GE VERNOVA

MiCOM

P40 5th Generation

Secure Deployment Guide

Software Version: AA

GE Publication Number: GER-4970

Publication Date: August 2024

Cybersecurity Disclaimer

The MiCOM P40 family of products are digital devices designed to be installed and operated in utility substations and industrial plant environments and connected to secure private networks. These products should not be connected to the public internet.

GE strongly recommends that users protect their digital devices using a **defence-in-depth** strategy which will protect their products, their network, their systems and interfaces against cybersecurity threats. This includes, but is not limited to:

- Placing digital devices inside the control system network security perimeter
- Deploying and maintaining access controls, monitoring and intrusion detection
- Security awareness training
- Security policies
- Network segmentation and firewalls installation
- Strong and active password management
- Data encryption
- Antivirus and other mitigating applicable technologies

MiCOM P40 Generation 5 relays are available with enhanced cybersecurity mechanisms with flexible configuration. GE Vernova strongly recommends usage of the security controls to protect the system against cybersecurity intrusion.

For additional details and recommendations on how to protect MiCOM P40 relays, please see the *Hardening Setup* section below. From time to time, we may also provide additional instructions and recommendations relating to the MiCOM P40 Family and cybersecurity threats or vulnerabilities.

As a user, it is your sole responsibility to make sure that all MiCOM P40 relays are installed and operated in accordance with its cybersecurity capabilities, security features, and the instructions and recommendations. Users assume responsibility for all risks and liabilities associated with damages or losses incurred in connection with any cybersecurity incidences.

Contents

1. Introduction

This document describes the best practices to securely install and operate your MiCOM P40 relay and the accompanying MiCOM S1 Agile configuration software. It also provides an overview of the supported cybersecurity features. This document applies to MiCOM P40 5th Generation, Software Version AA and later.

MiCOM P40 5th Generation relays have effective advanced security controls in place. The relay supports:

- Local as well as centralized user authentication
- Role Based Access Control (RBAC)
- Logging security events in the syslog format to configured syslog server
- Secure firmware upgrade

It supports the creation of up to 10 user accounts on the relay with unique usernames. Roles can be assigned to these accounts. As part of product hardening, it is possible to disable unused ports, protocols, and services.

This document describes security related information on the recommended configurations.

This document assumes that the reader is familiar with the product.

2. Product Defence-in-Depth Strategy

The product implements the following security features:

- Secure design process to ensure that cybersecurity is part of the design process and not an afterthought.
- Security and penetration testing to detect, as far as possible, vulnerabilities at the design stage.
- Digital signature of firmware and software, to allow verification of integrity and authenticity before installation.
- Monitoring of software components vulnerabilities and security bulletins, to inform users of newly discovered vulnerabilities and threats.
- User authentication.
- Role-based access control, to enforce correct privileges in accordance with the area of responsibility.
- Password and user account policies, to prevent use of weak passwords and password brute force attack.
- Centralized user management (using RADIUS), to allow prompt removal of user accounts.
- Security event logging for post-incident analysis.
- Centralized security event logging using SYSLOG protocol. This allows events to be sent to a Security Operations Centre (SOC) for close to real time security monitoring.
- Hardening to reduce the attack surface (making it more difficult for cybersecurity attacks).

To complement the defence-in-depth strategy, the product must be installed in a secure environment. The product cannot mitigate DoS attack through network interface overload.

3. Environment

The MiCOM P40 5th Generation relay and S1 Agile configuration software is designed to be installed and operated in a utility and industrial environment with connection to a private network inside the Electronic Security Perimeter (ESP).

Although the rest of this guide describes security measures at the product level, requirements to achieve good security go beyond just the product.

We recommend that your security concept considers the whole system, in which the relays are installed, in accordance with a **Defence-in-Depth** approach. Security includes (but is not restricted to):

- Physical security such as building access control and locked cabinets.
- Security policies.
- Access control.
- Network security measures, such as IP segmentation, use of firewalls and use of secure protocols. Consider employing an Operations Technology (OT) next generation firewall. This would enforce OT policy at the protocol level and monitor and block malicious activity and unintended disruptions.
- Protection/Control system devices, such as the MiCOM P40 Family, should not be connected directly to the internet.
- Security monitoring, such as network intrusion detection systems, security event logging using a centralized server.
- System hardening by disabling unused processes and ports, and removal of unused connection links.
- Remote configuration/monitoring of the device must be done from a secure engineering workstation through a trusted network link.
- Use secure methods for remote access, such as a Virtual Private Network (VPN), dual authentication, recognizing that the VPN is only as secure as the connected devices.
- We recommend that S1 Agile configuration software is not continuously connected to a MiCOM P40 relay when a relay is in service. It is not intended for SCADA/continuous monitoring applications.

