Eaton Cybersecurity Center of Excellence
Cybersecurity Recommendations

Eaton Product Secure Configuration Guidelines

EATON

Powering Business Worldwide

Documentation to securely deploy and configure Eaton products

Green Motion DC 30/60 has been designed with cybersecurity as an important consideration. A number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable, and competitive for customers. Eaton assures that guidelines and recommendations mentioned in this document are secure.

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):

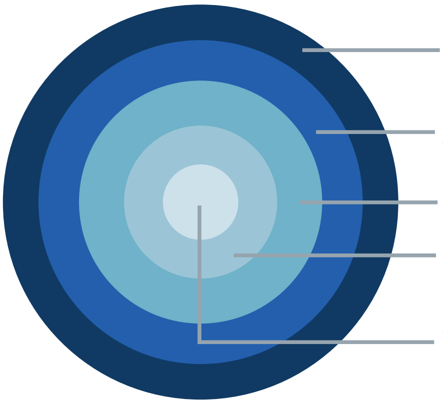
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

Cybersecurity Best Practices for Modern Vehicles - NHTSA

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

Category	Description
Intended use and deployment context	Intended Use and Deployment context provides clear understanding of product usage and expected outcomes to customer when used within the context. This also defines the boundaries for authorized usage. **Green Motion DC 30/60** consists of 3 sub-systems such as Power module, DC-SEC, and EV-CSC in addition to switch gear components. Power Module delivers the power as requested by DC-SEC which in turn requested by EV for EV battery charging. **Green Motion DC 30/60** provides following major features: • Compliance with the DC EV charger regulatory standards such as IEC61851-23:2024, ISO15118 etc. • Support of the standard OCPP protocol on the CS (communicate with cloud backend) • Translate the OCPP messages to/from the local Modbus communication with lower-level control unit (Supply Equipment Controller, EV-SEC) • Implement the internet gateway via multiple connection methods (ETH, WIFI, 4G) • Support the local control of the charging process: ◦ Load balancing (Static, Dynamic) ◦ Allow the standalone EV charging without a need to be connected to central system • EV charging using CCS gun • Charger events and alarm updates to OCPP server • Audible and visible charger status indication • Temperature control and monitoring • Safety checks • Metering EV-CSC communicates with the backend or cloud systems towards north side whereas it also communicates with DC-SEC for events, alarms and billing purposes.
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 key component. To facilitate this, **Green Motion DC 30/60** supports the following identifying information: In this guidance document, locations such as **Maintenance >>> Firmware** refer to individual menu items in the homepage of the webserver run on the device. Please be aware that the visibility of menu items depends on the user profile. For instance, a user belonging to the "Viewer" profile will not be able to access the Settings menu (it will not be even visible). Identifying information can be obtained using a web browser under: **Maintenance >>> Firmware:** • Status • Version • SHA • Generated On • Installed On • Activated On **Maintenance >>> System Information**: • UUID • Product • Vendor • Model number • Part number • Serial number • Hardware version • Firmware version • Firmware type • Bootloader version • MAC address Communication settings can be obtained from **Settings >>> Ports:** • Internet source • Wi-Fi settings • Cellular settings **Settings >>> TCP/IP:** • Hostname • IPV4 status, mode, address • IPV6 status, mode, address In addition to that, communication related settings can be found at the following locations: • **Settings >>> Firewall** • **Settings >>> CSMS** SNMP is not used.

<table>
<tr><th>Category</th><th>Description</th></tr>
<tr><td><b>Defense in depth</b></td><td>
Defense in Depth means applying multiple countermeasures 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.



Policy & Procedures
Risk Management, Incident Response, Supply Chain Management, Audit & Assessment, Trainings etc.,

Physical Security
Access Controls, ID Cards, Fences, CCTV etc.

Network Security
Firewalls, IDS/IPS, Sandboxing, Monitoring and Alerting etc.

Host Security
Secure Configurations, Restricting unwanted and insecure services, Whitelisting etc.

