HITACHI
Inspire the Next

APPLICATION NOTE

FOXMAN-UN in Firewalled Environment

Configuration and Operation

Hitachi Energy

Document ID	1KHW029012	
Document edition	FOXMAN-UN System Release:	R18
	Revision:	A
	Date:	2025-09-16

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 Purpose and Scope

1.1 General

The FOXMAN-UN system shall be deployed in a firewalled environment.

The FOXMAN-UN core component installs and activates a service file for firewalld (the firewall daemon) on the Linux server which will allow the use of all services of FOXMAN-UN in default configuration.

The firewalls should be configured to allow communications between the FOXMAN-UN components. The security risk can be minimized by opening only restricted port ranges.

This Application Note provides information for the firewall administrator to configure the firewalls in the following deployments:

- firewall between FOXMAN-UN Core and FOXMAN-UN Client,
- firewall between FOXMAN-UN Core and FOX61x network,
- firewall between DIRAC and SENC1 units in a FOX61x,
- firewall between FOXMAN-UN Core and FOX51x network,
- firewall between FOXMAN-UN Core and northbound OSS.

Deploying the FOXMAN-UN system in a firewalled environment raises the question of listening TCP/UDP ports used by applications on both sides of the firewall.

To provide answers to this question, the following major topics are covered:

- Overview of communications between the FOXMAN-UN components, focusing on the core/client processes and their corresponding port range to be opened in the firewall.
- Factors/considerations to estimate the number of ports to be opened based on your FOXMAN-UN specific implementation.

Please note:

- The actual firewall configuration procedures are beyond the scope of this document. It is up to the firewall administrator to use the FOXMAN-UN specific information provided in this document to configure his network firewalls accordingly.
- The current implementation of FOXMAN-UN restricts destination ports and some of the source ports.
- For SELinux some specific settings are required; see section 2.2 Linux Settings (on page 9).

1.2 FOXMAN-UN Components

FOXMAN-UN uses a Client/Server architecture. It consists of the following software components:

- FOXMAN-UN Core
- FOXMAN-UN Element Agent (EA)
- FOXMAN-UN Client

1.2.1 FOXMAN-UN Core component

The core component can only exist once in every FOXMAN-UN system, except for the case of Main/Standby setup where the main server and the warm standby server are two core instances with one of them being the active core while the other is a standby core.

The core component implements the business logic processing, the data storage, the network modeling and the data distribution towards user's GUI.

The core shares its resources with one or several FOXMAN-UN Clients.

1.2.2 FOXMAN-UN Element Agent (EA)

The agent component organizes the communication between the FOXMAN-UN Core and managed NEs.

It acts as a proxy, talking with NE in a specific manner, and dealing with the Core in a uniformed protocol.

An EA always runs on the same server as the Core it is associated with.

1.2.3 FOXMAN-UN Client

FOXMAN-UN Client offers a set of graphical user interfaces for operating the network, mainly for Fault, Configuration, Inventory, Performance and Security.

The main GUI interfaces are:

- NEM Desktop
- NEM Configurator
- NEM Network Browser
- NEM Homepage (Web UI)

Depending on the network management deployment, these components can be installed on a centralized system or distributed systems.

In the context of FOXMAN-UN deployment in a firewalled environment, this document focuses on implementing a firewall between

- Client and Core, and
- Agent and managed Network Elements.

1.3 Inter-Processes Communication between FOXMAN-UN Components

FOXMAN-UN uses different protocols to communicate between the components and the NE. All those protocols are based on TCP/IP and UDP/IP making them subject to restrictions driven by firewall setup.

The installation of the FOXMAN-UN core provides a consistent configuration including firewalld config files.

Some of the port ranges used for the internal communication of FOXMAN-UN could be adapted in configuration files. To make them consistent the following files need to be adapted:

- /opt/nem/etc/firewall.conf
- /etc/firewalld/services/nem.xml
- /opt/nem/etc/systemd/nem-systemd.env

1.3.1 Internal Behavior

In this scenario, the FOXMAN-UN Core and EA components reside on one machine, which shall be referred to as the FOXMAN-UN Server, while the FOXMAN-UN Client is installed and used on a separate machine, running on Linux or Windows®.

An overview of the communication between the FOXMAN-UN Server and the FOXMAN-UN Client is explained below:

1 The FOXMAN-UN Server listens for incoming client requests on the ports:
   - 9005, 9006, 5671 (fixed port numbers)

   and ports in range:
   - 40000 … 40099 (range configurable).

2 The FOXMAN-UN Client makes connections to the FOXMAN-UN Server services.
This requires several TCP port connections from the client's NEM Desktop to the FOXMAN-UN Core Server.

