyses of the organization /system. This exercise should be conducted in conformance with established technical and regulatory frameworks such as IEC 62443 and NERC-CIP.
Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** It's a Cybersecurity best practice for organizations to plan for Business continuity. Establish an OT Business Continuity plan, periodically review and, where possible, exercise the established continuity plans. Make sure offsite backups include • Backup of the latest f/w copy of easyE4. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated. • Backup of the most current easySoft project. • Documentation of the most current User List. Following section describes the details of failures states and backup functions • If a firmware update fails, the LCD will show 60 seconds after power-on a red backlight color and the word "error". Solution: Restart the device with a valid firmware update file on the SD card. If the firmware update fails again contact the support, please. • The ETH LED indicates Ethernet and NET status. On devices with LCD these statuses are shown on the start display. For details see device manual. • The power LED 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. For further details see device manual.
Time Synchronization	Many operations in power grids, IT networks, heavily depend on precise timing information. Ensure time synchronization provided in the device are properly configured. The device offers different options to synchronize system time: SNTP, radio clock (DCF), NET and manually through easySoft (for instructions see manuals).
COTS Security Hardening	Eaton recommends that customers Harden the platforms / products that are used to run Eaton applications / products. (eg. Dell computer, Windows Operating System, VmWare ESXi virtual host, Cisco switches, etc.) Customers are recommended to refer COTS vendor's documentation for guidance on Secure hardening of these components. • Vendor neutral guidance is made available by Center for Internet Security https://www.cisecurity.org • Only save easySoft projects on secure locations as they could be modified in a malicious way.
Malware defenses	Eaton recommends its customers to deploy adequate Malware defenses to the platforms / products that are used to run Eaton applications / products. Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations.

2 easyE4 – Secure Hardening Guidelines

2.1 Categories to consider

Category	Description
Customer Application Security	easyE4 provides a platform to the customers to customize their applications according to their requirement and host on the PLC. These applications may be developed and deployed without adequate security controls, thus opening the attack vector for the underlying device. Eaton recommends following best practices to develop and host the application on the device: • Communication Protection: easyE4 provides option to host any type of application which may need over the network communication. If application is using over the network communication, then it should be hashed and encrypted as per FIPS 140-2 standard. • Access enforcement: The application interface should have proper access enforcement to prevent unauthorized access to the application. Prevent unsuccessful access attempt and implement account lockout. • Always secure the easySoft project with a password (as described in easySoft manual). • Least Privilege: The application developed by the customers should not run with root account privileges. Root account has the full control over the operating system services. If any security vulnerability occurs in application, it can compromise the complete system. • Manual Input Checking: All input/output in the application should be sanitized before storing and processing by the application. • Sufficient and Minimal Error message content: 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: Customer application should store and transmit the password in encrypted format. Password complexity should be implemented and password should be masked while setting and entering. • Secure Coding Practices: Follow secure coding practice while developing applications for the device. • Remote interactive sessions: All the remote session to the device should be encrypted, logged and monitored in the device.
Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personnel information) which may be stored by easyE4 be adequately protected through the deployment of Organizational Security Practices.

3 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://ics-cert.us-cert.gov/Standards-and-References

[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

Eaton is dedicated to ensuring that reliable, efficient and safe power is available when it's needed most. With unparalleled knowledge of electrical power management across industries, experts at Eaton deliver customized, integrated solutions to solve our customers' most critical challenges.

Our focus is on delivering the right solution for the application. But decision makers demand more than just innovative products. They turn to Eaton for an unwavering commitment to personal support that makes customer success a top priority. For more information, visit www.eaton.eu or www.eaton.com.

Eaton addresses worldwide:
www.eaton.com/Worldwide Sites

E-Mail:infobonn@eaton.com
Internet: http://www.eaton.eu
http://www.eaton.com

Eaton Industries GmbH
Hein-Moeller-Str. 7–11
D-53115 Bonn

05/2019 MZ049001EN Doku/ICPD

Powering Business Worldwide