4. Secure Installation - Hardening

4.1. Verifying software integrity

Before installing any software, the installation package integrity must be verified.

GE Vernova software is digitally signed. You verify a piece of software by right-clicking on the filename and selecting the **Digital Signature** tab in the **Properties** menu. The signature details must read "This digital signature is OK".

The software must not be installed if the signature verification fails. If this happens, please contact your support organization.

As part of the "Secure Firmware Upgrade", the "Firmware Download Tool" verifies the firmware integrity and authenticity before upgrading the firmware in the relay.

4.2. Upgrading firmware to the latest version

We strongly recommend you upgrade the firmware to the latest sub-version of the major version used, to take advantage of all the fixed known vulnerabilities.

Any firmware upgrade should be organised through the After Sales Service department in Stafford, UK, or a regional Local Service Centre. The firmware upgrade should normally be performed by GE Vernova personnel, or by suitably prepared and competent persons after instruction from GE Vernova personnel. A separate MiCOM P40 firmware download procedure guide is available.

4.3. Disable unused protocols and ports

The MiCOM P40 5th Generation relay supports deactivation of the front USB port, rear RS485 ports and Ethernet ports. By default, these physical ports are enabled.

The MiCOM P40 5th Generation relay supports various protocols for interaction with SCADA and or another user system. Supported protocols include Courier, IEC 60870-5-103, DNP 3.0, IEC 61850, IRIG-B, SNTP, PTP and SNMP.

The list of logical ports with their default status is tabulated as part of Section 6, List of Physical and Logical ports.

In compliance with NERC-CIP, most of the MiCOM P40 logical ports are user-configurable - they can be enabled or disabled. We recommend that you disable the protocols and logical ports that will not be used. The logical port details can be found in the section "Supported Protocols".

4.4. User authentication and roles:

4.4.1. Modify default passwords

The MiCOM relay supports roles in line with IEC 62351-8:2020 – SECADM, SECAUD, ENGINEER, *OPERATOR, VIEWER, INSTALLER, RBACMNT. By default, the relay will support the following user accounts:*

User Name	IEC 62351-8 Roles	Default Password
ADMIN1	SECADM	ChangeMe1#
RBACMNT1	RBACMNT	ChangeMe2#
ENGG1	ENGINEER	ChangeMe3#
VIEWER1	VIEWER	ChangeMe4#

When you receive a MiCOM P40 5th Generation relay, we recommend that you log into the relay using the default password and change the passwords using unique strings for all the accounts.

Privileged users with “Administrator” roles can change passwords for all local accounts.

We recommend that you configure a unique and strong password. Passwords can be modified from the HMI as well as the S1 Agile configuration software.

4.4.2. Create non-shared user accounts

MiCOM P40 5th Generation relays support centralized or server authentication using a RADIUS server for up to 10 user accounts. This enables users to have non-shared accounts with restricted privileges. Only a user with role SECADM or RBACMNT can configure new users and their roles.

We recommend that you remove unused accounts from the server configuration. Only active accounts should be maintained.

5. MiCOM P40 5th Generation Secure Installation

MiCOM P40 5th Generation relays have security features including Role-Based Access Control.

5.1. Security recommendations

MiCOM P40 5th Generation relays offer flexible modification possibilities for the security configuration based on the user's setup and policies. We recommend the following configuration:

- **Serial inactivity timeout:** Inactivity timeout for front panel and UI interface (Setting name: FP InactivTimer and UI InactivTimer). Recommended value: 5 minutes
- **Password policy:** Recommended value: Strict
- **Maximum number of failed logins attempts before account lockout (Setting name: "Attempts Limit):** Recommended value: 3 Attempts Limit; Lockout Period = 30 seconds
- **Communication ports:** Disable communication ports and protocols when not used
- **Courier protocols:** Disable Courier protocols during normal operation phase
- **Communication ports and protocols:** Disable/disconnect communication ports and protocols when not used
- **Security bypass option:** Do not use this during normal operation
- **Remote/centralized authentication server:** Use this where possible

All security settings are explained in the product manual.

