MSM Security Whitepaper

Contents

PREPARED BY	STATUS Approved	SECURITY LEVEL Public		
APPROVED BY	APPROVAL DATE 2023-03-10			
OWNER	DOCUMENT KIND Article			
TITLE MSM Security Whitepaper				
OWNING ORGANIZATION PGHV	DOCUMENT ID 2GHV694671	REV. A	LANG. en	PAGE 1/6

Hitachi Energy

1. Overview

1.1. Applicability and Scope

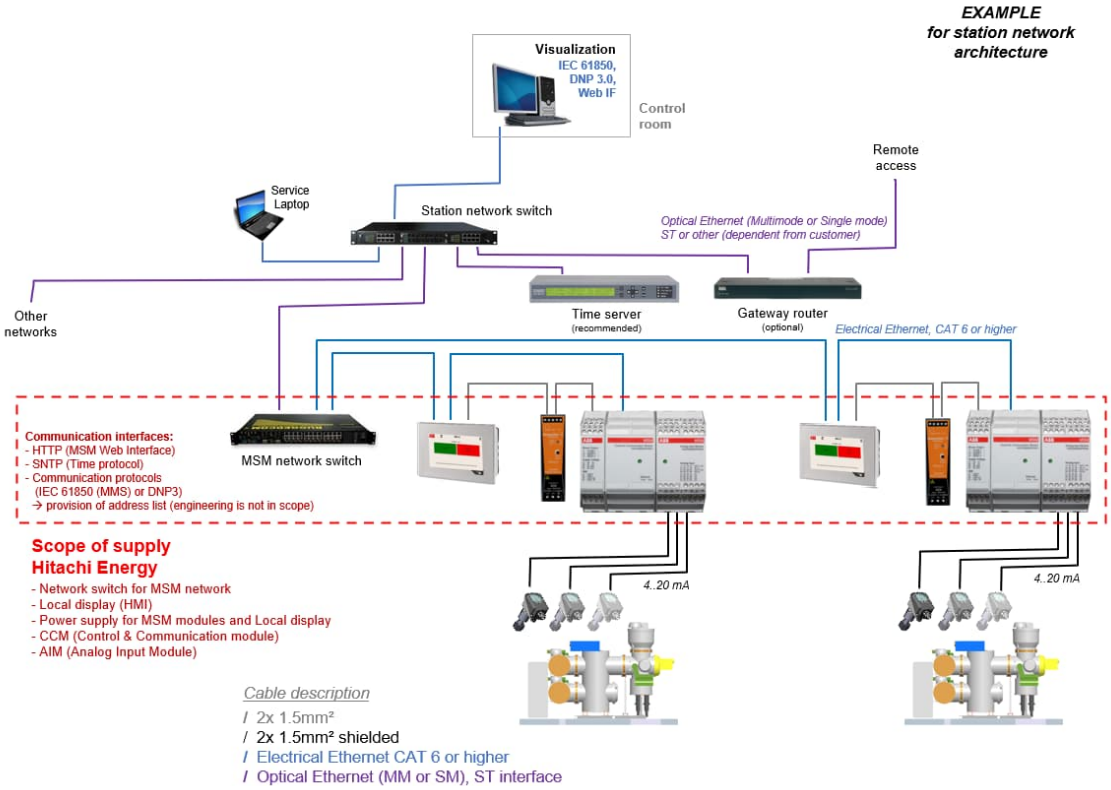
This document describes MSM’s security features with relation to IEC62443-4-2. Furthermore, the relation to ISO27001 is outlined. Beyond this, Hitachi Energy recommends its users to make sure that security procedures and network setup are in accordance with relevant standards and best practices.

MSM versions this document is applicable to:

- MSM 2.2.x and earlier

2. MSM System Layout

Below figure shows an MSM station network architecture example, where MSM is installed bay-wise at two bays. MSM stacks are connected to the required MSM network switch, which is connected to the station switch. On this optionally a gateway router for remote access and a time server can be connected.


EXAMPLE
for station network
architecture
Visualization
IEC 61850,
DNP 3.0,
Web IF
Control
room
Remote
access
Service
Laptop
Station network switch
Optical Ethernet (Multimode or Single mode)
ST or other (dependent from customer)
Other
networks
Time server
(recommended)
Gateway router
(optional)
Electrical Ethernet, CAT 6 or higher
Communication interfaces:
- HTTP (MSM Web Interface)
- SNTP (Time protocol)
- Communication protocols
(IEC 61850 (MMS) or DNP3)
→ provision of address list (engineering is not in scope)
MSM network switch
4..20 mA
4..20 mA
Scope of supply
Hitachi Energy
- Network switch for MSM network
- Local display (HMI)
- Power supply for MSM modules and Local display
- CCM (Control & Communication module)
- AIM (Analog Input Module)
Cable description
/ 2x 1.5mm²
/ 2x 1.5mm² shielded
/ Electrical Ethernet CAT 6 or higher
/ Optical Ethernet (MM or SM), ST interface

2.1. Network Interface

The availability of specific protocols depends on the configuration of the system. Below the list of supported protocols.

SNTP

An SNTP client is integrated into MSM. The clock of the MSM can be set by this service. An SNTP server sends the time to MSM and the MSM update the system time. This server can be activated by the configuration.

HTTP

An HTTP server is integrated into MSM. The server provides a user-friendly user interface that serves as a central interface for data visualization, updates, etc. Users need to authenticate themselves to get access to this inter-face.

Encryption algorithms:

The web server provides digest authentication for username and user password transfer. HTTPS is not supported.

SSH

An SSH server is integrated into MSM and supports SSH V1 and V2. The server provides an encrypted remote command line. An SSH client can connect to the server to get access to the command line. The user must authenticate, and the user gets a server authentication. The interface is not required for normal MSM operation.

