PDU Cybersecurity Manual

Cybersecurity consideration for PDU Network module

Powering Business Worldwide

Contents

Introduction

This Power Distribution Unit (PDU) Network module has been designed with Cybersecurity as an important consideration. Number of Cybersecurity features are now offered in the product which if implemented as per the recommendations in this section would minimize Cybersecurity risk to the Network module. This section "secure configuration" or "hardening" guidelines provide information to the users to securely deploy and maintain their product to adequately minimize the cybersecurity risks to their system.

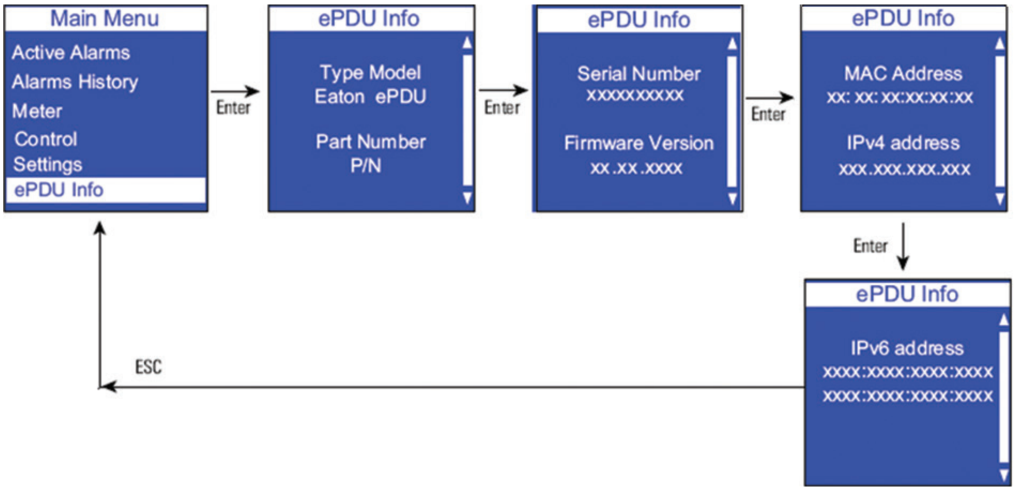
Eaton is committed to minimizing the Cybersecurity risk in its products and deploys cybersecurity best practices and latest cybersecurity technologies in its products and solutions; making them more secure, reliable and competitive for our customers. Eaton also offers Cybersecurity Best Practices whitepapers to its customers that can be referenced at www.eaton.com/cybersecurity

Secure configuration guidelines

Asset identification and Inventory

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 Network module supports the following identifying information - manufacturer, type, serial number, f/w version number, and location.

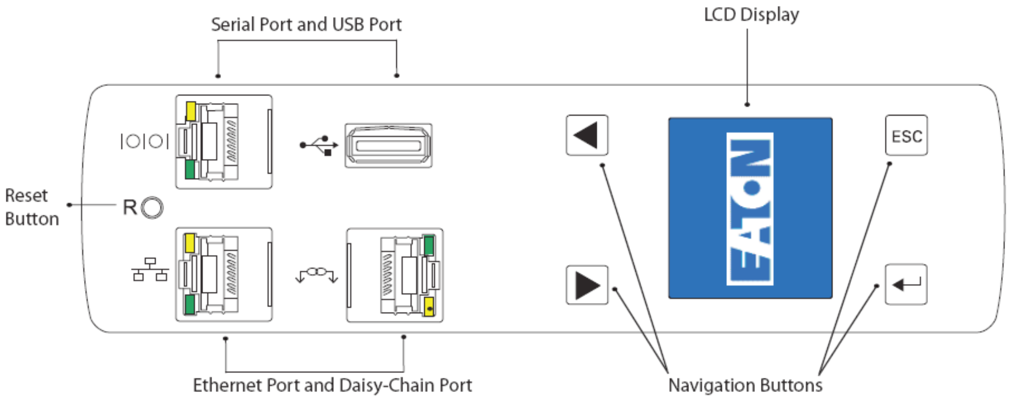
The previous information could be accessed through the LCD Display:



Physical protection

Industrial Control Protocols don't offer cryptographic protections at protocol level, at physical ports and at controller mode switches leaving them exposed to Cybersecurity risk. Physical security is an important layer of defense in such cases. Network module is designed with the consideration that it would be deployed and operated in a physically secure location.