5.2. Bypass access:

This option offers a bypass of the access control for the Local (Front Panel and Front port) as well as the Front Panel only. By default, the bypass is disabled.

We strongly recommend that you keep the **Bypass Access** setting disabled (not bypassed) when MiCOM P40 5th Generation relays are in service. It is important to ensure role-based access control is in place and unauthorized personnel are not allowed to modify the configuration or enter commands.

5.3. Local configurable user accounts

- The MiCOM P40 5th Generation relays offer configuration of up to 10 user accounts. It is advised to configure at least two user accounts with the SECADM role or one RBACMNT. This is to ensure easy access in case the password is lost for any account.
- Each user should be given the least privileges by associating them with an adequate role. This will give a user sufficient permission to perform their assigned tasks, but not more permissions than is necessary.
- User configuration allows the creation of a new account with a unique username, password and role for that user.

5.4. RADIUS authentication

The MiCOM P40 5th Generation relays support device level authentication as well as centralized authentication. It is recommended to utilize the centralized authentication facility as it offers easier user database management.

There are advantages for P40 5th Generation relay users to configure two RADIUS servers for authentication as this will provide for availability in case one of the servers cannot be reached. The NEW MiCOM relay will first try to get the user authenticated with the Primary RADIUS server. If it cannot be reached, then the relay will try to get the user authenticated using the secondary RADIUS server.

Configuration for RADIUS authentication (settings: server IP, port, vendor ID, timeout and retries) can be done using the P40 5th Generation relay HMI and the S1 Agile configuration software. The RADIUS server also needs an authentication secret to be available for the NEW MiCOM relay. The Secret is a string, that can be configured using the MiCOM P40 5th Generation relay and MiCOM S1 Agile.

5.5. Password expiry and age

The MiCOM P40 5th Generation relay supports configurable passwords life. Using this configurable option, user account passwords have a life of 30 days minimum to 730 days maximum. When Password Expiry is configured as Disabled, the passwords can be used until the user manually changes them.

We recommend enabling the password expiry feature and password age as 180 days (default), to ensure passwords are changed regularly.

5.6. Secure event logging

5.6.1. Syslog server

The P40 5th Generation supports **syslog over UDP**.

MiCOM P40 5th Generation relays capture security-related events and sends these to a centralized syslog server (assuming a syslog server is configured and reachable). We recommend using a syslog server for event logging as it provides a centralized view of all system events, and it enforces long term storage of logs. Depending on the level of severity, a syslog server (or a reporting tool gathering information from a syslog server) can produce reports and charts etc. All severity levels follow RFC 5424.

For a list of security events and their severity, please refer to the product manual.

5.6.2. Security events storage on relay

MiCOM P40 5th Generation relays save the security events as part of "Sequence of events" in the relay. There is no separate security events file in this first release of MiCOM P40 5th Generation relays. The user can read the events using the S1 Agile configuration tool.

Due to capacity limitations and the nature of the circular buffer, we recommend that you download and archive these files in a secure place for auditing purposes, at regular intervals.

5.7. Maximum user connections to relay

At any given time, a maximum of 4 users with role "VIEWER" can connect to a MiCOM P40 5th Generation relay, as long as they have accessed from a different interface (FP/RP/HMI/Ethernet Port). A single user with a role other than "VIEWER" can connect to a relay.

On one interface, only a single user is allowed to connect to the relay.

5.8. Role permission mapping

MiCOM P40 5th Generation relays support 7 roles with pre-defined permissions for each role. The roles and their permissions are aligned to standard IEC 62351-8:2020. For more details, please refer to chapter "Roles and Permissions" in the product user manual.

6. S1 Agile Configuration Software

S1 Agile is configuration software designed to be used with MiCOM P40 5th Generation relays. With this, you can manage offline projects, connect to the relay, update the relay configuration, and monitor actual values like status, metering and diagnostics.

Communication between the configuration software and the MiCOM P40 5th Generation relay is carried out over Courier protocol. Sensitive information like the user password is transmitted in an encrypted format.

The relay supports the disabling of the Courier protocol as part of hardening. When the courier protocol is disabled, the relay's configuration cannot be modified. GE Vernova recommends the disabling of the Courier protocol during normal operation and after installation of the relay.

6.1. Secure firmware upgrade

The *P40 Download and Calibration* firmware download software can validate the firmware file's digital signature to ensure authenticity (publisher verification) and integrity of the firmware file. The software prohibits the firmware upgrade process if the file verification fails. This behaviour complies with the NERC-CIP 10 requirement.