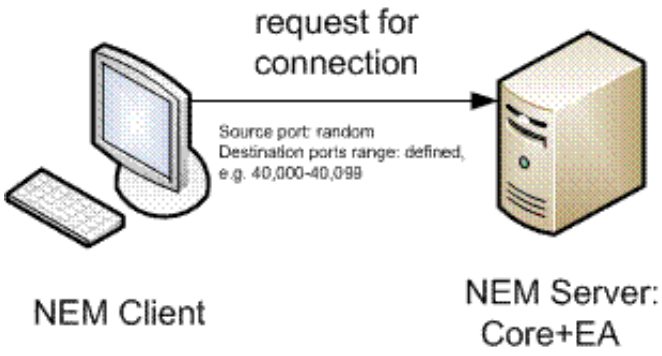

Figure 1: FOXMAN-UN Server listens, FOXMAN-UN Client initiates requests

3 The FOXMAN-UN Client actively listens for notifications and callbacks from the FOXMAN-UN Server on any available TCP ports, by default no restriction is applied.

Note:

As basic configuration, the FOXMAN-UN firewall configuration file proposes the port range 55000-55200 controlled by the following parameters:

- `nemdesktop_server_range`
- `hwview_server_range`
- `ucst_server_range`

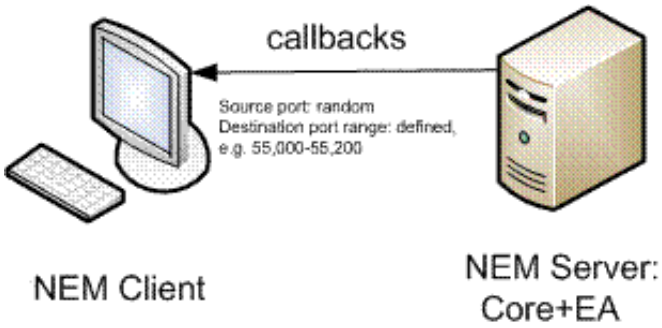

Figure 2: FOXMAN-UN Client listens, FOXMAN-UN Server initiates callbacks

4 Whenever the FOXMAN-UN administrator opens up new Client Application, e.g. NEM Network Browser, new TCP port connection is established between the two systems.

All these TCP ports or port ranges must be opened in the firewall in order to establish communications between FOXMAN-UN Client and FOXMAN-UN Server components.

1.4 Fixed TCP Ports

Table 1: FOXMAN-UN Core Process, fixed TCP ports

Process	Destination Port	Comment
RabbitMQ	5671	RabbitMQ TLS
Voyager	9005	NEM Voyager APIgateway
Voyager APIGateway	9006	Embedded FOXCST
Public REST interface	9443	Public APIgateway
CORBA	40000-40099	CORBA process (only used when installing FOXMAN-UN with install option -t)

1.5 FOXMAN-UN Server - FOX61x Communication

The FOXMAN-UN Server communication to the FOX61x network is based on

- TCP connections from FOXMAN-UN to the ports 5556 and 5558 on the FOX61x side,
- UDP notifications from FOX61x to the FOXMAN-UN Server on ports specified inside the FOXMAN-UN Agent properties (Agent Type “FOX61EA”, default port is 20736).

1.6 DIRAC to FOX61x Encryption Unit Communication

If the key manager DIRAC is installed it shall be installed on the same server as FOXMAN-UN and is therefore to be considered in the firewall rules. The communication of the key manager DIRAC to the FOX61x Encryption Unit of the “SENC1” series is based on

- TCP connections from DIRAC to the ports 9009 on the FOX61x (SENC1) side,
- TCP connections (SSH) from DIRAC to the port 22 on the FOX61x (SENC1) side.

1.7 FOXMAN-UN Server - FOX51x Communication

The FOXMAN-UN Server communication to the FOX51x network is based on

- FTP connections from FOXMAN-UN to the FTP port 21 and Telnet port 23 on the FOX51x (COBUX) side,
- FTP connection from FOX51x to the FOXMAN-UN Server on ports that cannot be reasonably narrowed down. You therefore need a stateful firewall and allow the FTP protocol for such connections, independent of the port.
- For UDP notifications from the FOX51x to the FOXMAN-UN Server, a firewall rule needs to created to pass such requests.

1.8 FOXMAN-UN Main - Standby Server Communication

In a redundancy setup with FOXMAN-UN Main and Standby servers the communication between the Main and the Standby servers is based on

- TCP connections from any port of the Main server to the port 9005 on the Standby server, and from any port of the Standby server to the port 9005 on the Main server.

