DEPLOYMENT GUIDELINE

FOXMAN-UN

Cybersecurity Deployment Guideline

Document ID	1KHD651697-R18	
Document edition	FOXMAN-UN System Release:	R18
	Revision:	A
	Date:	2025-09-24

Copyright and confidentiality

Disclaimer

This document contains information about one or more Hitachi Energy products and may include a description of or a reference to one or more standards that may be generally relevant to the Hitachi Energy products. The presence of any such description of a standard or reference to a standard is not a representation that all the Hitachi Energy products referenced in this document support all the features of the described or referenced standard. In order to determine the specific features supported by a particular Hitachi Energy product, the reader should consult the product specifications for that Hitachi Energy product. In no event shall Hitachi Energy be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, nor shall Hitachi Energy be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.

Hitachi Energy may have one or more patents or pending patent applications protecting the intellectual property in the Hitachi Energy products described in this document. The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy assumes no responsibility for any errors that may appear in this document.

All people responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including compliance with any applicable safety or other operational requirements. Any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.

The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

Hitachi Energy performs functionality testing on released products and updates. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed. Hitachi Energy and its affiliates are not liable for damages and/or losses related to security breaches, any unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

This document and parts thereof must not be reproduced or copied without written permission from Hitachi Energy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

Contents

1 Introduction

1.1 Purpose of this Document

This document forms an important part of the overall user documentation for FOXMAN-UN (further called 'Product'). It provides an overview about essential cybersecurity aspects and gives strong recommendations about hardening the Product in the context of the communication infrastructure it is used for.

The guideline intends to support system engineers being responsible for the installation, testing, upgrading or maintenance of the Product with information related to cybersecurity. A general familiarity with topics in the following areas is expected:

- OS cybersecurity hardening (CIS profiles),
- Role-based access control (RBAC),
- PCs, servers, and LINUX and Windows® operating systems,
- Networking, including TCP/IP and concept of ports and services,
- Security policies,
- Firewalls,
- Anti-malware and intrusion detection,
- Application whitelisting,
- Remote and secure communication.

1.2 Basic Cybersecurity Considerations

The important thing about security is to understand that security is a chain consisting of many components. Which components to implement in the network depends on both which security threats to address and what is considered the correct and balanced level of security for the network.

Physical security and upholding processes that support the organization's security policies are perhaps the most important parts of the network security. Also important is the authorization of users, logging, firewalls, hardening of unused ports and the use of secure protocols.

Dependence between different security measures needs to be considered to get the most implemented action. For example, to get the most out of audit logging you are depending on good authorization and the opposite is also true.

Security in a network also depends on the security of its constituent nodes. Remember that the overall security of a network equals the security of the weakest node.

1.3 A Formalized Security Model

Security is a process, not a static state. It is typically not possible to achieve security objectives through the use of a single countermeasure or technique. It involves the continuous application of fit-for-purpose, cost-effective mechanisms throughout the system lifecycle. A defense-in-depth strategy is essential to mitigate threats effectively.

To ensure adequate security, it is necessary to model and understand the communication infrastructure and assess potential threats to these assets. The IEC 62443 series of standards, particularly its foundational requirements (FRs) – such as Identification and Authentication Control, Use Control, System Integrity, Data Confidentiality, Restricted Data Flow, Timely Response to Events, and Resource Availability – provide a structured and comprehensive framework for capturing relevant security considerations across different system dimensions.

All information and recommendations provided in this Deployment Guideline address one or more of these foundational requirements and aim to harden the device within the broader network context.

1.3.1 Security Policies and Principles

Security policy is a set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

Principles are decisions, rules or good practices that are applied when designing systems or networks. Hitachi Energy solutions use certain specific security principles and best practices as a basis for providing network protection.

One important principle is the “defense in depth” which calls for employment of security mechanisms in layers.

1.3.2 Security Services

Security service is a fundamental concept in all security architectures. The service meets the security objectives identified by the threat-and-risk analysis. Security services are implemented by means of security functions and mechanisms. A confidentiality security service, for example, might be implemented using SNMPv3 with privacy protocol enabled. This, in turn, makes use of encryption mechanisms. The most important security services, according to the IEC 62443 series of standards, are the following:

- **Access Control (AC):**

  Control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.
- **Use Control (UC):**

  Control use of selected devices, information or both to protect against unauthorized operation of the device or use of information.
- **Data Integrity (DI):**

  Ensure the integrity of data on selected communication channels to protect against unauthorized changes.
- **Data Confidentiality (DC):**

  Ensure the confidentiality of data on selected communication channels to protect against eavesdropping.
- **Restrict Data Flow (RDF):**

  Restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.
- **Timely Response to Event (TRE):**

  Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission-critical or safety-critical situations.
- **Resource Availability (RA):**

  Ensure the availability of all network resources to protect against denial of service attacks.

2 Network Design

This section gives context and background information on the possible steps and measures taken to make best use of the security and hardening functions of the Product. The Product – a Network Management System (NMS) – is a software consisting of Database, Server, and Client components.

2.1 Network Design

For the network design basics refer to the application note [1KHW029209] Application Note – FOXMAN-UN Server Setup in a Secure Network published on Hitachi Energy Publisher via https://publisher.hitachienergy.com (registration required).

2.1.1 Zones

Network segmentation into security zones is a measure to minimize the impact when one zone is compromised. The security level of one zone can be different from another zone. In case zones shall be introduced either at the initial project design or as a later extension is not the topic of this document, however the example is meant to clarify the concept and highlight possible options.

Possible zones in a typical NMS implementation are:

- The Management Control Network (MCN);
- The regions of the MCN, if there is regional partitioning;
- The NMS Interconnection Network (NIN);
- The internal company network;
- The Internet.

Note that not all zones are always present. In the case of an NMS consisting of a single server, exclusively connected to the MCN, there is only the MCN zone. In this case, protection might be limited to physical access protection and the use of proper passwords.

Added standby servers (see [1KHW029097] User Manual – FOXMAN-UN Main/Standby Solution) and/or client computers are often interconnected using a separate IP network. This NMS Interconnection Network (NIN) creates a second security zone, which blocks direct access to the MCN from the client computers. Clients can only access the MCN through the NMS applications. As the NMS server does not route traffic between MCN and NIN no direct access to the MCN is possible. Other zones may be assigned within the MCN itself. Regional responsibilities in a large network can be one reason; the use of third party communication services another. Regional responsibilities may require the addition of external router and the use of IP address based access control lists. This is to allow the central NMS servers to access all network devices the regional network Devices are however not able to connect to devices in other regions. To facilitate such configuration, it is good practice to assign distinct IP address ranges to each region from the very beginning of a project.

The use of third party communication services may prompt the use of encryption on the corresponding network connection.

More critical security issues may arise from an NMS that is directly connected to the internal company network in turn connected to the Internet. The use of firewalls is a strong requirement in this case. In addition, IP based access control lists and role based access control should be used.

The picture below highlights the discussed zones in different colors.