Encryption algorithms:

3DES, AES, Blowfish, CAST, DES, MD5, MD5-96, RC4, RC4-128, SHA1, SHA1-96

SFTP

An SFTP server is integrated into MSM. The server provides encrypted remote file system access. An SFTP client can connect to the server to get access to the file system. The user must authenticate, and the user gets a server authentication. The interface is not needed for normal operation.

Encryption algorithms:

3DES, AES, Blowfish, CAST, DES, MD5, MD5-96, RC4, RC4-128, SHA1, SHA1-96

IEC61850

An IEC61850 MMS server is integrated into MSM. The server needs to be activated in the configuration. It provides all measured and calculated values of MSM. An IEC61850 client can connect to the server to poll for data.

DNP3

A DNP3 slave is integrated into MSM. The slave needs to be activated in the configuration file. It provides all measured and calculated values of MSM. A DNP3 master can connect to the slave to receive the data.

MQTT(s)

A MQTT client is integrated into MSM. The client provides all measured and calculated values of MSM. Via an MQTT broker, the data can be received. A signal list can be exported from MCT.

OPC UA

An OPC UA client is used for communication with an optional local HMI/web panel.

3. IEC62443 Security

In this section MSM 2.x is outlined in relation to IEC62443. It is important to note that the product itself is not currently certified for IEC62443 compliance, however, Hitachi Energy MSM development team is certified as can be seen in the official documentation [1].

IEC62443 provides guidance on how automation systems can be secured against cybersecurity threats. The standard defines a Defense in Depth approach addressing different aspects of cybersecurity such as patch management, lifecycle requirements, and network and systems security. Here we will focus on the latter as defined in IEC62443-4-2 and refer to the most relevant requirements stated in the standard.

IEC62443-4-2 requirement mapping to MSM implementation

Requirement ID	Requirement Title	MSM Implementation
CR 1.3	Account Management	MSM implements an embedded user management, implementing roles based on the (Wikipedia, 2023) [2] The MQTT interface supports client-side certificates for *Unique identification and authentication.*
CR 1.7	Strength of password-based authentication	No password policy is enforced in the MSM. It is up to the user organization to put proper processes and rules in place.
CR 1.10	Authenticator feedback	Login attempts are reflected in a log file.
CR 1.13	Access via untrusted networks	MSM is sold as a system where the devices are located in a trusted, separate network segment with no internet access.
CR 2.1	Authorization enforcement	Role based access is enforced where certain activities are restricted to certain roles, e.g., only administrator can add and remove users. This is true for all users
CR 2.5	Session lock	A session timeout can be configured for automated termination of a session, and users can end a session.
CR 2.8	Auditable events	MSM records system events in a log file (e.g., login, configuration update, system error). Each event has an ID, timestamp, source, and description.
CR 2.9	Audit storage capacity	The storage capacity for the MSM log files sufficient for the typical lifetime of the device.
CR 2.11	Timestamps	The MSM produces accurate timestamps for all events in its logs. MSM can be configured to use the Network Time Protocol (NTP) to get the time from a time server.
CR 2.12	Non-repudiation	User logins and particular actions are recorded together with the username.
CR 3.2	Malicious code protection	The MSM does not support the execution of dynamically linked code.
CR 3.4	Software and information integrity	The MSM Configuration Tool (MCT) validates all configuration before exporting and applying to the device.
CR 3.5	Input validation	Inputs to the monitoring functions are validated before use. Validation errors are recorded in the system log files.
CR 3.9	Protection of audit information	Log files are only accessible to authorized users and can only be viewed or downloaded and not be deleted from the filesystem.
CR 4.1	Information Security	Access to monitoring data requires access to the MSM network and login. Some protocols are unencrypted, e.g., IEC61850. Hence, the system shall be installed in an isolated network segment with no direct internet access.
CR 4.2	Information Persistence	Upon decommissioning, all data can be erased by removing and formatting the SD from the device.

CR 5.1	Network segmentation	MSM is usually sold as a system, including the installation of the devices within an isolated network segment for monitoring devices.
CR 6.1	Audit log accessibility	The log files can be accessed by authorized users on a read-only basis. I.e., the files cannot be changed on the MSMs storage device.
CR 7.1	Denial of service protection	The system has protection against DoS events, e.g., rate limiter which is setup during commissioning with the MSM system.
CR 7.2	Resource management	Task management and rate limiting in the network mitigate issues causing temporary peaks in resource use.
CR 7.3	Control system backup	The MSM can be requested to provide a full system backup (system report) which can be used to restore the system is needed.
CR 7.4	Control system recovery and reconstitution	The MSM does not perform any control, hence CR 7.3 is addressing the concern sufficiently.
CR 7.6	Network and security configuration settings	The MSM is delivered with the appropriate network settings.
CR 7.7	Least functionality	Only explicitly configured protocols and services are active and necessary ports open.
EDR 3.10	Support for updates	Firmware and configuration can be updated by authorized users.
EDR 3.11	Physical tamper resistance	The device is always installed inside the locked LCC inside of a substation which itself is a secured area with access control.

4. Relation to ISO27001

IEC62443 address specific security needs for OT equipment and environments. These needs need to be fulfilled in addition to the requirements of the ISO27001, which is out of the scope of the MSM system.

5. References

[1] Certificate of Conformity – Industrial Cyber Security Capability, Link to Hitachi Energy Webpage

[2] https://en.wikipedia.org/wiki/Principle_of_least_privilege

6. Key terms and abbreviations

Abbreviation or Term	Description
MSM	Modular Switchgear Monitoring
OT	Operational Technology

7. Revision History

Rev.	Description	Date
1	Initial version	06.03.2023