2 FOXMAN-UN Firewall Configuration File: firewall.conf

2.1 firewall.conf

To fit the FOXMAN-UN processes in a firewalled deployment, the port ranges of the FOXMAN-UN processes can be defined and activated:

- FOXMAN-UN core:
  `/opt/nem/etc/firewall.conf.`
- FOXMAN-UN client for Windows®:
  `C:\Program Files\FOXMAN-UN_18.0.0\etc\firewall.conf`

Note:

To activate entries, remove the comment (hash) symbol at the beginning of the line when editing the firewall.conf file. The FOXMAN-UN processes need to be restarted (via the commands `nemstop, nemstart)` for the changes to take effect.

2.1.1 Adapting Core Server Range

To change the core_server_range it is required to change the settings in two configuration files:

1 `firewall.conf` as shown above,
2 in file `/opt/nem/etc/systemd/nem-systemd.env` search for the following line:
`ORBendPoint=giop:ssl::40000-40099`
and change the port range to match the settings of core_server_range.

2.1.2 Proposed Basic Configuration

The proposed basic configuration values for a setup **without UCST** are shown below. When using UCST, remove the "#" in front of the three lines containing `nemdesktop_server_range, hwview_server_range,` and `ucst_server_range` below:

```
# Firewall port configuration

# for the GUI clients that listen for notifications and
# callbacks, the ORB is listening on a port in the
# ranges defined below. It is possible to define the same
# range for all the GUI client; in this case the next
# available port is used.
# No definition means any port.
# ---------------------------------------
#nemdesktop_server_range       55000-55200
#hwview_server_range           55000-55200
#ucst_server_range             55000-55200

# port range used for the pm data collector
core_server_range             40000-40099

# for the GUI clients colocated to the core server that connect to the
core,
# the ORB will use the ports in the defined ranges;
# as each process of the core has its own ORB,
# the GUI client uses as many ports as ORBs it connects to.
# For R16B and following 10 ports are required
```

```
# No definition means any ports.
# Each client requires up to 10 ports:
# -> e.g. 2 clients requires 2 x 10 = 20 ports
# -> nemdesktop_client_range should be set to 48000-48020
# ------------------------------------
#nemdesktop_client_range       48000-48020
```

Note:

Each client requires up to 10 ports. The default setting is for 2 clients. If you use more than 2 clients, remove the "#" in front of the last line and increase the "nemdesktop_client_range" by 10 ports per additional user; e.g., for 5 concurrent users set the range to 48000-48050.

2.1.3 GUI Client Port Ranges

The FOXMAN-UN GUI client port ranges define the ranges to be used by the FOXMAN-UN Client processes/applications as listening ports for callbacks and notifications from the FOXMAN-UN Core.

With the proposed configuration, all the client applications as listed in the table below, listen for notifications and callbacks in any of the ports within the range 55000-55200. This limits the number of simultaneously running client applications (using asynchronous calls) to 200.

It is sufficient to have one listening port per client application, e.g. 1 listening port per NEM Desktop client, 1 listening port per map browser, 1 listening port per UCST client, etc.

It is possible to define the port range per client application to limit the number of instances an individual application can run simultaneously, e.g. setting the <<nem_desktop_server_range>> to 55000-55010 limits the NEM Desktop clients that can simultaneously connect to FOXMAN-UN Core to 10.

Likewise, setting the <<ucst_server_range>> to 55061-55080 allows only a maximum of 20 UCST GUIs to be opened simultaneously. The default <<ucst_server_range>> is 55000-55200.

<<nemdesktop_server_range>> is used for the case when one or more clients are run on the server machine. In this case, up to 10 ports are used per client, starting from 55000. However, running clients on the server machine is not recommended.

Table 2: FOXMAN-UN Client Processes/Applications

Client process port range parameters	Purpose
`nemdesktop_server_range`	- Defines the port range that can be used by NEM Desktop process as listening port for callbacks and notifications from FOXMAN-UN Core. - Defines the number of NEM Desktop clients that can simultaneously connect to FOXMAN-UN Core. - 1 listening port/NEM Desktop client.
`hwview_server_range`	- Defines the number of allowed simultaneously opened FOX51x Hardware Views. Only required for networks that include FOX51x nodes. - 1 listening port per Hardware View.
`ucst_server_range`	- Defines the number of allowed simultaneously opened UCST GUIs. Only required for networks that include FOX51x nodes. - 1 listening port per UCST GUI.

2.2 Linux Settings

Note that for the following settings you need appropriate permissions (usually root).