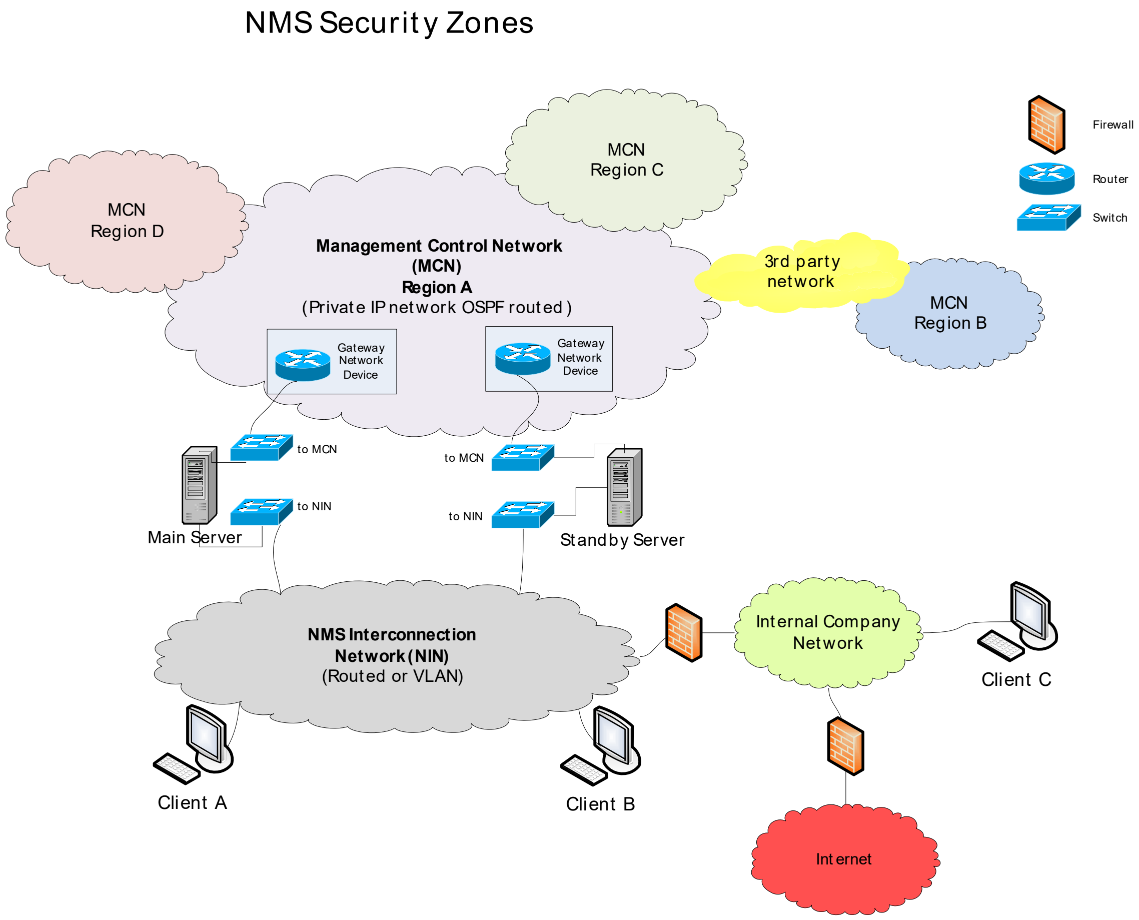

Figure 1: NMS Security Zones

2.1.2 Possible External Communication (including Remote Access)

As discussed above, our Product operates in isolation, almost exclusively without any connection to an external system. Modems being used until a few years ago are now replaced by solutions using the Internet. Most companies have their established security rules and established remote access solutions to access the Internal Corporate Network from the Internet; therefore, the implementation of a remote access requires close cooperation with the customer.

Below three types of remote access are discussed which are examples for possible implementation only. Other possible solutions are available but are within the responsibility of the customer.

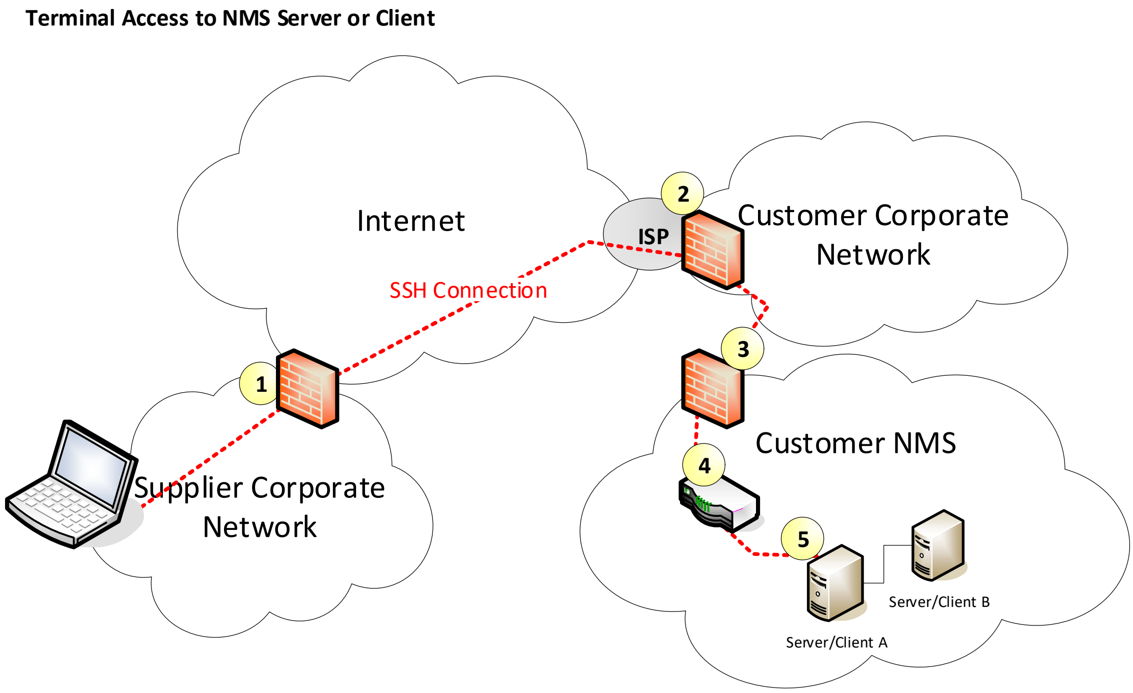
Terminal Access to NMS Server or Client
Internet
SSH Connection
ISP
2
Customer Corporate Network
1
3
Customer NMS
4
Supplier Corporate Network
5
Server/Client B
Server/Client A

Figure 2: Remote Terminal Access using SSH through Customer Corporate Network Firewall

The remote access using the SSH protocol provides access to a character based terminal port on the target system, e.g. the NMS Server. To access the graphic console, it is possible to use one additional TCP channel embedded in the SSH protocol. This channel can be used to interconnect one additional program pair on both ends of the link. This program pair typically provides access to the graphical console using Client/Server based solutions such as X11 or VNC. The interconnected Computers can in addition exchange files using the SFTP protocol.