Application and Data Security
Security Updates, Secure Communications,
Data Encryption etc.
</td></tr>
<tr><td><b>Defense in depth</b></td><td>
<table>
<tr><th>Defense in depth layers</th><th>Threats addressed</th></tr>
<tr><td>Policies and Procedures</td><td>• Compliance violation with various Federal, State, and Industry regulations
• Improper usage
• Unintentional errors
• Phishing</td></tr>
<tr><td>Physical Security</td><td>• Theft
• Physical access of the hardware
• Disruption
• Accidental or intentional errors</td></tr>
<tr><td>Network Security</td><td>• Data leakage
• Data spoofing
• DoS, DDoS
• MiTM
• Unauthorized remote access
• DNS spoofing
• HTTPS spoofing
• IP spoofing
• ARP spoofing
• SSL hijacking
• Wi-Fi hacking</td></tr>
<tr><td>Host Security</td><td>• Sensitive data leakage
• Rootkits
• Malwares
• Unauthorized access
• Malicious upgrades
• Unauthorized changes</td></tr>
<tr><td>Application Security</td><td>• Privilege Escalation
• Session Hijacking
• CSS
• CSRF
• Buffer Overflows
• Remote file inclusion
• XML External Entity (XXE)
• Known Vulnerabilities</td></tr>
</table>
Eaton's Defense in depth strategy is discussed in the whitepaper - Cybersecurity considerations for electrical distribution systems[R1].
</td></tr>
</table>

Category	Description
Policies and procedures	Policies and procedures tie up the whole security management system. They address people and process part of the security. It also helps organizations to comply with various Federal, State, and Industry regulations Eaton recommends using security policies to manage security. Customer should customize policies to suit the specific environment. Policies and procedures increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties and telling them what they can do and what they cannot do with the organization sensitive information. It helps to educate employees about their importance of responsibility in protecting the organization sensitive data and proper usage. It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened. Following are some recommended cybersecurity policies but not limited to: **1. Virus and Malware Protection policy** to detect, remove, and repairs the side effects of viruses and malwares risks by using signatures. **2. Firewall policy** to block the unauthorized users from accessing the systems and networks that connect to the Internet and to remove the unwanted sources of network traffic. **3. Intrusion Detection/Prevention policy** to detect and block the network attacks and browser attacks. It also protects applications from vulnerabilities. **4. Patch management policy** to manage and implement patches in a timely fashion based on organizations security profile. **5. BCP/DR policy** to manage any unexpected security events. **6. Audit Log policy**
	Sensitive information disclosure: EV-CSC is designed to store limited data locally (Linux filesystem on the flash memory). Eaton recommends that sensitive information (i.e., connectivity, log data, personal information) that may be stored by **Green Motion DC 30/60** be adequately protected through the deployment of organizational security practices and policies. It is considered that RFID ID can be treated as potentially sensitive information. Even though it can't be traced to any physical person, extracted ID can be theoretically used for cloning the original RFID (feasibility of such attack depends on the RFID card technology and encryption) and cloned RFID card can be used for "free" EV Charging.
Physical Security	An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols do not 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. **Green Motion DC 30/60** 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 **Green Motion DC 30/60** and the associated system. Always Monitor and log the access. • Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. It is a best practice to use metal conduits for the network cabling running between equipment cabinets. • **Green Motion DC 30/60** supports the following physical access ports. Access to these ports should be restricted. Ethernet › Used to connect to OCPP server, Point of Sale (POS) USB › Enabled for the first 30 mins after powering ON the charger RS485 › Used for communication between DC-SEC and EV-CSC LCD is connected on DSI interface. • Do not connect removable media (e.g., USB devices, SD cards, etc.) for any operation (e.g., firmware upgrade, configuration change, or boot application change) unless the origin of the media is known and trusted. • Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.