2.2.1 Firewall Settings

The following settings are required. During installation the nem.firewalld file is copied from “/opt/nem/share/install/lib/nem.firewalld” to “/etc/firewalld/services/nem.xml”. Make sure the contents of the file “nem.xml” are as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<service>
 <short>NEM Core Services</short>
 <description>NEM Core Service required by NEM Software</description>
 <port protocol="tcp" port="2809"/>
 <port protocol="tcp" port="40000-40099"/>
 <port protocol="udp" port="20736-20756"/>
 <port protocol="tcp" port="10161"/>
 <port protocol="udp" port="10162"/>
 <port protocol="tcp" port="9005"/>
 <port protocol="tcp" port="9006"/>
 <port protocol="tcp" port="8086"/>
 <port protocol="tcp" port="9443"/>
 <port protocol="tcp" port="5671"/>
</service>
```

If you want to use CLIs you need the following additional entries in “nem.xml” as required:

```
 <port protocol="tcp" port="2500"/>
 <port protocol="tcp" port="2600"/>
 <port protocol="tcp" port="2700"/>
```

2.2.2 Firewalld Setup

The following specific script is required for the firewall daemon (firewalld). The script requires the above “nem.xml” file (see Firewall Settings) and has to be executed to apply the firewall rules:

```
#!/bin/bash
# Activate / Start firewalld service
systemctl enable firewalld
systemctl start firewalld

# Apply firewalld rules for the NEM Core Services
firewall-cmd --zone=public --add-service=nem

# Make it persistent
firewall-cmd --zone=public --permanent --add-service=nem

# Exclude FOX51x network e.g. eth1 (avoid problems with ftp protocol)
firewall-cmd --zone=trusted --change-interface=eth1
```

If a separation of FOX61x network communication from FOX51x network communication is not possible the FTP protocol should be allowed in the firewall settings. For that purpose the script should be complemented by the following lines.

Add a rich rule for a group of FOX51x running on a specific network (example):

```
firewall-cmd --permanent --zone=public --add-rich-rule='rule
family=ipv4 source address=192.168.2.0/24 accept'
firewall-cmd –reload
```

Add a rich rule for a list of FOX51x; specify the single FOX51x IP address (example):

```
firewall-cmd --permanent --zone=public --add-rich-rule='rule
family=ipv4 source address=192.168.2.230/32 accept'
firewall-cmd --reload
```

Add a rule to allow FTP service for FOX51x - this command ensures that `firewalld` uses the correct FTP connection flow inspection and gets notified when a new server port is opened from the command channel:

```
firewall-cmd --permanent --add-service=ftp --zone=public
firewall-cmd --reload
```

To apply the firewall rules reload the firewall configuration via the command

```
firewall-cmd --reload
```

Enable netfilter conntrack helper kernel parameter. To do this, execute the following command (using sudo as shown in the command):