This solution requires one in-bound port (default port number is 22) to be opened at firewall 2 and 3. Device 4 is a switch or can represent the internal layer 2 infrastructure consisting of a hierarchy of switches. Allowed traffic should be restricted to start at a specific IP or IP range, e.g. from the Hitachi Energy Corporate Network, and terminate at the target machine only. As it is impractical to enable and disable the configurations of the firewalls per each individual remote access, firewalls will be set-up once and remain. However, as an additional security measure the customer can switch on and off the Ethernet Connection at point 4. This will allow the customer to control the remote access to the NMS and corresponds to switching on and off the modem in the earlier solutions.

The next picture shows an Hitachi Energy solution for the provision of a secure remote access through a mobile provider's network via the Internet to an Hitachi Energy server. The small access box takes care of running the SSH protocol and includes a firewall and other security features. The advantage of this solution, it is secure and very easy to use. No access to the Internet through the customer corporate network is required and no configuration is required on the customers NMS client computer. The only requirement is a free LAN interface on the target computer and access to a wireless 3G/4G/5G network.

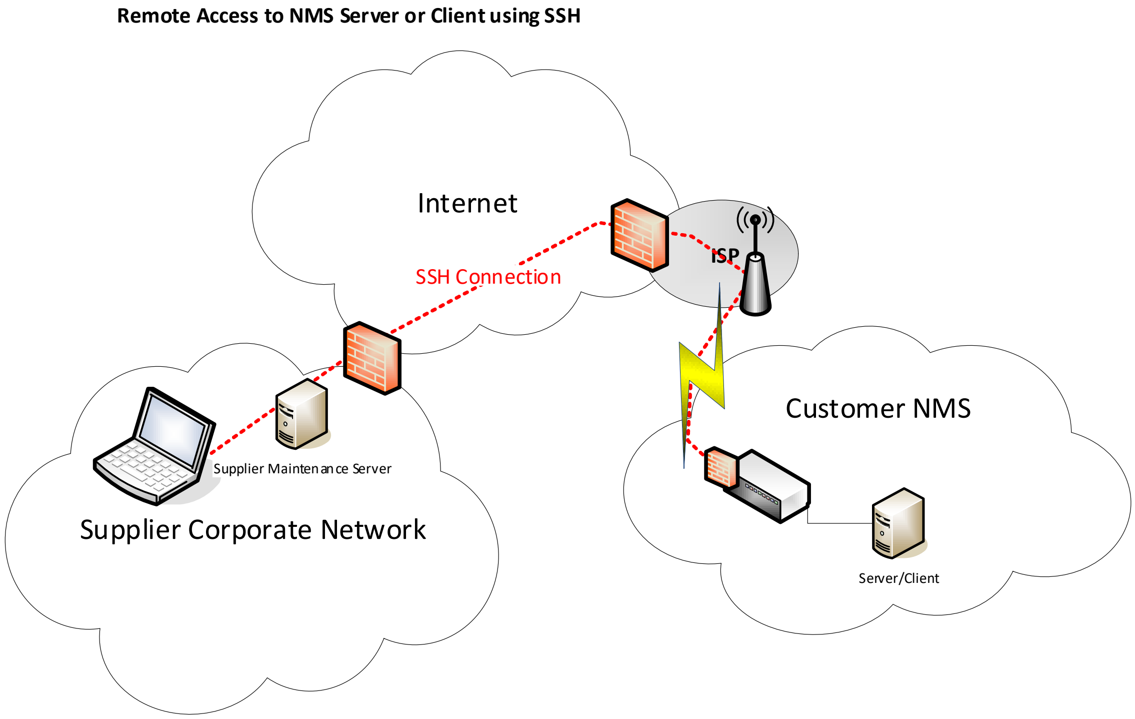
Remote Access to NMS Server or Client using SSH
Internet
SSH Connection
ISP
Customer NMS
Supplier Maintenance Server
Supplier Corporate Network
Server/Client

Figure 3: Remote Access using SSH secured through dedicated hardware (access box)

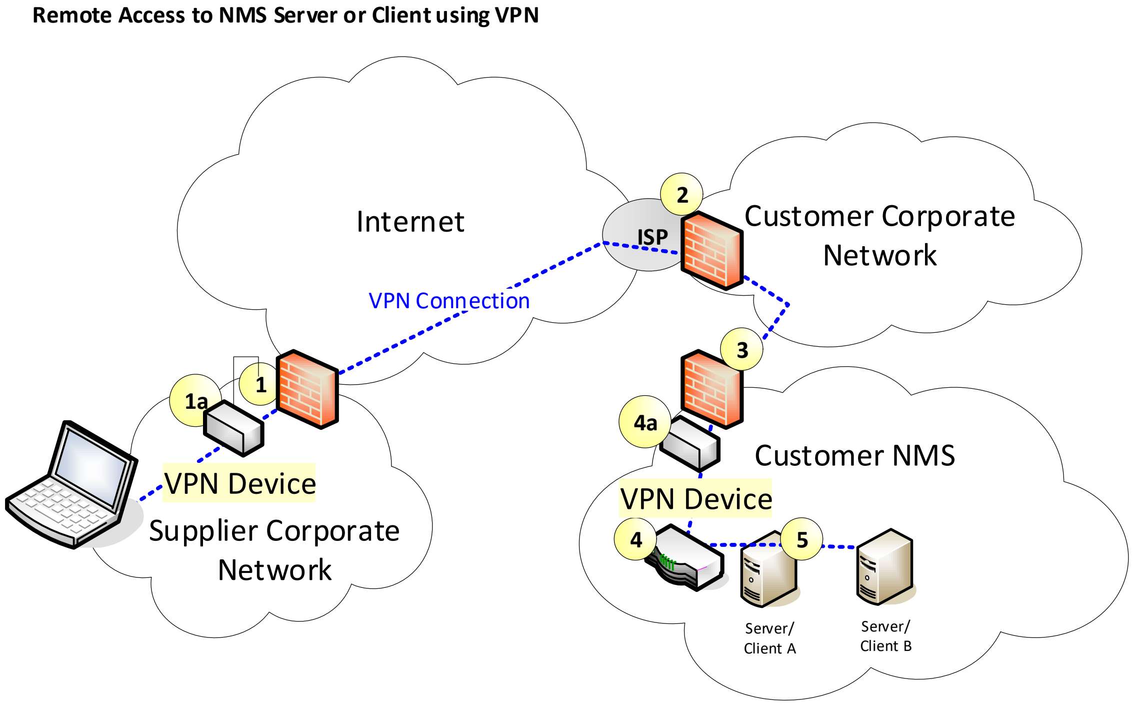
Remote Access to NMS Server or Client using VPN
Internet
2
ISP
Customer Corporate Network
VPN Connection
3
1a
1
4a
Customer NMS
VPN Device
Supplier Corporate Network
VPN Device
4
5
Server/ Client A
Server/ Client B

Figure 4: Remote access using VPN

This solution is similar to a solution using SSH in the way that it also requires opening a TCP port in the firewalls. Several VPN protocols can be used e.g. OpenVPN and IPsec. The VPN software can run on a dedicated hardware or directly on the communicating devices. The protocol supports authentication and encryption. The difference to the first solution is that access is granted not to a specific computer but to a remote IP network, e.g. the NMS Interconnection LAN. The remote computer could therefore install NMS Client software and be used as an NMS operator workplace. Again, remote access could be switched on and off at point 4 – a specific port of a switch belonging to the NMS Interconnection Network.