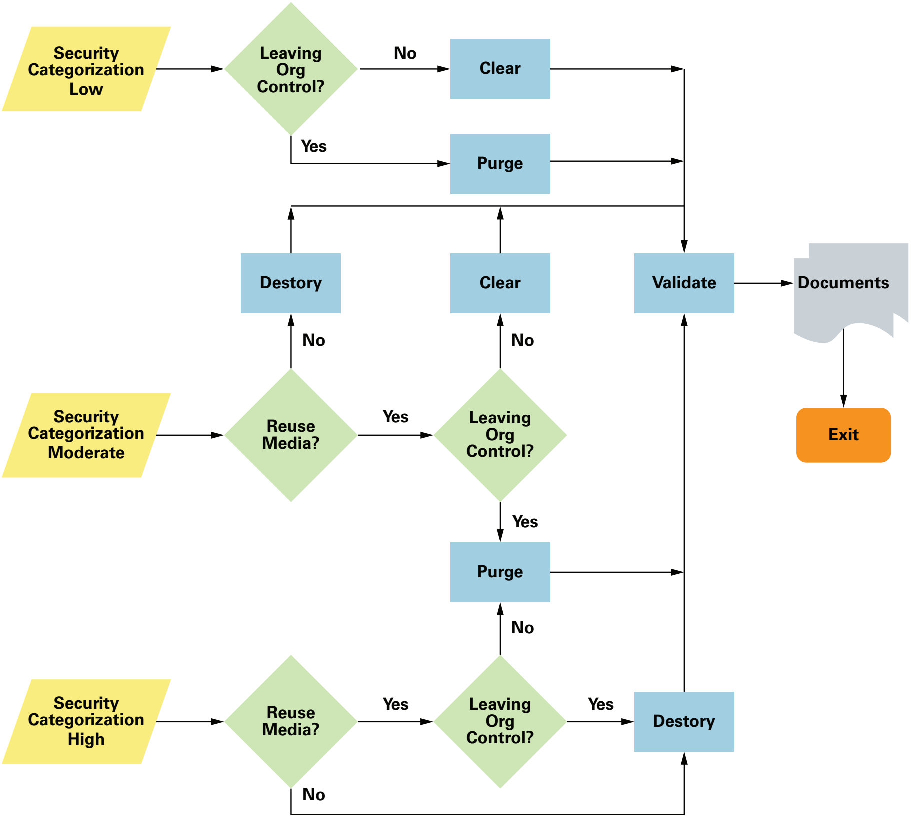
Category	Description
Network Security	Network security is the practice of preventing and protecting against unauthorized intrusion into corporate networks. It complements endpoint security, which focuses on individual devices; network security instead focuses on how those devices interact, and on the connective tissue between them. **Green Motion DC 30/60** supports network communication with other devices in the environment. This capability can present risks if it is 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. Communication Protection: **Green Motion DC 30/60** 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: **Green Motion DC 30/60** has been designed with maximum security in mind and therefore the key network security settings have been set in line with the current security requirements, and they are not configurable. Configuration of local and trusted remote certificates can be done under: **Settings >>> Certificate** Follow embedded help for instructions on how to configure it. Eaton recommends opening only those ports that are required for operations and protect the network communication using network protection systems like firewalls and intrusion detection systems / intrusion prevention systems. Use the information below to configure your firewall rules to allow access needed for **Green Motion DC 30/60** to operate smoothly. The following ports are open in the device in the default configuration: • 80/tcp: http • 443/tcp: https • 8883/tcp: secure-mqtt Some ports are configurable using the firewall. To access the firewall, navigate to: **Settings >>> Firewall** The firewall allows activate/deactivate individual services (such as http redirect, secure web, etc.) for various interfaces (Ethernet, Wi-Fi, ...). Apart from that, you can change the port number used by that service, and to create a whitelist address filter (follow embedded help for instructions on how to configure it). SNMP is not used. For external communication with energy meters, EV-CSC uses Modbus protocol. You can choose either Modbus RTU or Modbus TCP and set the respective settings as desired under: **Settings >>> Energy Meters** (Follow embedded help for instructions on how to configure it.) For SMTP, the respective settings, including the port number, can be found under: **Settings >>> General** (Follow embedded help for instructions on how to configure it.) When the 4G feature of **Green Motion DC 30/60** is being used, it is necessary to comply with the following requirements: • Mutual authentication between sim card and base station must be implemented using LTE AKA protocol. • At a minimum, AES 128-bit encryption algorithm should be used to secure communication channel end-to-end. • It is recommended that Telecom Service Providers provide a modem for 4G sim cards and cover the security of firmware. In addition to that, the following settings is highly recommended: • UICC pin should be enabled to prevent unauthorized access to network.