```
echo "net.netfilter.nf_conntrack_helper = 1" | sudo tee /etc/sysctl.d/
90-conntrack_helper.conf
```

After this configuration has been applied, the NMS server must be restarted.

3 Summary

The following tables summarize the proposed firewall concept.

Table 3: FOXMAN-UN Main - Standby Servers Communication

FOXMAN-UN Main Server	Ports		FOXMAN-UN Standby Server Ports
REST Interface HTTPS			
Main-Standby communication	any	TCP →	9005
Standby-Main communication	9005	TCP ←	any

Table 4: FOXMAN-UN Client - Server Communication

FOXMAN-UN Client	Ports		FOXMAN-UN Server Ports
REST Interface HTTPS			
any	any	TCP →	9005
any	any		9006
Client Operations			
nemdesktop_client_range	48000 - 48020	TCP →	40000 - 40099 (core_server_range)
Keep Alive			
nemdesktop_client_range	48000 - 48020	TCP ←	any
nemdesktop_server_range	55000 - 55100		
hwview_server_range	55000 - 55200		
ucst_server_range	55000 - 55200		
Advanced Message Queuing Protocol (RabbitMQ)			
any	any	TCP →	5671

Table 5: FOXMAN-UN Server - FOX61x Network Communication

FOXMAN-UN Server	Ports		FOX61x Ports
Polling			
any	any	TCP →	5556
Port specified in Agents	Agent ports	UDP ←	any
KOAP over SSH	any	TCP →	5558

Table 6: FOXMAN-UN Server - FOX51x Network Communication

FOXMAN-UN Server	Ports		FOX51x Ports
Notifications			
Port specified in agents	Agent ports	UDP ←	any

Table 7: DIRAC - FOX61x Network Communication

DIRAC	Ports		FOX61x (SENC1) Ports
GRPC Interface HTTPS			
any	any	TCP →	9009
SSH, SFTP	any	TCP →	22

Table 8: FOXMAN-UN Server - HLM/OSS Communication

FOXMAN-UN Server	Ports		HLM Ports
Northbound SNMP interface	10161[1]	TCP ←	any
Northbound inventory CLI (if required)	2500	TCP ←	any
Northbound ECLI proxy daemon (if required)	2600	TCP ←	any
Northbound line test CLI (if required)	2700	TCP ←	any

1. This is the default port; the port can be configured in /opt/nem/etc/snmpagentd.conf

4 Annex

4.1 List of Open Ports on FOXMAN-UN Server

For all processes with “core_server_range”, a port is picked randomly in the range and will be opened for a client/server communication.

In FOXMAN-UN R18 the default range is 40000-40099.

Process	Port	Firewall	Target	Type	Authentication	conf/nem.conf	Description
nem-base							
nem-omni-event.service	core_server_range		nem-base	C++			
nem-bp-rmqvh.service	5671/tcp	ON				/etc/rabbitmq/rabbitmq.conf	Local
nem-bp-securitymgrd.service	core_server_range			C++			
Agents							
FOX61EA agent	core_server_range			C++			KOAP notification receiver. One port per agent.
	range from: 20736/udp						
FOX51x agent	core_server_range			C++			One port per agent.
	range from: 20736/udp						
	21/ftp	ON FTP				ftp_port	
	23/telnet	ON TELNET				telnet_port	
SNMP agent	core_server_range			C++			SNMP trap receiver.
	default: 162/udp						One port per agent.
OMS agent	core_server_range			C++			SNMP trap receiver.
	range from: 20736/udp						One port per agent.
Voyager Java processes							
nem-bp-apigateway.service	9005	ON	nem-base	java		/opt/nem/etc/NMS.properties:rest_port	Client rest communication, Internal REST router
	9006	ON	nem-base				Embedded FOXCST gateway
nem-bp-publicgateway.service	9443	ON		java			9443: swagger web page describing the public REST API.
nem-core							
nem-bp-alarmmgr.service	core_server_range			C++			
nem-bp-blm.service	core_server_range			C++			
nem-bp-eventlogmgr.service	core_server_range			C++			
nem-bp-reportmgr.service	core_server_range		nem-core	C++			

Process	Port	Fire-wall	Target	Type	Authen-tication	conf/nem.conf	Description
	2500	ON/OFF				nbi_inventory_oss_port	NEM inventory northbound interface. By default restricted to localhost, but could be reconfigured to be available remotely.
nem-bp-linetestmgr.service	2700	ON/OFF	nem-core	C++		nbi_linetest_oss_port	By default restricted to localhost, but could be reconfigured to be available remotely.
nem-bp-networkmgr.service	core_server_range			C++			
nem-bp-networkquerymgr.service	core_server_range			C++			
nem-bp-pmasyncmgr.service	core_server_range			C++			Send PM requests to Nodes (FOX61x, FOX51x).
nem-bp-pmcollector.service	core_server_range			java			Schedule PM jobs and write PM records to Postgres database.
nem-enp-mgr.service	core_server_range			C++			
nem-enp-secmgr.service	core_server_range			C++			Listening port of DPM
nem-hlm-snmpnbi.service	core_server_range			C++	V1/V2/V3	snmp_request_port	SNMP requests
	default: 10161/tcp					snmp_v1v2_support	
nem-np-networkmgr.service	core_server_range			C++			
nem-bp-taskmgr.service	core_server_range			C++			
nem-bp-servicemgr.service	core_server_range			C++			Local rest communication
Others							
systemd/rpcbind	111	OFF					
rsyslogd	514	OFF					
postgres	5432	OFF				/opt/nem/etc/odbc.ini	

5 Document history

Table 9: Document history

Document ID	FOXMAN-UN Release	Rev.	Date	Changes since previous version
1KHW029012	R14A	A	2020-07-31	First revision for this product release.
1KHW029012	R14A	B	2020-09-04	Extended CORBA / EA port range to 40099. Added list of open ports per process in section 4.1.
1KHW029012	R14B	A	2020-12-02	Updated for latest product release.
1KHW029012	R15A	A	2021-07-06	Updated for latest product release.
1KHW029012	R15B	A	2022-02-02	Updated for latest product release.
1KHW029012	R16A	A	2022-10-20	Reworked for current product release.
1KHW029012	R16B	A	2023-08-14	Reworked for current product release.
1KHW029012	R17A	A	2024-08-08	Updated for current product release.
1KHW029012	R18	A	July 2025	Updated for current product release.

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

Document ID: 1KHW029012 R18 Rev. A