The firmware upgrade for MiCOM P40 5th Generation relays can only be performed by a privileged user with the role "INSTALLER".

A separate MiCOM P40 firmware download procedure guide is available.

7. Maintaining Security

Once good security has been properly configured, it is important to create procedures to maintain security over time.

7.1. Periodic security audits

The configuration applied in the secure installation paragraph must be recorded.

Periodically, particularly after maintenance activity, the security configuration must be audited, and deviations tracked and fixed.

7.2. Backup and restore procedures

Firmware installation packages and configuration files must be backed up following any configuration/maintenance activity.

A restore procedure must be prepared for quick service restoration following an incident.

7.3. Vulnerability monitoring and firmware updates

GE Vernova responsibly discloses vulnerabilities found in its products.

Users should periodically check for newly published vulnerabilities @Security bulletins and available firmware updates.

Users should define a security update policy.

All GE Vernova software packages are digitally signed. Digital signatures must be verified before installation.

7.4. Reporting a vulnerability

Providing a legitimate pathway for vulnerability disclosure is an essential link between GE Vernova and the cybersecurity community.

To submit a vulnerability in a Grid Solutions product to the GE Vernova PSIRT team, please fill in the form at https://www.ge.com/security. Please do not include identifiable sensitive data (e.g. personal data and specific system configuration) within the body of the communication or any attachments (e.g. screenshots, images, or log files).

We actively encourage reports to be sent to us for remediation prior to a public disclosure, so that we can properly address any vulnerabilities.

We request the following when you report a vulnerability:

- Please provide your report in English.
- Include specific information about affected products, including model or serial numbers, geographic location, software version, and the means of obtaining the product.
- If you have developed a proof-of-concept for exploiting the vulnerability, please include the code and explanation.
- If you are aware of any incidents of this vulnerability being exploited on equipment in the field (e.g. a Grid Solutions' customer was directly impacted by this vulnerability), please inform us.
- Information on how you discovered the vulnerability, your thoughts on impact or CVSS scoring, and potential remediations will help us to triage the vulnerability more quickly.
- Please include relevant information about yourself or the company/organization you are representing, or whether you prefer to remain anonymous.
- Please let us know if you have a preferred method of contact during our internal triage process.
- Please include your intentions for disclosing the vulnerability to us, or if you intend to disclose the vulnerability to the public.

In response, you can expect the following from us:

- We will acknowledge receipt of your message within 48 hours.
- In the following phase of initial triage and assessments, an appropriate member of the GE Vernova PSIRT may reach out to you to:
    - Request additional information, or
    - Communicate an expected process and timeline, or
    - Notify you that the report is either out of scope or will not be triaged for other reasons
- Once we have conducted our own assessment of the vulnerability, we will communicate our process and findings after investigation.
- We will provide public recognition for the security researcher (if requested) and if the report results in a public disclosure.

By submitting a request, you acknowledge that Grid Solutions may use in an unrestricted manner (and allow others to do the same) any data or information that you provide to Grid Solutions. Your submission does not grant you any rights under Grid Solutions intellectual property or create any obligations for Grid Solutions.

8. Decommissioning

8.1. Secure decommissioning - configuration and sensitive data

The goal of secure decommissioning is to prevent unauthorized disclosure of information.

For organizations to have appropriate controls on the information they are responsible for safeguarding, they must first identify and classify information.

MiCOM P40 5th Generation relays:

- Information is stored in soldered flash memory on the CPU board.
- Passwords are stored locally and are protected by PBKDF2 with SHA-256, and a unique 64-bits salts to make clear text recovery extremely difficult by today's standards.

MiCOM P40 5th Generation relays support ways to help the user to Restore factory Defaults in the relay.

1. Defaulting security settings: The "Restore Security" setting is available under the SECURITY CONFIG column. Only the user with SECADM privileges can change this setting. If "Restore Security" setting has been done, all the security settings (including device users created) will be changed to factory defaults. The configuration will match the shipped relays from the factory environment.
2. Defaulting other than security configuration: The "Restore Defaults" setting is available under the CONFIGURATION column. It is possible to set the "Restore Defaults" setting to All Settings to restore the default values to all the relay settings, not only one setting group. An ENGINEER or INSTALLER Role is required to perform this action.