Category	Description
Host Security	Strong host security addresses the key aspects of your hosts, including hardware, software, server and storage components. It ensures you are equipped to defend yourself against, and appropriately respond to, cyber-attacks, when they occur. **Account Management** Logical access to the system | device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization's written policies: • Ensure default credentials are changed upon first login **Green Motion DC 30/60** should not be deployed in production environments with default credentials, as default credentials are publicly known. • No account sharing – Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security. • Restrict administrative privileges - Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be assigned only to accounts specifically designated for administrative duties and not for regular use. • Leverage the roles / access privileges – Administrator, Viewer, or Operator – to provide tiered access to the users as per the business /operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role). • Perform periodic account maintenance (remove unused accounts). • Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters, and expire every 90 days, or otherwise in accordance with your organization's policies). • Enforce session time-out after a period of inactivity. **User and profiles management** **User profiles** Three user profiles are defined in the device: Administrator • Has access to all user-configurable settings, i.e. all items in the device menu tree: Home, Settings, Location Settings, Wizard home, Maintenance Viewer • Can only view the information on the homepage of the charger, and Resources and System information under Maintenance Operator • Has access to charger operation related items in the device menu tree: Home, Location Settings, Wizard home, Maintenance. Under Maintenance, only Resources and System information are accessible. **User settings** The menu item where all the necessary functions are located is: **Settings >>> Users** • Add users of various profiles, i.e. Administrator, Viewer, Operator • Remove users • Edit users **Password/Account/Session management:** **Settings >>> Users** Password strength rules – Minimum length / Minimum upper case / Minimum lower case / Minimum digit / Special character Password expiration – Number of days before password expiration / Number of tries before locking the account / Lock account for XX minutes / indefinitely Session expiration – No activity timeout / Session lease time See "Default settings parameters" in the embedded help for (recommended) default values. Additionally, it is possible to enable account expiration to force users renew their password periodically. Default credentials: admin/admin The change of the default "admin" password is enforced at the first connection. It is also recommended to change the default "admin" username through the Users page **(Settings >>> Users)**. Follow embedded help for instructions on how to edit a user account. Supported authentication methods: LDAP and Radius, follow embedded help for instructions on how to configure it. The predefined account (admin) is set by default as "User account never blocks". It is recommended to edit these settings: On **Settings >>> Users**, Local Users section, click the Edit icon for the admin account to edit the settings. Uncheck the box for "User account never blocks" in Lock account section and click Save. This will result in enforcing the policies related to unsuccessful login attempts and account locking for the "admin" account.

Category	Description
Host Security	**Vulnerability Scanning** It is possible to install and use third-party software with **Green Motion DC 30/60**. Any known critical or high severity vulnerabilities on third party component/libraries used to run software /applications should be remediated before putting the device | system into production. • Eaton recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. For COTS components (e.g., applications running on Windows), vulnerabilities can be tracked on the National Vulnerability Database (NVD), available at https://nvd.nist.gov/. • Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as possible. **Note:** Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.
	Malware Defenses - Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.
Application Security	Application security is important as applications are most actively used and exposed interface s in a device. This makes applications prime target to attackers. **Green Motion DC 30/60** provides a platform on which customers can customize and host applications according to their requirements. Security vulnerabilities in these applications may expose the underlying device to attack. Eaton recommends observing best practices for secure system development when customers develop and host an application on the device: • Privacy and Security by Design: The application should take security and privacy into consideration from the outset, including at the stage of defining requirements and assessing the associated risks. • Communication Protection: If the application communicates over the network, Eaton recommends encrypting the communications in accordance with the applicable level described by the FIPS 140-2 standard. • Access Enforcement: The application should provide the ability to enforce access controls to protect the application against unauthorized access and to protect accounts against unauthorized authentication attempts (for example, through account lockout). • Least Privilege: Any application developed by the customers should not run with root account privileges. The root account has full control over and access to the operating system. Therefore, if an application that requires root privileges has any security vulnerability, it endangers the entire system. • Input Checking: All input to the application should be sanitized before storing and processing by the application to protect against malicious code injection. • Output Handling: Data output by the application for user consumption, including error messages, should be appropriately handled to avoid revealing valuable information about the application and the underlying system. • Password Management: The application should securely store and transmit credentials (for example, encrypting authentication traffic, and salting and hashing passwords in transit and at rest). Password complexity should be implemented, and password should be masked when entered on-screen. • Secure Coding Practices: Follow secure coding practice while developing applications for the device (for example, implementing multiple security layers, verifying authorization for all requests, conducting code reviews, etc.). • Administration Interface: The interface for administering the application should be separated from the end-user interface. • Session Controls: All application sessions should be encrypted, logged, and monitored. • Event Log Generation: The application should have the capability to log security related events at a minimum, including the time, date, and user.
Risk Assessment	Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, and reputation), organizational assets, individuals, other organizations resulting from the operation and use of information systems. Eaton recommends conducting a risk assessment to identify and assess 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. Customer are recommended to use relevant security tools at the system level to support administration, monitoring and incident handling and security evaluation of the product.

