H49

Deployment guide

Product secure Deployment Guide

Submitted by: GE Vernova

Revision No. 1.0

Month 08, 2025

Table of Contents

1 Introduction

This document lists best practices to securely install and operate H49.

It applies to H49-2.1.0 and later.

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

This document is the response to IEC62443-4-1 “Practice 8 - Security Guidelines” requirements.

2 Product Defense-in-Depth strategy

Note: This paragraph is the response to IEC62443-4-1 SG-1 requirement.

The product implements the following security features:

- Secure design process to ensure that cyber security is part of the design process and not an after thought;
- Security and penetration testing to detect as much as possible vulnerabilities at the design stage;
- Digital signature of firmware/software package to allow integrity and authenticity verification before installation;
- Monitoring of software components vulnerabilities and security bulletins to inform users of the newly discovered vulnerabilities and threats;
- User authentication and personal account;
- Role based access control and least privileges to enforce area of responsibilities;
- Password and user account policies to prevent use of weak passwords and password brute force attack;
- Centralized user management (using LDAP) to allow prompt removal of user accounts;
- Security event logging for post-incident analysis;
- Centralized security event logging using SYSLOG protocol to send event to a SOC and allow close to real time security monitoring.
- Secure configuration protocols using TLS to protect credentials and sensitive information while in transit;
- Hardening to reduce the attack surface;

To complement the defence in depth strategy, the product shall be installed in a secure environment. See paragraph 3 Environment.

Particularly, the product cannot mitigate DoS attack through network interface overload.

3 Environment

Note: This paragraph is the response to IEC62443-4-1 SG-2 requirement.

H49-2.1.0 is designed to be installed and operated in an industrial environment, connected to a private network.

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

GE Vernova recommends that security applies to the whole system in which the H49-2.1.0 is installed, following a defence-in-depth approach. Security includes (but is not restricted to):

- User security awareness training,
- Security policies,
- Access control
- Network security measures, such as segmentation, use or firewalls, use of secure protocols…
- Security monitoring, such as network intrusion detection systems, security event logging…
- Physical security, such as building access control, locked cabinets.

In addition, remote configuration/monitoring of the device (i.e. not from the front panel) shall be done from a secure engineering workstation through a trusted network link.

Refer to the H49-2.1.0 Secure Deployment Guide part in user manual (H49/EN M/R32) for more information on how to integrate H49 in a secure environment providing layers of security.

4 Secure Installation - Hardening

Note: This paragraph is the response to IEC62443-4-1 SG-3 and SG-6 requirements.

4.1 Verifying software integrity

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

GE Vernova firmware images are digitally signed.

H49-2.1.0 verifies the firmware signature during the firmware upgrade process.

An unverified firmware will be rejected.

In such a case, please contact your support organization.

4.2 Upgrading firmware to the latest version

H49 firmware must be upgraded to the latest version available for the major version used, to take advantage of all fixed known vulnerabilities.

To upgrade H49 product from a release prior to h49-2.1.0 follow below process:

1- Download the H49 configuration files

2- **Upgrade first to previous firmware release version h49-2.0.3.1**, if it is not yet your current version.

3- **Upgrade to h49-2.1.0**
DO NOT CHECK the option
"Check this box if you want to save the configuration before upgrading the firmware"

4- After the firmware upgrade, power off then power on the H49 product.

5- Restore your H49 configuration file

Refer to chapter "7.5.1.5 MANAGEMENT" of H49-2.1.0 user manual (H49/EN M/R32) for detailed information configuration management and firmware upgrade.

4.3 Disabling unused protocols

Hardening consists in disabling unused features in H49.

Most features won't be enabled unless explicitly configured.

The features listed below may be enabled by default or during the deployment and shall be reviewed:

- SSH command line interface
  Refer to “7.5.3.1 SECURITY SETTINGS” chapter of H49-2.1.0 user manual (H49/EN M/R32)
- SNMP
  Refer to “7.5.1.4 SNMP” chapter of H49-2.1.0 user manual (H49/EN M/R32)
- LDAP
  Refer to “7.5.3.3 LDAP SERVER” and “8.2.4.3.1 LDAP/SYSLOG” chapter of H49-2.1.0 user manual (H49/EN M/R32)
- PTP and NTP
  Refer to “4.8 TIME SYNCHRONIZATION” and “7.5.1.2 GLOBAL SETTINGS” chapters of H49-2.1.0 user manual (H49/EN M/R32)

See “8.1 List of supported protocols” for a list of all protocols and services that can be enabled by configuration.

4.4 Configuring certificates

H49 uses the secure protocols in the following cases:

- Access to the configuration interface through HTTPS
- Security event logging to a syslog server through TCP over TLS
- Central authentication through LDAP with STARTTLS

TLS needs a private key and public key certificate (PKC) to be deployed on the H49, and a PKC to be deployed on the engineering workstation.

Refer to “8.2.4.3 CERTIFICATE MANAGEMENT” chapter of H49-2.1.0 user manual (H49/EN M/R32).

Limitations:

- As H49-2.1.0 does not support Certificate Revocation Lists nor certificate auto provisioning, GE Vernova recommends self-signed certificates with a long expiring date.

