# Product Cybersecurity Guideline
# easyE4

Powering Business Worldwide

**Service**

For service and support, please contact your local sales organization.
Contact details: Eaton.com/contacts
Service page: Eaton.com/aftersales

**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
2nd Edition 2019, publication date 05/19
3rd Edition 2021, publication date 05/21
4th Edition 2022, publication date 12/22



Author: Center of Excellence

# Contents

# 1 Introduction

easyE4 has been designed with cybersecurity in mind. 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 document provides 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 any cybersecurity risk in its products and to making them more secure, reliable and competitive by deploying cybersecurity best practices.

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

The following 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):**
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

# 2 easyE4 – Security Instructions

| Category | Description |
|---|---|
| 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.<br><br>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.<br><br>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.<br><br>After deployment the easyE4 either has no permanent connection to an Ethernet network or shall be used in protected ethernet network zone only.<br>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. |
| 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:<br><br>The printing on the easyE4 enclosure include<br>• manufacturer including location<br>• type ID<br>• firmware version number (at time of production) as part of the QR code<br>• Ethernet MAC-ID<br><br>This information can also be retrieved through these means:<br>• on the device display itself<br>• in the easySoft<br>• in the web client (if activated)<br><br>The printing on the EASY-COM-SWD-C1 and EASY-COM-RTU-M1 enclosure include<br>• manufacturer including location<br>• type ID<br>• firmware version number (at time of production) as part of the QR code<br><br>This information can also be retrieved through the easySoft.<br>For details see device and easySoft manual and at Download Center-Documentation easyE4 manual,MN050009. |
| Risk Assessment | Eaton recommends conducting a risk assessment to identify and assess any foreseeable internal and external risks to the confidentiality, availability and integrity of the system \| device and its environment. Any such assessment should be conducted in accordance with the applicable technical and regulatory frameworks, such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically. |

| Category | Description |
|---|---|
| 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:<br>• Restricting physical access to any cabinets and/or enclosures containing easyE4, EASY-COM-SWD-C1, EASY-E4-RTU_M1 attached expansions and the associated system. Any such access should be monitored and logged at all times.<br>• Restricting physical access to the communication lines and network cabling to protect against any attempts to intercept or sabotage communications. To this end, we recommend using metal conduits for the network cabling between equipment cabinets.<br>• Utilize additional physical access restriction mechanisms such as locks, card readers, and/or guards etc. as appropriate.<br>• easyE4 supports the following physical access ports: *Ethernet port, SD card slot*<br>• Access to them need to be restricted.<br>• Only insert SD cards with known/valid content for any operation (e.g. firmware upgrade, Configuration change and boot application change).<br>• Before inserting a SD card, ensure that no malicious easyE4 program or unauthorized easyE4 firmware is stored on the SD card.<br>• Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations. |

| Category | Description |
|---|---|
| Account Management | 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.<br><br>Set an easyE4 device password before commissioning it for Production.<br>If you activate the easyE4 webserver the configuration dialog will force you to set a web administrator password.<br>No password sharing – If you activate the webserver users admin, user1 and/or user2 make sure each user group gets his/her own password vs. sharing the passwords across groups. 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.<br>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).<br>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.<br>Change passwords and other system access credentials no longer than every 90 days, or as per the organizational policy.<br>Enforce complex passwords.<br><br>easyE4 user roles<br><br>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.<br>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.<br>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:<br>admin: access is limited to machine vendor and trained personnel of the end user company<br>“user1”: access can be limited to maintenance personnel<br>“user2”: access can be granted for machine operators<br>The webserver allows concurrent login with the same user1 to allow different persons access through one user role. Make sure that the password is limited to authorized personnel only.<br>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. |
| Time Synchronization | Many operations in power grids and IT networks heavily depend on precise timing information.<br>Ensure time synchronization provided in the device are properly configured. The easyE4 offers different options to synchronize system time: SNTP, radio clock (DCF), easyNET and manually through easySoft (for instructions see manuals). |