- Physical access to cabinets and/or enclosures containing Network module and the associated system should be restricted, monitored and logged at all times.
- 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.
- Attacker with unauthorized physical access to the device could cause serious disruption of the device functionality. A combination of physical access controls to the location should be used, such as locks, card readers, and/or guards etc.
- Network module supports the following physical access ports : serial, Ethernet, Daisy-Chain and USB ports. Access to them need to be restricted. The next figure presents the location of this physical access ports :



- Do not connect unauthorized USB device for any operation (e.g. Firmware upgrade, Configuration change and Boot application change).
- Before connecting any portable device through USB, scan the device for malwares and virus.

Authorization and access control

It is extremely important to securely configure the logical access mechanisms provided in Network module to safeguard the device from unauthorized access. Eaton recommends that the available access control mechanisms be used properly to ensure that access to the system is restricted to legitimate users only. And, such users are restricted to only the privilege levels necessary to complete their job roles/functions.

- Ensure default credentials are changed upon first login. Network module should not be commissioned for production with Default credentials; it's a serious Cybersecurity flaw as the default credentials are published in the manuals.
- No password sharing – Make sure each user gets his/her own password for that desired functionality vs. sharing the passwords. Security monitoring features of Network module are created with the view of each user having his/her own unique password. Security controls will be weakened as soon as the users start sharing the password.
- Restrict administrative privileges - Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Limit privileges to only those needed for a user's duties.
- Perform periodic account maintenance (remove unused accounts).
- Change passwords and other system access credentials whenever there is a personnel change.
- Use client certificates along with username and password as additional security measure.

Access methods

CLI with serial port

Security Access	Description
Access is by user name and password	Always enabled

CLI with LAN Ethernet port

Security access	Description
Available methods: • User name and password • Access protocols that can be enable or disable • Secure SHell (SSH)	For high security, use only SSH. • With Telnet, the user name and password are transmitted as plain text. • Enabling SSH disables Telnet • Enabling SSH provides encrypted access to the CLI commands to provide additional protection during data transmission.

SNMPv1 and SNMPv3 access

Security access	Description
Available methods for SNMPv1: • Community name with public or private profiles • Three access communities with read/read-write/no access	SNMPv3 has additional security features including : • An authentication password • Encryption of data during transmission with a privacy key
Available methods for SNMPv3: • Four User Profiles • Authentication through an authentication password • Encryption through a privacy key	

Energy wise access

Security access	Description
Available methods: • Energy wise Domain name definition • Authentication through shared secret password/key	Enables EnergyWise on the network device, assigns it to a domain with the specified domain-name Sets the domain security mode, and sets the domain password to authenticate all communication in the domain

File Transfer Protocols

Security access	Description
Available methods: • User name and password • Selectable server port • FTP Server and access protocols can be enabled or disabled • FTP over SSL (FTPS) available and can be enabled or disabled	With FTP, the user name and password are transmitted as plain text and files transferred without encryption. Using FTPS encrypts the user name and password and the files being transferred, such as firmware updates, configuration files, log files, Web files.

Web server

Security access	Description
Available methods: • User name and password • Selectable server port • Web interface access that can be enable or disable • Secure Sockets Layer (SSL) with certificate key size from 1024 to 2048	In HTTP authentication mode, an authentication by challenge-response is used. In consequent the user name and password are never clearly transmitted. SSL is available on the Web browsers supported for use with the PDU Network module. The Web protocol HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.

LDAP

Security access	Description
Available methods: • Centralized authentication of access rights • Selectable server port • LDAP over SSL (LDAPS) or Start TLS encryption method • Authority Certification certificate • Simple or SASL Digest MD5 Bind type	LDAP (Lightweight Directory Access Protocol) is an authentication, authorization, and accounting service used to centrally administer remote access for PDU Network module or other device.

RADIUS

Security access	Description
Available methods: • Centralized authentication of access rights • Selectable server port • Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) authentication protocol • RADIUS server access that can be enable or disable • A server secret shared between the RADIUS server and the PDU Network module.	RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization, and accounting service used to centrally administer remote access for PDU Network module or other device.

Users, roles and privileges management

The level of access privilege determines what the user will see and what actions the user can perform. For example, the level of access privilege determines which menu items the user can access or which fields display on individual setting and configuration dialogs. Any menu or dialog functions that are not included in the access privilege set for a user do not display, or are they are grayed-out.

These accounts can be configured not only for individuals, but also for groups. All remote users and administrators belong to a remote group and their access privileges are defined from this group. Remote accounts also provide a way to attach LDAP users

Three user roles can be assigned these access privilege levels:

- SuperUser Administrator
- Local or Remote Administrators
- PDU-User

SuperUser administrator

There can be one SuperUser and up to eight standard local or remote administrators.