4.5 User access control

While creating user accounts, care must be taken to associate only a minimum number of roles to accomplish the needed tasks.

4.5.1 Default user accounts

H49-2.1.0 is delivered with 2 factory user accounts:

User name	Default password	Roles
root	root	root
user	user	viewer engineer secadm secaud

The username of “root” account cannot be changed, cannot be deleted and cannot be disabled.

The password of “root” account can be updated through the Web HMI.

Password change is mandatory at first connection.

“root” account’s password shall be changed at the end of commissioning (e.g. SAT) activity.

“user” account’s password shall be changed at the end of commissioning (e.g. SAT) activity.

The root user is accessible only through the internal serial link connection.

Refer to following chapters of H49 user manual (H49/EN M/R32):

- “7.5.3.2 USER ACCOUNTS”
- “8.2.4.2 PASSWORD MANAGEMENT”

4.5.2 Local user account

H49-2.1.0 supports the creation of personal user accounts.

When centralized authentication is not used, personal user accounts shall be used for authentication.

When centralized authentication with LDAP is used (see section Central Authentication with Radius Below), at least one local user with required roles shall be created, to be used when the central authentication server is unreachable.

The passwords for these local accounts shall be kept secret until needed and changed after use.

Refer to following chapters of H49 user manual (H49/EN M/R32):

- “7.5.3.2 USER ACCOUNTS”
- “8.2.4.2 PASSWORD MANAGEMENT”

4.5.3 Role base access control

H49-2.1.0 supports 4 roles:

- Viewer
- Engineer
- Secadm
- Secaud

Refer to “7.5.3.2 USER ACCOUNTS” chapter of H49 user manual (H49/EN M/R32).

For details of permissions associated with each role, refer to “8.2.3.1 ROLE-BASED ACCESS” chapter of H49-2.1.0 user manual (H49/EN M/R32).

4.5.4 Local security policies

Local security policies shall be configured:

- Password complexity. Recommended value: enabled
- Password minimum length. Recommended value: 12 or more
- Password expiration period (in months). Recommended value: none.
- Consecutive Login Attempts. Recommended value: 5
- Session’s inactivity timeout (in minutes). Recommended value: 15
- Locking period (in minutes). Recommended value: 1

Refer to following chapters of H49 user manual (H49/EN M/R32):

- “7.5.3.2 USER ACCOUNTS”
- “8.2.4.2 PASSWORD MANAGEMENT”

4.5.5 Central authentication

When a central authentication server is available, H49 product shall be configured to authenticate users against it. This facilitate user management and account revocation, which is mandated by many standards and regulations.

The H49-2.1.0 supports LDAP with STARTTLS to connect to the authentication server.

Refer to “7.5.3.3 LDAP SERVER” chapter of H49-2.1.0 user manual (H49/EN M/R32).

4.6 Configuring security event logging

4.6.1 Local security event logs

H49-2.1.0 firmware logs security events in a text file.

The log file cannot be modified. The file stores up to 512kb data and is circular: when the log file is full, the oldest event is deleted and the newest added.

Local security logging cannot be disabled and there is no need to configure it.

Last local security logs may be consulted from the H49 Status page.

Refer to “7.5.1.1 STATUS” chapter of H49-2.1.0 user manual (H49/EN M/R32).

4.6.2 Central logging

H49-2.1.0 support logging security events to a central syslog server.

GE Vernova recommends forwarding all security logs to a central syslog server to provide a unique view of all system events as well as enforce log long term storage and integrity.

GE Vernova recommends configuring syslog over TLS when supported by the syslog server.

Logging to a syslog server is configured from the Security section of H49.

Refer to “7.5.3.4 SYSLOG SERVER” chapter of H49-2.1.0 user manual (H49/EN M/R32).

4.7 Configuring network Interfaces

4.7.1 Ethernet interfaces

Network interfaces of H49 switch can be enabled, disabled or configured to support different modes.

GE Vernova recommends disabling unused ports.

Refer to “7.5.2.1 INTERFACE” chapter of the H49-2.1.0 user manual (H49/EN M/R32).

4.7.2 VLAN

In order to enforce network segregation and reduce the network attack surface, GE Vernova recommends configuring VLANs on all Ethernet ports.

Refer to “7.5.2.2 VLAN” chapter of H49-2.1.0 user manual (H49/EN M/R32).

5 Maintaining security

Note: This paragraph is the response to IEC62443-4-1 SG-3 requirement.

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

Describe here:

- instructions and recommendations for periodic security maintenance activities;
- instructions for reporting security incidents for the product to the product supplier; and
- description of the security best practices for maintenance and administration of the product.

5.1 Periodic security audits

The configuration applied in Secure installation paragraph shall be recorded.

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

5.2 Backup and restore procedures

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

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

H49 switch provides backup and restore features.

Refer to “7.5.4 BACKUP RESTORE” chapter of the H49-2.1.0 user manual (H49/EN M/R32).

5.3 Vulnerability monitoring and firmware updates

GE Vernova responsibility discloses vulnerabilities found on its products.