Category	Description
COTS Platform Security	Commercial off the shelf software (COTS) refers to any software pre-built by a third-party vendor and purchased or licensed for use by an enterprise. COTS provide powerful tools at a cost-effective price to meet your company's needs. There are many benefits to using COTS, bringing in untested third-party applications can leave your company open to the same threats as using any untested code. Vulnerabilities in third-party applications or software layers can lead to data loss, denial of service, cross-site-scripting (XSS), SQL Injection and a variety of other attacks by hackers or malicious software. 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.
Time Synchronization	Time synchronization is important as every aspect of managing, securing, planning, and debugging a network involves determining when events happen. Network operations require time-synchronized information to ensure optimal network performance. Time also provides the only frame of reference between all devices on the network. Many operations in power grids and IT networks heavily depend on precise timing information. Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588). Time synchronization can be configured under **Settings >>> General**, DATE & TIME section User can select a time zone and sync mode: Dynamic (NTP) / Manual. NTP server can be obtained from DHCP. CSMS server regularly sends heartbeat messages to CSC that contain a timestamp and can be used to sync time as well. **If the NTP service is enabled and running, however, OCPP time synchronization is disabled.**
Remote Access	Industrial control systems are migrating to new communication technologies. Technologies associated with remote access can often create situations that cause industrial control systems to inherit undesirable security vulnerabilities. Remote access is mostly targeted. 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 security. Remote access can be configured for LDAP or RADIUS servers. After properly configuring the server, the remote access capabilities and permissions can be configured under **Settings >>> Users**, LDAP or RADIUS section. Follow embedded help for instructions on how to configure it.
Logging and Event Management	Audit logs are required to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. • Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities. • Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.). • Ensure that logs are retained for a reasonable and appropriate length of time. • Review the logs regularly. The frequency of review should be reasonable, considering the sensitivity and criticality of the system | device and any data it processes. • Log files have defined maximum size. If that size is reached a new file is created and the previous one is backed up. The CSC can hold, for each of the logfile types, up to 3 backup versions plus the current version (which is being supplemented by new lines when any logged event occurs). Upon the next file rotation, a new file is created, and the oldest backup file is deleted. Logging is configured by default and cannot be disabled. Logs can be accessed under MAINTENANCE section: • **Maintenance >>> System logs** • **Maintenance >>> Services, Maintenance section**
Secure Maintenance	A system/device needs maintenance to make sure it functions securely and optimally. This involves continuous monitoring processes, perform scheduled reviews and assessing the components periodically and when needed. Various tools intended to facilitate the activities of maintenance personnel can be found in the device under Maintenance menu item. Under **Maintenance >>> Services**, the following tools are available: **Maintenance >>> Services >>> Sanitization** • Performs sanitization of the CSC. See the Decommissioning or Zeroization section below. **Maintenance >>> Services >>> Reboot** • Performs reboot of the system. **Maintenance >>> Services >>> Settings** • Allows to save/restore the settings of the CSC. **Maintenance >>> Services >>> Maintenance** • Allows to download the maintenance report. The report consists of a number of logs from various components of the system. It can be accessed under