Only one user can be the SuperUser Administrator. This defaults to the local user, but a SuperUser should be assigned at first connection. This account is not accessible or editable by the standard administrators or PDU-Users/ Outlet Users. The SuperUser always has read-write privileges to view and edit all data, plus the following privileges restricted only to the SuperUser:

- Exclusive access to modify the SuperUser account settings
- Exclusive access to XML Web services
- Upgrade firmware

The default Administrator login and password is “admin” and must be changed at the first connection.

Local or remote administrator

Up to eight standard administrators (local or remote) can be assigned. Only accessible menu items display for the user according to the assigned permissions.

Read-write access

A local or remote administrator who is assigned read-write access can perform the following:

- Access to up-to-date PDU data and measurements
- Create, modify, or disable an administrator or user account except for the SuperUser
- Configure e-mail recipient addresses for e-mail notification to users
- Restart the communications module
- Access to both the Serial interface and the Web interface (some restrictions apply)
- Access to all menus on the Web interface
- Access to retrieved PDU up-to-date data and measurements
- Clear logs

Read-only access

A local or remote administrator with read-only access has limited privileges, including:

- Access to up-to-date PDU data and measurements
- Has the authority to change the password, but not the login (Remote PDU-Users cannot change the login or password)
- Access to the Network and Date and Time Settings menu (some restrictions apply)
- Access to both the Serial interface and the Web interface
- Can access the log and notifications submenu, but cannot clear the logs data
- Cannot configure the TCP/IP, SNMP Global Security, and LDAP settings

No access

An administrator with no access is not authorized to access to the Web page.

Local or remote PDU-user

Read-write access

A local or remote PDU-User with read-write access has limited privileges, including:

- Cannot access the following menus: Devices, Syslog, Network (TCP/IP, SNMP, EnergyWise, Global security, LDAP, and Radius
- Has the authority to change the password and e-mail address and the login (Remote PDU-Users cannot change the login or password, but can change their own e-mail address.)
- Only accessible menu items display for the user according to the assigned permissions.

Read-only access

A PDU-User with read-only access has limited privileges, including:

- Access to up-to-date PDU data and measurements
- Access to both the Serial interface and the Web interface (some restrictions apply)
- Access to the log and notifications submenu, but cannot clear the data from logs
- No access to the TCP/IP, SNMP Global Security, and LDAP settings
- Cannot upload the communication module configuration file or upgrade the firmware
- Cannot change his profile or another user's account

No access

A PDU-User with no access privileges is not authorized to access to the Web page.

Session management

The following session management restrictions apply:

- There can only be one SuperUser with read-write access rights and up to eight multi-users with configurable access rights.
- When the administrator connects, any existing read-write sessions are closed. The other user (or users) will be asked to authenticate and open a new read-only session.
- If a user with read-write access is logged in and another user with read-write access wants to log in, the following message displays: "Another user is logged in with R/W access. Continue as R/O?"

PDU sessions are also limited in the following ways:

- Only five standard sessions without SSL (Secure Sockets Layer) or SSH (Secure Shell) sockets are allowed.
- Only two secure sessions can be running at the same time.
- Only an administrator can have two simultaneous sessions open in HTTP/HTTPS (Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure), Telnet/SSH.

During an HTTP/HTTPS or Telnet/SSH session, the session times out if there is no activity for five minutes. After a session times out, you must login again.

The **Lightweight Directory Access Protocol (LDAP)** allows the sharing of information about users over an Internet Protocol (IP) network.

A password has to be set to authenticate an user with a LDAP directory.

The eNMC card proposes two ways to encrypt LDAP connections with SSL/TLS:

- **LDAPS** encryption method
- or Start TLS encryption method

Using a simple or a SASL Digest MD5 mechanism to authenticate the user.

A Certificate Authority can be uploaded by the Web interface of the eNMC card to validate the identity of the LDAP client.

The **Remote authentication dial-In User Service (RADIUS)** centralizes Authentication, Authorization and Accounting management for users who connect to the eNMC card. The client and Radius server are authenticated through the use of a shared secret string. The RADIUS server checks that the information is correct using authentication schemes such as:

- Password Authentication Protocol (PAP)or Challenge-Handshake Authentication protocol (CHAP).