| Category | Description |
|---|---|
| Network Security | easyE4 supports network communication with other devices in its environment. This capability may present certain risks if not configured securely. Eaton recommends the following best practices to help secure the network. Additional information about various network protection strategies is available in the Eaton white paper Cybersecurity Considerations for Electrical Distribution Systems [R1].<br><br>Eaton recommends segmenting networks into logical enclaves, denying any traffic between segments except that which is specifically allowed, and restricting any communication to host-to-host paths (for example, by 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.<br><br>Deploy adequate network protection devices like Firewalls, Intrusion Detection / Protection devices.<br><br>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. Therefore, please ensure that encryption options are not disabled.<br><br>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 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.<br><br>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.<br>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.<br>For both options TLS version 1.2 is used.<br>For SMTPS the following TLS cipher suites are supported:<br>- TLS_RSA_WITH_AES_128_CBC_SHA,<br>- TLS_RSA_WITH_AES_256_GCM_SHA384,<br>- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,<br>- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,<br>- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,<br>- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,<br>- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,<br>- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,<br>- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA.<br>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.<br>- 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.<br>- 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.<br>- easySoft (default port 443, 80 or 10001): The communication with easySoft can be established using 3 different options.<br>Option a) Use easyCOM v2 encrypted based on ws/TLS (standard port 443) |

| | |
|---|---|
| | (default option)<br>Option b) Use easyCOM v2 unencrypted based on ws (standard port 80) (not recommended)<br>Option c) Use easyCOM v1 unencrypted based on TCP (standard port 10001) (not recommended)<br>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. |
| Network Security | - 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.<br>- 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.<br><br>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 the system \| device creates another entry point into the network. Strict management and validation of termination of such access is therefore vital for maintaining control of overall ICS security.<br>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.<br>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.<br>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.<br>• For further recommendations please read Security best practices checklist |

<table>
<tr><th>Category</th><th>Description</th></tr>
<tr><td>Logging and Event Management</td><td>
<ul>
<li>Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities.</li>
<li>The logs should be protected from tampering and other risks to their integrity (for example, by restricting the permissions to access and modify them, by transmitting them to a security-information and event-management system, etc.).</li>
<li>The logs should always be retained for a reasonable and appropriate length of time.</li>
<li>The logs should be regularly reviewed. A reasonable review frequency should be selected, taking into account the sensitivity and criticality of the system | device and any data it processes.</li>
<li>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:</li>
</ul>
<table>
<tr><th>Event code.</th><th>Description</th></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>
<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>Vulnerability Scanning</td><td>Any third-party component/libraries used to run software /application should not have any publicly known Critical/High vulnerabilities.<br><br>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/.<br>Users are encouraged to keep a track of the security patches released by the COTS vendors and apply them to their environment as appropriate.<br><br>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>Malware Defenses</td><td>Eaton recommends deploying adequate malware defenses to protect the product as well as the platforms used to run it.<br>Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations.</td></tr>
</table>

| Category | Description |
|---|---|
| Secure Maintenance | The device includes a web client to allow a service engineer to retrieve information from an easyE4 device which includes:<br>- Active easyE4 diagnostic IDs<br>- Network settings<br>- SMTOP settings<br><br>Best Practices<br><br>The device firmware should be updated prior to putting the device into production. Thereafter, firmware updates and software patches should be applied regularly.<br>Eaton regularly publishes patches and updates for its products to protect them against any vulnerabilities that are discovered. Eaton encourages customers to consistently monitor the availability of new firmware updates and to install them promptly.<br><br>• A firmware update file can be downloaded from the Eaton website. 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).<br><br>Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates: Download Center – Software. |

| Category | Description |
|---|---|
| Business Continuity / Cybersecurity Disaster Recovery | **Plan for Business Continuity / Cybersecurity Disaster Recovery**<br><br>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<br>- 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.<br>- Backup of the most current easySoft project.<br>- Documentation of the most current User List.<br><br>Following section describes the details of failures states and backup functions<br>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".<br>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.<br>The ETH LED indicates Ethernet and easyNET status.<br>On devices with LCD these statuses are shown on the start display.<br>For details see device manual.<br>The power LED of the easyE4 indicates operation mode (STOP/RUN) and communication status to the IO extension modules (if configured).<br>On devices with LCD this information is shown on the start display.<br><br>The power LED of the EASY-COM-SWD-C1 and EASY-COM-RTU-M1indicates 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.<br>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.<br><br>For further details see device manual. |
| Customer Application Security | easyE4 provides a platform to the customers to customize their applications according to their requirement. These applications may be developed and deployed without adequate security controls, thus opening the attack vector for the underlying device.<br>Eaton recommends following best practices to develop and host the application on the device:<br>- Communication Protection:<br>o easyE4 provides option to protect the interface to easySoft by the device password. This option should be activated always.<br>o easyE4 provides option to encrypt webserver communication (https). It is recommended to always activate this feature.<br>o easyE4 provides option to restrict the access to operands via the webserver. Only the necessary operands shall be exposed via the webserver.<br>- Always secure the easySoft project with a password (as described in easySoft manual).<br>- 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.<br>- 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. |