Category	Description
Secure Firmware updates	The device purchased may be running on older firmware version. It is recommended to check for latest firmware updates available from Eaton. Update device firmware prior to commissioning/deploying the device into your environment. 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. There are few processes involved in the FW update: • FW version is automatically checked during product installation/commissioning and when needed, Installer is asked to download and upgrade the FW. • CSC is typically connected to the 3rd party CSMS system (using OCPP1.6+ standard protocol). CSMS system can force the CSC to upgrade FW when a new version is available. • Optionally CSC can be registered and communicate via the Eaton Charge Central cloud gateway. Charge Central will be able to trigger FW upgrade when selected by customer (using the same OCPP protocol) Please check Eaton’s cybersecurity website for information bulletins about available firmware and software updates.
Business Continuity / Cybersecurity Disaster Recovery	The BCP coordinates efforts across the organization and uses the disaster recovery plan to restore hardware, applications and data deemed essential for business continuity. BCP’s are unique to each organization as they describe how the organization will continue business in an emergency situation. **Plan for Business Continuity / Cybersecurity Disaster Recovery** Eaton recommends incorporating **Green Motion DC 30/60** into the organization’s business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system | device data should be backed up and securely stored, including: • Updated firmware for **Green Motion DC 30/60**. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated. • The current configuration. • Documentation of the current permissions / access controls, if not backed up as part of the configuration. The Save Reset Restore (SRR) feature is available in the **Green Motion DC 30/60**. The last step in the configuration in the user interface allows the user to export configuration. At the same time, when the user starts to configure the **Green Motion DC 30/60**, there is the option to upload the saved configuration.
Secure Operations Guidance	Operations Guidance contributes to demonstrate that appropriate and proportionate measures have been taken to control cyber security risks. It helps users to view operations from the perspective of an adversary in order to protect sensitive information from falling into the wrong hands. Eaton recommends that end user should follow the recommended practices in the above sections for secure operations of the product. Following points are also recommended - • Administrators should regularly monitor user accounts and keep an eye for any unauthorized activities, users etc. • Users should not share their passwords and accounts and change passwords at regular intervals in accordance with your organization’s policies. • Implement precise change management processes that your employees should follow when network changes are performed. All changes should be logged and controlled so they can be monitored and audited. • Restrict access to network devices using AAA authentication. In the military and other government entities, a “need-to-know” basis is often used as a rule of thumb regarding access and sharing of information. • Give your employees the minimum access necessary to perform their jobs. Practice the principle of least privilege. • Implement dual control. Make sure that those who work on your network are not the same people in charge of security. • Automate tasks to reduce the need for human intervention. Humans are the weakest link in any organization’s operational security initiatives because they make mistakes, overlook details, forget things, and bypass processes. • Incident response and disaster recovery planning are always crucial components of a sound security posture. Even when operational security measures are robust, you must have a plan to identify risks, respond to them, and mitigate potential damages.
Vulnerability Disclosure	Eaton recommends reporting all cybersecurity incident and vulnerabilities. Eaton has an incident response process to handle reported incidents/vulnerabilities. The incident response process helps in determining fix/mitigations and communicate advisory to customer in time. Link below should be used for reporting cybersecurity incident and vulnerabilities: https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/vulnerabilitydisclosure.html

Category	Description
Product Integration	The purpose of Product Integration (PI) guideline is to deploy components, ensure that the product, as integrated, behaves properly and deliver the product. Eaton recommends following the installation and user manuals provided with the product for deployment and integration of the product in its intended environment. It is also recommended to end user to follow guidelines provided in Part 3 – Defense in Depth during integration of product for the following for a secure product integration: • Policies & Procedures • Physical Security • Network Security • Host Security • Application Security Product is delivered in the integrated and tested form to the customer. Following documents are provided to the customer and relevant personnel for different purposes: • Installation Manual • Service Manual • User Manual
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.  Security Categorization Low Leaving Org Control? No Clear Yes Purge Destory Clear Validate Documents No No Security Categorization Moderate Reuse Media? Yes Leaving Org Control? Exit Yes Purge No Security Categorization High Reuse Media? Yes Leaving Org Control? Yes Destory No **Figure 1:** Sanitization and disposition decision flow **Embedded Flash Memory on Boards and Devices** • Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory. • **Clear:** If supported by the device, reset the state to original factory settings. • The **Green Motion DC 30/60** allows to clear the data by sanitization (**Maintenance >>> Services**, SANITIZATION section). By sanitization, data is removed from a device. Data may not be recovered or reconstructed using normal system functions or software file/data recovery utilities. Please not that there are no PII data present in the CSC. • **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. • As the flash memory of the **Green Motion DC 30/60** board can be identified using the documentation, the option to destroy the memory independently is advisable. • **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] 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

[R8] Characterization of Potential Security Threats in Modern Automobiles - NHTSA
https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization PotentialThreatsAutos(1).pdf

[R9] Threat Modeling for Automotive Security Analysis
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Powering Business Worldwide

Eaton Industries Manufacturing GmbH
Place de la Gare 2
1345 Le Lieu, Switzerland

Publication No. MZ090023EN
June 2025