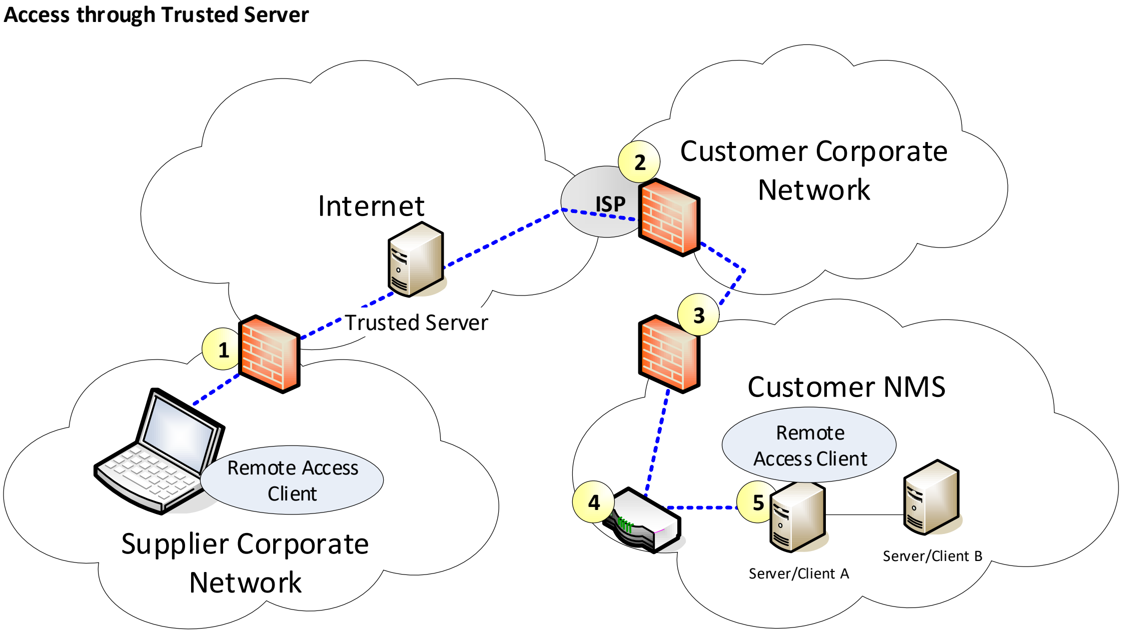

Figure 5: Access through Trusted Server

To establish a remote connection each side needs connecting to a special server. This server then joins the two sides. There are specialized companies offering such servers. This solution allows taking over the screen, keyboard, and mouse of a remote computer and supports the upload and download of files.

The advantage is that connections must be initiated from the target computer, i.e. the customer, who is in full control of the access and can watch the screen while the remote supporter works on his system. Another advantage is that it is not required to open an incoming TCP port in the customers firewall. A standard outgoing HTTP port is all that is required. The firewall at point 3 will block all incoming traffic to the customer NMS. A common solution is to connect a dedicated LAN port to the company's Corporate Network and use the firewall from the Server Operating System to block incoming traffic. In case of a need for remote access the operator will enable this dedicated LAN port; otherwise it stays disabled.

2.2 Network Elements (NE)

For FOX61x NE related security deployment guidelines refer to [1KHW028641] FOX61x Cybersecurity Deployment Guideline published on Hitachi Energy Publisher via https://publisher.hitachienergy.com (registration required).

When connecting the FOX61x NEs with NE authentication enabled using fingerprint, a finger print verification can be done to make sure the fingerprint used to connect to the NE is correct. If the fingerprint configured in the NMS differs from the fingerprint provided by the NE, the client will warn the operator via a security alert. Such an alert may indicate that a man-in-the-middle attack is being carried out.

2.3 Hosts

Hosts in the context of this document are the computers on which the NMS server and/or client software resides. This section addresses issues and measures that are generic and apply to the operating system used on the host. In the next section, additional recommendations are given to secure the NMS software (the applications / services of the Product) using additional built in feature such as a second level of user management and additional logging facilities.

2.3.1 User accounts

As a default, e.g. during factory acceptance, two default accounts are set-up on the server. The administration account for the LINUX Operating System (OS) and an account to administrate the NMS server software. For pure client computers set-up on a Windows® OS it is also possible to use the Windows® administration account for both purposes.

User accounts should then be added on an individual basis. It is recommended to use Active Directory for user account creation and management. Also refer to [1KHW029190] Application Note – FOXMAN-UN Integration with Active Directory (AD).

It is highly recommended that the customer changes the passwords provided by Hitachi Energy to their own strong password. Responsibility for the passwords is with the customer, Hitachi Energy has no means to reset the password. For requirements on passwords refer to [1KHW029185] FOXMAN-UN R18 RHEL9 CIS Hardened Installation or later versions of that document.

NOTICE **Non-observance could result in equipment damage.**
Non-observance of security measures conceals security risks. Therefore:

→ Enforce password change defining a lifespan and a password cycle through the facilities of the OS.

→ Use administrator accounts for installation and maintenance only.

→ Create operator accounts with minimal required privileges.

→ Password must meet “strong password” definition as defined by the customer policy.

→ Remove unused accounts.

2.3.2 Services

Some specific services may be required by the Product in order to operate correctly.

NOTICE **Non-observance could result in equipment damage.**
Non-observance of security measures conceals security risks. Therefore:

→ Install only the services required by the Product.

2.3.3 Patches

During factory installation, the latest available OS and Product patches are applied. Most systems operate in isolation with no connection to any other network. Hitachi Energy recommends a service contract to upgrade the Product in regular intervals. Advertised recommended Product patches can be downloaded from the Utility Communication Web site or from the Hitachi Energy Publisher via https://publisher.hitachienergy.com (registration required).

2.3.4 Host based Firewall

Hosts that use an additional LAN interface to enable remote access shall enable the internal firewall on this interface. Only the ports and protocols required for the remote access shall be permitted. If possible, the source and destination address of packets should also be restricted. More information on firewall settings can be found in a specific application note specific to this subject.

NOTICE **Attention to access control. Risk of equipment damage!**

Non-observance of security measures conceals security risks. Therefore:

→ Deny inbound connections by default.

→ Document all firewall rules clearly.

→ Configure the firewall to log blocked traffic.

2.3.5 Physical access / device lock down

Connecting physical media to a computer bears a great risk of e.g. virus infection. Disabling physical connections also prevents unauthorized persons from installing any software on the system.