| Category | Description |
|---|---|
| Sensitive Information Disclosure | A Eaton recommends that any sensitive information (i.e., information about connectivity, log data or personal information) that may be stored by easyE4 be adequately protected through the deployment of organizational security practices. |
| 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 that the data are unrecoverable. |

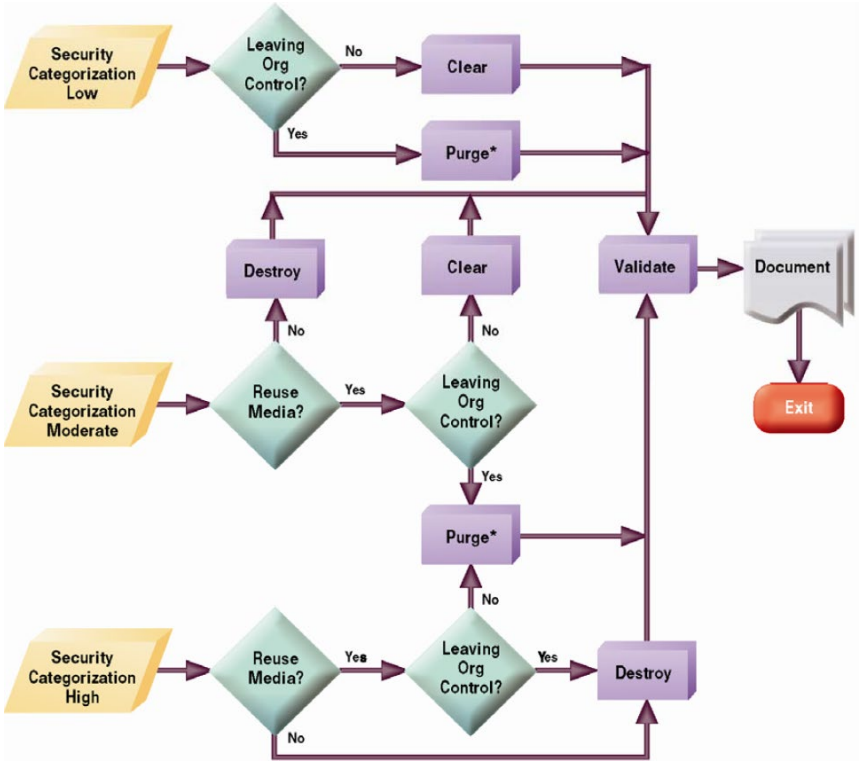


Figure 4-1: Sanitization and Disposition Decision Flow; Source: NIST SP800-88

**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**: Where possible, the device should be reset to the 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, it may be destroyed independently of the board that contained it. 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**: The device should be shred, disintegrated, pulverized or incinerated by burning it in a licensed incinerator.

# 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

[R6] Cybersecurity Best Practices for Modern Vehicles - NHTSA

https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[R7] A Summary of Cybersecurity Best Practices - Homeland Security

https://www.hsdl.org/?view&did=806518

Eaton is an intelligent power management company dedicated to improving the quality of life and protecting the environment for people everywhere. We are guided by our commitment to do business right, to operate sustainably and to help our customers manage power – today and well into the future.
By capitalizing on the global growth trends of electrification and digitalization, we're accelerating the planet's transition to renewable energy, helping to solve the world's most urgent power management challenges, and doing what's best for our stakeholders and all of society.

Founded in 1911, Eaton has been listed on the NYSE for nearly a century.
We reported revenues of $19.6 billion in 2021 and serve customers in more than 170 countries.

For more information, visit Eaton.com. Follow us on Twitter and LinkedIn.

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


12/2022 MZ049001EN (PMCC)

Powering Business Worldwide