   Data (events, DR, fault records etc.) is left untouched when the Restore Defaults option is used.
3. Removing data records: Clearing of Records is possible using MiCOM S1 Agile. Only a user with ENGINEER role can clear the records in the relay. Using MiCOM S1 Agile, use the option of "Supervise Device" to bring up the Clear Records section and select the file types to be cleared.

   This behaviour matches with the Cybersecurity standards requirement to remove all customer specific data from the relay, when needed in situations like, returning the relay to GE Vernova for any service or to be released from active service and/or decommissioned. The goal of secure decommissioning is to prevent the unauthorized disclosure of information.

   After corrective action and return of the relay to the customer, MiCOM P40 5th Generation relays allow easy restoration of configuration. The product user manual has additional information in section "APPLY APPLICATION-SPECIFIC SETTINGS" regarding how a user can back-up a copy of the in-service settings for each commissioned MiCOM relay, to revert to the commissioned settings after servicing of the relay, or inadvertent unauthorized, or temporary setting changes after the settings defaulted due to a firmware upgrade, or when the device must be replaced.

9. Secure Operation Guidelines

To ensure secure operation of the MiCOM P40 5th Generation relay, we recommend that:

- Users are assigned a specific role at a level sufficient for the tasks they must perform.
- Users change their passwords when they believe there might be a possibility of unwanted disclosure.
- Default account passwords are changed before putting the device into operation.
- Users log out of their session when finished (although an inactivity timeout can be set to automatically terminate user sessions).
- The product is never connected to a public network, nor the Internet.
- Only the required services are configured and enabled.
- Periodically review all user accounts and disable/remove those accounts that are not active.

10. Appendices

10.1. The secure development life cycle process: IEC 62443-4-1

The IEC 62443-4-1:2018 is an internationally and widely recognized standard, which specifies process requirement for the secure development of products used in industrial automation and control systems". The life-cycle description includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life.

In ongoing efforts to support our customers and their challenges, Grid Solutions is pleased to announce that it has achieved IEC 62443-4-1 certification. This certification ensures that a secure development lifecycle process is well defined, implemented and enforced across all the product's lifespan - from the design to the end-of-life cycle.

10.2. Certification: IEC 27001

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.

GE Vernova has a culture of cybersecurity and is committed to protect its own and its customers data. Our MiCOM P40 5th Generation relay manufacturing site is IEC 27001:2013 compliant.

10.3. List of supported protocols

For MiCOM P40 5th Generation relays, communication protocols are supported based on options in the order code. The following table shows protocols, ports used, and their default configuration.

All the ports that are enabled by default cannot be disabled by design as they are a core service required for the reliable function of the device. The following tables detail the port/service list that would enable a user to facilitate port control through a firewall device found in their ESP.

MENU TEXT	UI	Col	Row	Data Type	Strings	Default Setting	Cell Type	Available Setting	Min	Max	Step
PORT HARDENING		25	1B	Secondary Heading			Heading				
Front Port		25	1C	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1
Rear Port 1		25	1D	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1
Rear Port 2		25	1E	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1
Ethernet Port		25	1F	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1
Courier Tunnel		25	20	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1
IEC 61850		25	21	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1

MENU TEXT	UI	Col	Row	Data Type	Strings	Default Setting	Cell Type	Available Setting	Min	Max	Step
SNTP		25	23	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1
PTP		25	24	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1
SNMP		25	25	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1
RADIUS		25	26	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1
SYSLOG		25	27	Indexed String	G37	Enabled	Setting	0 = Disabled or 1 = Enabled	0	1	1

10.4. IEC 62443-4-1 mapping

This SDG (Secure Deployment Guide) provides alignment with IEC 62443-4-1 requirements as shown in the table below:

SG-1 Product defense in depth	2 Product defence-in-depth strategy
SG-2 Defense in depth measures expected in the environment	3 Environment
SG-3 Security hardening guidelines	5 Secure installation 7 Maintaining security
SG-4 Secure disposal guidelines	8 Decommissioning
SG-5 Secure operation guidelines	9 Secure operation guidelines
SG-6 Account management guidelines	4 Secure installation
SG-7 Documentation review	Covered by NPI process and quality processess

11. List of Acronyms

ESP - Electronic Security Perimeter

PSIRT - Product Security Incident Response Team

RBAC - Role Based Access Control

OC - Order Code

Imagination at work

GE Vernova
St Leonards Building
Redhill Business Park
Stafford, ST16 1WT, UK
+44 (0) 1785 250 070
contact.centre@ge.com