If a computer is placed outside a locked system cabinet all physical interface units giving access to file transfer, e.g. USB, serial and parallel ports, floppy and CD drives, should be disabled.

Setting the PC BIOS/UEFI to enable Chassis Intrusion Detection will generate a log entry that the PC-chassis has been opened.

2.3.6 BIOS/UEFI and boot configuration

The BIOS/UEFI configuration is vital to the correct functioning and to the security posture of a system. Enabling or disabling devices for instance can have a big impact on a system. Security mechanisms provided by the operating system (e.g. file access permissions) can be circumvented by loading a different operating system, e.g. by booting from CD.

If physical access to the system by unauthorized persons is a concern, the BIOS/UEFI shall be protected by at least a strong password.

Multiple operating systems or copies thereof shall not be installed on the same computer.

NOTICE **Attention to access control. Risk of equipment damage!**

Non-observance of security measures conceals security risks. Therefore:

→ Protect access to the BIOS/UEFI with a strong password.

→ Disable booting from floppy, CD-ROM or USB sticks.

2.3.7 Appropriate use banners

Appropriate use banners are needed to prevent authorized users to elevate their privileges unintentionally. They are also needed for legal purposes.

NOTICE **Attention to access control. Risk of equipment damage!**

Non-observance of security measures conceals security risks. Therefore:

→ Configure the server to display an appropriate use banner upon user login on the NEM Client. To do so, refer to [1KHW002414] User Manual – FOXMAN-UN under Linux, section “legalMessages.json (NEM login banner)”.

2.3.8 Backup / Recovery

Accurate backups are needed to be able to recover a system after an incident quickly. An incident might e.g. be a security attack or an unintentional misconfiguration that cannot be undone. They might also be useful to prove the state of a system upon delivery.

2.3.9 Anti Malware

For Microsoft Windows® based hosts, the initial Software Installation when done by Hitachi Energy may include, depending on the contractual agreements, anti-malware software, e.g. Microsoft Defender. After hand-over the customer is responsible for updating or replacing the anti-malware protection. As most of the systems are never connected to external systems the threat is limited to infections from connected external devices such as memory sticks. Therefore, as an alternative or as an additional protection, USB ports can be disabled or only used for upgrades with dedicated scanned memory sticks.

For Linux based hosts running the Product core, Hitachi Energy does not install any anti-malware software as there are less user interactions and hence less attack surfaces.

See also section 3.1.7 "Virus Scanner".

2.3.10 User Groups

NMS User accounts shall be created without administrator rights, belonging to the Standard Users group, therefore preventing them from making accidental or intentional system wide changes.

On Windows® Systems the Default Windows® “Guest” accounts should be disabled, and the Administrator account renamed. Also see 3.2 "Windows® Security Recommendation".

For Linux based Systems the correct group permissions are automatically set, see section 3.1 "LINUX Security Recommendation".

2.3.11 File System

Our Windows® installations use the NT files system (NTFS) on all disks and partitions to support Access Control Lists (ACLs) which afford a higher level of protection to the operating system and its data. NTFS also allows for the auditing of access to files and folders contained in the file system.

2.3.12 Network shares

The Product does not use the LINUX Network File System (NFS) or Windows® shares in its default configuration. If such shares shall be created to e.g. share data with other computers, limit access rights and visibility of such shares to authorized hosts/users only.

2.4 Applications / Services

Install the Product on a clean OS precisely following the Installation Instructions. This will ensure that only the services and applications required for the proper operation of the NMS will be available. Do not use the same machine to install any additional service or application. For additional information on how to harden the Product after using the standard installation procedure, see section 3 "Product Related Details".

2.5 Physical Security

Planning and implementing physical security is in the responsibility of the end-customer. The following guidelines should be considered.

Obviously, any plant site has a defined boundary as well as entry points on roadways that are typically managed by fences, barriers and guardhouses. There are also areas inside the facility that require additional physical security due to the critical content contained within.

A key element in maintaining physical security is the identification of the Physical Security Perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical assets reside and all access points. Some control system assets may be classified as critical assets such as controller cabinets, operator and engineering workstations, servers, network components and communication equipment and data highways. Security for critical assets can be provided for with differing approaches such as:

- Card key
  A means of electronic access where the access rights of the card holder are pre-defined in a computer database. Access rights may differ from one perimeter to another.
- Special locks
  These may include locks with non-reproducible keys, magnetic locks that must opened remotely.
- Security officer personnel
  Responsible for controlling physical access 24 hours a day. These personnel would reside on-site or at a central monitoring station.
- Security enclosure
  A cage/safe/cabinet system that controls physical access to the critical asset (for environments where the nearest six-wall perimeter cannot be secured).
- Other authentication devices
  Biometric, keypad, token, or other devices that are used to control access to a critical asset through personnel authentication.

As a minimum, Hitachi Energy suggests that all control cabinets and enclosures be with unique keys and that the keys are controlled by senior personnel. Protection maybe afforded by the use of door switches that generate a security alarm.

In addition to defining critical assets and implementing a method of controlling access to said assets, a program that actually monitors and logs the physical access enhances physical security. If access is being controlled electronically by card keys, biometrics or keypads, the controlling system should be able to alert security services that unauthorized access is being attempted as well as log all activity. Other approaches may include CCTV, alarm contacts or manual log books on controlled access areas.

Organizations should realize that security is an on-going process not a one-time installation task. Therefore, documentation identifying the access control(s) implemented for all physical access points should be maintained. The documentation should also identify any request for access (its reasons and duration), authorization, and revocation process implemented for each access control system. Individuals, assigned access to critical assets, should be receiving training on a regular interval and periodically reviewed to determine if continued access is necessary. Finally, a process for verification and testing of access controls, monitor and alarms should be in place to ensure they are functioning properly.

- **Access control and monitoring**
  - Monitor access to rooms.
  - Evaluate access logs to rooms with critical equipment regularly.
- **Site**
  - Secure access to the site by a fence or a wall.
  - Visitors should only be granted access after identification by a security guard / reception at the border of the site.
- **Buildings**
  - Restrict access to buildings to authorized personnel.
  - Visitors accessing the building must be under supervision of an authorized personnel member.
- **Rooms**
  - Restrict access to rooms to authorized personnel.
  - Visitors accessing the room must be under supervision of an authorized personnel member.
- **Cabinets**
  - Restrict access to cabinets to authorized personnel.
  - Locate cabinets in restricted rooms, equipped with locks with unique keys.

  - Visitor accessing the cabinet must be under supervision of an authorized personnel member.
- **Servers / Workstations**
  - Place servers and workstations in a closed cabinet in a room with restricted access.
  - Allow access to USB-ports and DVD drives only through personally owned administrator accounts.
  - After usage of such devices authorized administrators will be responsible to set them back to disabled state.
- **Network equipment**
  - Place all devices, which have no own keyboard or monitor, e.g. a controller, in cabinets with unique keys, in restricted rooms.
- **Network cabling**

  LAN connections can be accomplished in several ways:
  - Copper (CAT5/5E/6/7),
  - Fiber Optic,
  - Wireless.