User’s shall periodically check for newly published vulnerabilities and available firmware updates and define a security update policy.

https://www.gevernova.com/grid-solutions/automation/critical-infrastructure-communications/reason-h49

All GE Vernova software packages are digitally signed. Digital signature shall be verified before installation.

5.4 Reporting a vulnerability

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

To submit a vulnerability in a GE Vernova product to the GE Vernova PSIRT team, please fill up the form at:

https://www.gevernova.com/security.

Please do not include identifiable sensitive data (e.g. personal data, 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 reporting 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 for the exploit
- If you are aware of any incidents of this vulnerability being exploited on equipment in the field (for example, a GE Vernova customer was directly impacted by this vulnerability)
- 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're representing, or if you'd 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:

- Acknowledgement of receipt of your report within one business day
- During our initial triage of the vulnerability, the GE Vernova Cybersecurity team may reach out to you to do one of the following:
- Request additional information to your initial report
- Communicate our expected triage process and timeline
- 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 as a result of the investigation
- If requested, we will include the reporter’s name in our final report if it results in a public disclosure

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

6 Decommissioning

Note: This paragraph is the response to IEC62443-4-1 SG-4 requirement.

6.1 Secure decommissioning recommendations

GE Vernova recommends preventing unauthorized disclosure of information from the device using an appropriate decommissioning method.

Decommissioning is a complex matter: physical destruction may be forbidden by recycling/waste management laws, filesystem format is ineffective, advanced technical may be conducted offsite introducing supply chain and audit complications.

Hence GE Vernova cannot recommend a decommissioning method.

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

Regarding H49-2.1.0:

- The H49 product can be reset to factory following process in “7.5.2.1.1 REVERT TO DEFAULT FACTORY CONFIGURATION” chapter of the H49-2.1.0 user manual (H49/EN M/R32).
- Information is stored in soldiered flash memory and a removable SD card on the CPU board.
- Passwords are stored locally protected by PBKDF2 with SHA-256 and a unique 64 bits salts to make clear text recovery extremely difficult per today’s standards.

7 Secure operation guidelines

Note: This paragraph is the response to IEC62443-4-1 SG-5 requirement.

For a secure operation of the product, GE Vernova recommends that:

- Users be assigned a specific role at a level sufficient for the tasks they must perform.
- Users don’t share their passwords.
- Users change their passwords when they believe there might a possibility of unwanted disclosure.
- Default account passwords be changed before putting the device in operation.
- Users log out of their session when finished (although an inactivity timeout can be set to automatically terminate user sessions).
- GE Vernova delivered certificates be replaced with certificate provided by the end user.
- The product never be connected to a public network, nor the Internet.
- Only the required services are configured and enabled.
- Transient asset that must be connected to the product be carefully controlled and checked for malware.
- If testing accounts are used during installation, then these accounts be disabled / removed for normal operation.
- Periodical review of all user accounts be performed and inactive accounts be disabled / removed.

8 Appendices

8.1 List of supported protocols

H49-2.1.0 supports the following protocols (as server):

Protocol	Port	Comment
HTTPS	tcp 80, 8080, 8443	Configuration web server
NTP	udp 123	H49 as NTP server
PTP	udp 319, 320	H49 as PTP server
SSH	tcp 22	(Secure) H49 Shell
SNMP	tcp 161	

H49-2.1.0 supports the following protocols (as client):

Protocol	Port	Comment
LDAP with STARTTLS	tcp 389	Central authentication, LDAP with STARTTLS
NTP	udp 123	H49 as NTP client
PTP	udp 319, 320	H49 as PTP client
Syslog	tcp 514	Syslog over TCP
Syslog	tcp 6514	Secure syslog (TCP over TLS)
Syslog	udp 514	Syslog over UDP

8.2 Deterministic output

This is a requirement from IEEE1686 that applies to IED.

In the event of an anomaly, H49-2.1.0 triggers the physical watchdog relay.

Additionally, depending on the type of anomaly, H49-2.1.0 will enter:

- Downgraded mode: affected data will be marked “invalid”
- Fault mode: a restarting loop during which no data is available
- Halt mode: all output relays are de-energized, no data is available, operation is stopped.

8.3 Resource management

This is a requirement from IEEE1686 that applies to IED.

By using the following features, H49-2.1.0 makes sure that security function does not interfere with operations:

- Circular local log file (protect against filesystem over usage)
- Dedicated Ethernet management interface
- Capability to disable front panel authentication
- Redundancy support, to upgrade one IED’s firmware while the backup IED is in charge of operations.

8.4 IEC62443-4-1 mapping

SG-1 Product defense in depth	2 Product Defense-in-Depth strategy
SG-2 Defense in depth measures expected in the environment	3 Environment
SG-3 Security hardening guidelines	4 Secure Installation - Hardening 5 Maintaining security
SG-4 Secure disposal guidelines	6 Decommissioning
SG-5 Secure operation guidelines	7 Secure operation guidelines
SG-6 Account management guidelines	4.5 User access control
SG-7 Documentation review	Covered by GE Vernova NPI process and quality processes.