The **Simple Network Management Protocol (SNMP)** is an internet standard protocol for collecting and organizing information about devices over IP network. Use SNMPv3 to get security features:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorized source.
- Integrity – Message integrity to ensure that a packet has not been tampered while in transit including an optional packet replay protection mechanism.
- Authentication – to verify that the message is from a valid source.

For that, configure:

- An Authentication Password
- A Privacy Key

Deactivate unused features

Network module provides multiple options to upgrade firmware, change configurations, set power schedules, etc. The device also provide multiple options to connect with the device i.e. SSH, SNMP,SMTP,HTTPS etc. Services like SNMPv1 are considered insecure and Eaton recommends disabling all such insecure services. **HTTPS should be activated on the first use of the Network module to reinforce the Network Security.**

Network security

Network module provides network access to facilitate communication with other devices in the systems and configuration. But this capability could open up a big security hole if it's not configured securely.

Eaton recommends segmentation of networks into logical enclaves and restrict the communication to host-to-host paths. This helps protect sensitive information and 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,

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 Network module to operate smoothly.

The following server protocols and features may be enabled or disabled:

Protocol	Default state	Port number (Configurable)
FTP	Disable	21
FTPS	Enable	21
SSH	Enable	22
TELNET	Disable	23
HTTP (Basic and MD5 message-digest)	Enable	80
HTTPS (SSLv3/TLSv1)	Disable	443
Serial Port - Command Line Interface	Enable	N/A
USB port	Enable	N/A
SNMPv1	Disable	161,162 (Trap)
SNMPv3	Disable	161,162 (Trap)

The following client protocol and features may be enabled or disabled:

Protocol	Default state	Port number (Configurable)
DHCP	Enable	68
DNS	Enable	53
Email/SMTP	Disable	25
LDAP	Disable	389
RADIUS	Disable	1812 (UDP)
SNTP	Disable	123
Syslog	Disable	514 (UDP)
TFTP	Enable	69 (UDP)
EATON scan port	Enable	4679 (UDP)
EATON alarm port	Enable	4680 (UDP)
Energywise	Disable	Remote Port : 43440 Listen Port : 48296

For secure Web communication with PDU Network Module, the Secure Sockets Layer (SSL) must be enabled by selecting HTTPS as the protocol mode to use for access to the Web interface.

The activation of the HTTPS limits the Daisy Chain capability and the simultaneous open sessions. The maximum number of Daisy Chain PDU is limited to 1 + 3 with 2 open HTTPS sessions.

For more details about the configuration of the previous protocol, please refer to the User Guide.

Logging and event management

Best practices

- Eaton recommends that all remote interactive sessions are encrypted, logged, and monitored including all administrative and maintenance activities.
- Ensure that logs are backed up, retain the backups for a minimum of 3 months or as per organization's security policy.
- Perform log review at a minimum every 15 days.

The Network module supports logging of system events both internally and externally. An internal log of more than 1000 events is automatically maintained for the review by administrative users. For permanent or long term log storage, Network module supports Syslog protocol; for immediate notification, Network module supports Email notification and SNMP traps.

The log entries include a sequential entry number, date/time stamp and event message. The event message is preceded with a number code heading defining the alarm or Event condition (for more detail, please refer to the User Guide).

The next key actions could be managed on the Network Module :

- Logs can be cleared
- Logs can be downloaded to your local PC
- Logs are saved in csv format and can be easily used with any spreadsheet program, such as Microsoft Excel, Open Office Calc, or Google SpreadSheets
- Logs can be attached to an alert email or a periodic email
- Logs contain all login/logoff, system information, user settings modification, and any alarm on a measurement exceeding a threshold

Secure maintenance

Best practices

Apply Firmware updates and patches regularly

Due to increasing Cyber Attacks on Industrial Control Systems, Eaton implements a comprehensive patch and update process for its products. 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.

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://eaton.com/cybersecurity and patch through http://powerquality.eaton.com/Support/Software-Drivers/Downloads/ePDU-firmware.asp

Conduct regular Cybersecurity risk analyses of the organization /system.

Eaton has worked with third-party security firms to perform system audits, both as part of a specific customer's deployment and within Eaton's own development cycle process. Eaton can provide guidance and support to your organization's effort to perform regular cybersecurity audits or assessments.

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 Network module. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated on Network module.
- Backup of the most current configurations.
- Documentation of the most current User List.
- Save and store securely the current configurations of the device.

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

Eaton
EMEA Headquarters
Route de la Longeraie 7
1110 Morges, Switzerland
Eaton.eu

Publication No. IMXXXXXXXXE / TRE-P-1456
August 2018

Powering Business Worldwide