  Copper can be easily tapped if it can be physically accessed.

  Wireless is easy to pick up and there is basically no physically way to protect it unless it is used within an electromagnetic shielded room or building. It is therefore recommended not to use wireless in any location.
  Fiber cables are more difficult to tap and cannot be picked up in the air.
- **LAN connections within a building**

  For LAN connections within a secure building both copper and fibers can be used.
- **LAN connections between buildings**

  Fibers should be used for LAN connections between buildings.
- **WAN connections between sites**

  Connections between sites using WAN cannot be physically protected and must therefore be protected by the use of encryption and/or an access filter, e.g. a firewall.

2.6 Documentation

For each NMS project, the Product’s Factory Acceptance Test (FAT) procedure should be carefully followed. The FAT protocol includes references to project specific documents if available. For more complex systems this project specific documentation usually includes the MCN/NIN network topology and configuration data such as the IP address plan and OSPF areas if implemented.

The FAT protocol also documents version and patches of the installed software including project specific configurations such as configured options and created user accounts. A checklist is included which demands the execution of basic system tests and the creation of backups. Backups include the configuration files of the managed devices, a backup of the NMS database and a complete snapshot of the NMS computer’s hard disk to be used for a system recovery should it be necessary.

3 Product Related Details

This section gives examples of requirements or actual steps to take. As the configuration of this NMS Product closely relates to the setup of the corresponding managed devices, it is also useful to consult their Deployment Guidelines.

The Product installs on the REDHAT LINUX Operating System, and this guide assumes the following:

- The used LINUX OS major version is as defined in the Products Release Notes.
- The Product software is at the latest Hitachi Energy verified patch level.
- The server does not control Uninterruptable Power Sources (UPS).
- Hitachi Energy does not recommend that domains and wireless networks are used.

i

Please note:
The Product Installer does not automatically configure security settings such as firewall, security policies or disables system services. Check the recommendations given below and if applicable configure manually.

3.1 LINUX Security Recommendation

The Product requires the use of a Linux Operating System (OS). It is verified and supported solely under RedHat Enterprise Linux. The matching OS version for a specific Product Release is documented in the Product's Release Notes. This section describes available security options to be implemented on the OS level.

It is however recommended to apply the CIS hardening profile to the Linux OS on the server where the Product services are installed and will be running.

The description on how to apply the CIS profile to the Linux OS can be found in [1KHW029185] FOXMAN-UN R18 RHEL9 CIS Hardened Installation (or a later version, as applicable to the current Product version) published on Hitachi Energy Publisher via:
https://publisher.hitachienergy.com.

Further detailed OS version specific configuration instructions can easily be looked up in the extensive RedHat Enterprise Linux documentation, e.g. in the Security Guide, which can be downloaded from the Internet. Frequently used settings or recommended security defaults may also be documented in the Products installation instructions or FAT procedure.

Here is a list of security relevant "Things to consider" taken from the above-mentioned Linux Security Guide. They reflect the reasoning behind the recommendations given in this section.

- BIOS/UEFI and boot loader security
  Can an unauthorized user physically access the machine and boot into single user or rescue mode without a password?
- Security-Enhanced Linux (SELinux)
  A mechanism that is implementing security policies for access control, including mandatory access control (MAC).
- Password security
  How secure are the user account passwords on the machine?
- Administrative controls
  Who has an account on the system and how much administrative control do they have?
- Available network services
  What services are listening for requests from the network and should they be running at all?
- Personal firewalls
  What type of firewall, if any, is necessary?
- Security enhanced communication tools
  Which tools should be used to communicate between workstations and which should be avoided?
- Keep all services current, to protect against the latest threats.

- Use secure protocols whenever possible.
- Monitor all servers carefully for suspicious activity.

3.1.1 BIOS/UEFI and Bootloader Passwords

If an intruder has access to the BIOS/UEFI, they can boot into rescue or single user mode, which in turn allows them to start arbitrary processes on the system or copy sensitive data.

Therefore, if unauthorized persons may gain physical access to your machine

→ Enable BIOS/UEFI passwords.

The system uses the GRUB boot loaded which can be accesses during startup. The boot loader interface also allows a user to boot into unprotected single user mode. To prevent this

→ Password protect the Linux boot loader.

3.1.2 Enable SELinux

Security-Enhanced Linux is preventing any access that is not allowed via security policies when in enforcing mode. We recommend to set SELinux to “enforcing”, and set the policy type to “targeted”.

After Linux installation this is usually the default. If this is not the case, to set this mode edit the file “/etc/selinux/config” as root user and make sure the following entries are present and uncommented:

```
SELINUX=enforcing
SELINUXTYPE=targeted
```

3.1.3 Require Authentication for Single User

Single-user mode is intended as a system recovery method, providing a single user root access to the system by providing a boot option at startup. By default, no authentication is performed if single-user mode is selected. This provides a trivial mechanism of bypassing security on the machine and gaining root access.

To require entry of the root password even if the system is started in single-user mode, add the following line to the /etc/inittab file:

~:S:wait:/sbin/sulogin

3.1.4 Disable Interactive Boot

Edit the file /etc/sysconfig/init. Add or correct the setting:

```
PROMPT=no
```

The PROMPT option allows the console user to perform an interactive system startup, in which it is possible to select the set of services which are started on boot. Using interactive boot, the console user could disable auditing, firewalls, or other services, weakening system security.

3.1.5 OS Patch Management

All software contains bugs. Often, these bugs can result in a vulnerability that can expose your system to malicious users. Unpatched systems are a common cause of computer intrusions. You should have a plan to install security patches in a timely manner to close those vulnerabilities, so they cannot be exploited.

However if your system is not connected to the Internet the risks for attacks is rather low. OS upgrades can then be planned in sync with the recommended Product updates/upgrades.

3.1.6 Removing Unused Programs

It is a recommended practice to install only the packages you will use because each piece of software on your computer could possibly contain a vulnerability.

→ Remove unused programs or services from your system.

3.1.7 Virus Scanner

Anti-malware software is highly recommended to prevent the execution of unknown, potentially malicious software on a Linux machine.

3.1.8 Enforcing Read-only Mounting of Removable Media

This is an option to prevent that users can execute programs, e.g. software installers, scripts directly from the plugged-in media. If this is configured the administrator must either copy to a local disk or remount an inserted DVD before he can run a Product upgrade script on this media.

3.1.9 Configurable Logon/Warning Banner

The computer must present a warning banner for authorized and unauthorized users at all access points.

This is needed for successfully prosecuting unauthorized users who use the computer improperly. For more information on how to configure a banner, see the Product's installation procedure. A banner can be implemented for the text console (TTY) and the GUI.

3.1.10 Password Security

Passwords are the primary method that Red Hat Enterprise Linux uses to verify a user's identity. This is why password security is so important for protection of the user, the workstation and the network. The single most important thing a user can do to protect his account against a password cracking attack is create a strong password. In Red Hat Enterprise Linux, the pam_cracklib module – Pluggable Authentication Modules (PAM) – can be used to check a password's strength against a set of rules. It can be stacked alongside other PAM modules to configure a custom set of rules for user login. Examples of available options are

- Password aging,
- Locking inactive accounts,
- Access control based on login names, host or domain names, or IP addresses,
- Time based access,
- Applying account limits.

The use of screen savers with automatic screen locking is recommended if the Product is not used in a physically secured control room but in the general office environment.

3.1.11 Administrative Controls

The use of the Linux Administration account (the root user) should be restricted to trusted users only. Through a PAM module called pam_console.so, some activities normally reserved only for the root user, such as rebooting and mounting removable media are allowed for the first user that logs in at the physical console.

Other important system administration tasks, such as altering network settings or mounting network devices, are not possible without administrative privileges. As a result, system administrators must decide how much access the users on their network should receive. It is also possible to deny root access through remote access using the SSH protocol.

3.1.12 Insecure Services

For a list of services to be configured, please consult the Product's installation manual. On a standard installation of the current RedHat Releases the older insecure remote access tools e.g. Telnet, RCP and FTP are disabled by default and have been replaced by

- SSH
  a secure remote console access client,
- SCP
  a secure remote copy command,
- SFTP
  a secure pseudo-FTP client that allows interactive file transfer sessions.

3.1.13 Firewall (Ports and Services)

For most users, the best tool for configuring a simple firewall is the graphical firewall configuration tool which ships with Red Hat Enterprise Linux, the Firewall Configuration Tool (system-config-firewall). This tool creates broad iptables rules for a general-purpose firewall using a control panel interface. For advanced users and server administrators, manually configuring a firewall with iptables is preferable. The incoming ports which need to be opened to accept a remote client login are the ports of the ALS server as set in the ALS Configurator, the ports used by the CORBA protocol, and the ports used by the REST based services.

CORBA listens on one static port and many dynamically created ports. The default of the static TCP port is 2809 as defined in the file omni.cfg. The range of the dynamic ports can be restricted in the file firewall.conf. The dynamic ports are opened by the software processes creating CORBA objects as they exchange information. Without specifying port ranges in the firewall.conf file a firewall cannot be used as all ports needed to remain open.

On the remote client side either Windows® or LINUX the ports used by the ASR (defined in the ALS Configurator) need to be opened as well. The CORBA ports are defined in the files omni.cfg and firewall.conf which are available in both Operating Systems. For more details and the file locations refer to the Product's installation document. For more details on firewall settings refer to the [1KHW028766] Application Note – FOXMAN-UN in Firewalled Environment.

3.1.14 Logging and Auditing

For basics on logging to a syslog server see [1KHW028929] Application Note – FOXMAN-UN Usage of Syslog.

Successful local or network attacks on systems do not necessarily leave clear evidence of what happened. It is necessary to build a configuration in advance that collects this evidence, both in order to determine that something anomalous has occurred, and in order to respond appropriately. In addition, a well-configured logging and audit infrastructure will show evidence of any misconfiguration which might leave the system vulnerable to attack.

Logging and auditing take different approaches to collecting data. A logging infrastructure provides a framework for individual programs running on the system to report whatever events are considered interesting: the sshd program may report each successful or failed login attempt, while the sendmail program may report each time it sends an e-mail on behalf of a local or remote user. An auditing infrastructure, on the other hand, reports each instance of certain low-level events, such as entry to the setuid system call, regardless of which program caused the event to occur.

Auditing has the advantage of being more comprehensive, but the disadvantage of reporting a large amount of information, most of which is uninteresting. Logging (particularly using a standard framework like syslogd) has the advantage of being compatible with a wide variety of client applications, and of reporting only information considered important by each application, but the disadvantage that the information reported is not consistent between applications.

A robust infrastructure will perform both logging and auditing, and will use configurable automated methods of summarizing the reported data, so that system administrators can remove or compress reports of events known to be uninteresting in favor of alert monitoring for events known to be interesting.

Red Hat Enterprise Linux provides rsyslog, with logwatch providing summarization, and auditd should be used for auditing, with aureport providing summarization.

3.2 Windows® Security Recommendation

The Product supports the installation of the Client software under the Windows® Operating System. Such a Windows® Client could be set-up on a dedicated computer to be used as a permanent NMS console, it could be set-up on a maintenance laptop or on a company maintained Office PC. Dependent on these different usages the ownership and security responsibility for the Product may not coincide with the responsibility for the maintenance of the Hardware and the Windows® Operating System. Different departments with different security policies may be involved. In such a situation it is not uncommon to end up with a system which is either not fully functional or has relaxed security requirements. This section states measures which should be carefully considered.

3.2.1 BIOS/UEFI Settings

- Enable passwords
- Remote wake-up/Wake on LAN is disabled.

3.2.2 Data Execution Prevention (DEP)

Data Execution Prevention (DEP) is a security feature that can help prevent damage to the user's computer from viruses and other security threats. DEP can help protect the user's computer by monitoring that different programs use the system memory safely. If a program tries to execute code from the memory in an incorrect way, DEP closes the program. DEP automatically monitors the essential Windows® programs and services.

The default configuration of the operating system is used.

3.2.3 Removing Unused Programs

Some Windows® Components are not used by the Product and can be manually removed.

3.2.4 Windows® Updates/Patch Management

There are nine update classifications defined by Microsoft. These include, for example, critical updates, drivers, security updates, and service packs. The Product is regularly tested with the latest Microsoft security updates and service packs. In general, it is recommended to install all Windows® updates.

3.2.5 Virus Scanner

Anti-virus software is highly recommended to prevent the execution of unknown software on a machine (for example, due to enabling of removable devices or USB ports).

Virus scanners distinguish between on-access scanning (only files that are currently requested to load are checked) and on-demand scanning (all files are checked during a scheduled scan). The minimum requirements for the virus scanner are on-demand scanning and virus definition updating features.

On-access virus scanners on servers are a trade-off between security and performance. We recommend that the performance of the system is tested with normal virus scanner settings.

3.2.6 Disabling Devices

In general, it is a good practice to disable any unused devices in your system. This may include USB ports, CD/DVD drives or communication ports.

If it is not possible to disable a device, it is good to disable the autorun functionality of the device. To prevent the automatic start of malicious code contained in a removable device, the autorun functionality must be disabled. For more information, see the Product's Installation Procedure.

3.2.7 Configurable Logon/Warning Banner

The computer must present a warning banner for authorized and unauthorized users at all access points.

This is needed for successfully prosecuting unauthorized users who use the computer improperly. For more information on how to configure a banner, see the Product's Installation Procedure.

3.2.8 User Account Control (UAC)

UAC is a security feature in Windows® and Windows® Server versions and is enabled by default.

If a program requires privilege elevation, the behavior is the following:

- For administrators: Prompt for consent. A dialog is shown where either Continue or Cancel can be selected. In Windows® Server edition, value Prompt for consent for non-Windows® binaries is used.
- For standard users: A message box stating that a program has been blocked is shown.

A shield is used in the program icon to indicate that it requires administrative privileges to run. This is automatically detected by the operating system if, for example, "run as" administrator flag is set in the file properties or if the program has previously asked for administrative privileges.

3.2.9 Create Unprivileged User Account

Define a minimum of two Windows® user accounts, the privileged administrator account and a normal unprivileged user account. Only trained engineers should use the administrator account and only for Product upgrade and maintenance. All other NMS users should use unprivileged account. Hitachi Energy recommends the usage of personal accounts with adequate password policy settings.

3.2.10 Firewall (Ports and Services)

Windows® firewall is a stateful firewall that can be configured to restrict inbound and outbound connections. Consult the Product's documentation for the ports and services used. The [1KHW002426] User Manual – FOXMAN-UN Installation Guideline suggests default settings.

Also refer to [1KHW028766] Application Note – FOXMAN-UN in Firewalled Environment.

3.3 Product User Accounts

The Product requires a second user authentication once a user starts the NMS Client application. The software asks once again for a user name and password, which must be one of the Linux user accounts authorized for use with the Product. We recommend to create these additional Linux user accounts using the Product provided command "nemuser …" as documented in section "Creation of FOXMAN-UN User Accounts" of the [1KHW002414] User Manual – FOXMAN-UN under Linux. This command will set the correct group permissions for the secure use of the Product.

The NMS administrator “nemadm” is a system account without login which runs the Product application and is the owner of the installed file system of the Product.

The NEM security administrator is a Linux account which needs to be created before installing the Product. The username will need to be entered during Product installation. The NEM security administrator will then be able to assign Product specific access permissions to other Linux accounts. The assignment of access rights to a user is based on roles. Predefined roles can be used to restrict access to the system for different users based on their tasks in the system. Custom roles can also be created by a system administrator.

The definition of the roles and domains via Role-Based Access Control (RBAC) is part of the security setup. It is well documented in the section “Security Configuration” of the [1KHW002412] User Manual – FOXMAN-UN Help and further detailed in the application note [1MRC000110] FOXMAN-UN Role-based Access Control (RBAC).

Only the required functions and domains should be authorized for each user.

3.4 RADIUS Configuration

The Product can be configured to use a RADIUS server for centralized user authentication. This RADIUS server can be installed on the same hardware and OS together with the Product. This is usually done if the FOX61x are configured to use a RADIUS server. For details scan the FOX61x and Product documentation using the keyword RADIUS. The installation of a RADIUS server, e.g., FreeRadius for LINUX is also part of some versions of the Product documentation package, see [1KHW029092] Application Note – FOXMAN-UN FreeRADIUS Integration.

3.5 Installing a Redundant Network Management System

For improved availability the Product gives you the option of installing the software in two different locations.

This gives you the following redundant design options:

- the network management station itself,
- the connection between the two network management stations.

However the addition of redundant availability introduces additional attack vectors. These additional attack vectors are as follows:

- the redundant network management station itself,
- the redundant connection between the two network management stations.

Take the same security provisions for the redundant components as for the main components.

For installation details see [1KHW029097] User Manual – FOXMAN-UN Main/Standby Solution.

3.6 Verify Authenticity of Obtained SW Distribution

During Product life cycle, you may update/upgrade SW, respectively, of the devices or the Product. The distribution means of such code may vary over time. To verify the authenticity of the obtained code two methods exist, depending on the type of SW:

- The code is signed with an Hitachi Energy-certificate that is based on a trusted certificate of a Certification Authority (CA), currently DigiCert. The Product software is normally distributed using this method.
- In case the code is not signed due to technical restrictions the authenticity can be verified by an associated hash-value. Before loading a new software, the user can generate a SHA-256 hash and cross-check it against the values published on the Hitachi Energy website.

3.7 Decommissioning

Installation data and all additional data created and stored on disk during the life cycle of the Product is stored non-volatile on the disk (HDD / SSD). When decommissioning the Product, the application shall be uninstalled using the command as specified in [1KHW002414] User Manual – FOXMAN-UN under Linux, section “Removing the FOXMAN-UN Software”. For clients running on Windows® the removal shall be done by uninstalling it as per Windows® standard software removal by calling the “Add or remove programs” utility, identify the FOXMAN-UN client software in the list of installed apps, and select “uninstall” from the three-dots menu.

4 Reporting a Cybersecurity Vulnerability or Incident

Any Cybersecurity incident related to a Hitachi Energy product can be securely reported to Hitachi Energy using

https://www.hitachienergy.com/products-and-solutions/cybersecurity/reporting

More information related to vulnerability disclosure can be found at

https://www.hitachienergy.com/products-and-solutions/cybersecurity/vulnerability-disclosure-policy

5 Annex

5.1 Bibliography/Referenced Documents

[1KHW002412] User Manual – FOXMAN-UN Help

[1KHW002414] User Manual – FOXMAN-UN under Linux

[1KHW002426] User Manual – FOXMAN-UN Installation Guideline

[1KHW029097] User Manual – FOXMAN-UN Main/Standby Solution

[1KHW002690] ALS Configurator

[1KHW002399] Installation Guide – ALS for FOXMAN-UN

[1KHW029209] Application Note – FOXMAN-UN Server Setup in a Secure Network

[1KHW028766] Application Note – FOXMAN-UN in Firewalled Environment

[1KHW029092] Application Note – FOXMAN-UN FreeRADIUS Integration

[1KHW029190] Application Note – FOXMAN-UN Integration with Active Directory (AD)

[1KHW028929] Application Note – FOXMAN-UN Usage of Syslog

[1KHW029185] FOXMAN-UN R18 RHEL9 CIS Hardened Installation

[1MRC000110] FOXMAN-UN Role-based Access Control (RBAC)

[1KHW028641] FOX61x Cybersecurity Deployment Guideline

[1MRC000089] FOXMAN-UN Technical User Documentation

The manuals are published on the Hitachi Energy Publisher (https://publisher.hitachienergy.com), either within the **Technical User Documentation** package for the Product or as separately published, single documents.

5.2 Document History

Table 1: Document History

Document ID	FOXMAN-UN Release	Edition	Date	Changes since previous version
1KHD651697	R18	A	2025-09-24	Updated for system release R18. Now referencing IEC 62443 series of standards.
1KHD651697	R17A	A	2024-10-03	Reworked for system release R17A.
1KHD651697	R11B (SP01)	D	2019-12-01	Minor editorial changes and error corrections.
1KHD651697	R11B	C	2019-09-20	Revised edition, issued for R11B. Recommendation for Linux anti-virus software changed. SELinux recommendation added.
1KHD651697	R11A (SP01)	B	2019-05-10	Second edition, adopted for R11A SP01.
1KHD651697	R9C (SP03)	1 (A)	2016-08-23	Initial Deployment Guideline for FOXMAN-UN.

Hitachi Energy Ltd
Bruggerstrasse 72
5400 Baden - Switzerland

Phone: please refer to https://www.hitachienergy.com/contact-us/Customer-Connect-Center
(Customer Connect Center)
Email: communication.networks@hitachienergy.com

www.hitachienergy.com/communication-networks