MSM Security Whitepaper

Contents

1. Overview .......................................................................................................................................................2
   1.1. Applicability and Scope........................................................................................................................2

2. MSM System Layout ....................................................................................................................................2
   2.1. Network Interface.................................................................................................................................2

3. IEC62443 Security ........................................................................................................................................3

4. Relation to ISO27001 ....................................................................................................................................5

5. References ....................................................................................................................................................5

6. Key terms and abbreviations ......................................................................................................................5

7. Revision History ...........................................................................................................................................6
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.

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 interface.

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 access 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

<table>
<thead>
<tr>
<th>Requirement ID</th>
<th>Requirement Title</th>
<th>MSM Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR 1.7</td>
<td>Strength of password-based authentication</td>
<td>No password policy is enforced in the MSM. It is up to the user organization to put proper processes and rules in place.</td>
</tr>
<tr>
<td>CR 1.10</td>
<td>Authenticator feedback</td>
<td>Login attempts are reflected in a log file.</td>
</tr>
<tr>
<td>CR 1.13</td>
<td>Access via untrusted networks</td>
<td>MSM is sold as a system where the devices are located in a trusted, separate network segment with no internet access.</td>
</tr>
<tr>
<td>CR 2.1</td>
<td>Authorization enforcement</td>
<td>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</td>
</tr>
<tr>
<td>CR 2.5</td>
<td>Session lock</td>
<td>A session timeout can be configured for automated termination of a session, and users can end a session.</td>
</tr>
<tr>
<td>CR 2.8</td>
<td>Auditable events</td>
<td>MSM records system events in a log file (e.g., login, configuration update, system error). Each event has an ID, timestamp, source, and description.</td>
</tr>
<tr>
<td>CR 2.9</td>
<td>Audit storage capacity</td>
<td>The storage capacity for the MSM log files sufficient for the typical lifetime of the device.</td>
</tr>
<tr>
<td>CR 2.11</td>
<td>Timestamsp</td>
<td>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.</td>
</tr>
<tr>
<td>CR 2.12</td>
<td>Non-repudiation</td>
<td>User logins and particular actions are recorded together with the username.</td>
</tr>
<tr>
<td>CR 3.2</td>
<td>Malicious code protection</td>
<td>The MSM does not support the execution of dynamically linked code.</td>
</tr>
<tr>
<td>CR 3.4</td>
<td>Software and information integrity</td>
<td>The MSM Configuration Tool (MCT) validates all configuration before exporting and applying to the device.</td>
</tr>
<tr>
<td>CR 3.5</td>
<td>Input validation</td>
<td>Inputs to the monitoring functions are validated before use. Validation errors are recorded in the system log files.</td>
</tr>
<tr>
<td>CR 3.9</td>
<td>Protection of audit information</td>
<td>Log files are only accessible to authorized users and can only be viewed or downloaded and not be deleted from the filesystem.</td>
</tr>
<tr>
<td>CR 4.1</td>
<td>Information Security</td>
<td>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.</td>
</tr>
<tr>
<td>CR 4.2</td>
<td>Information Persistence</td>
<td>Upon decommissioning, all data can be erased by removing and formatting the SD from the device.</td>
</tr>
</tbody>
</table>
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 if 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


6. Key terms and abbreviations

<table>
<thead>
<tr>
<th>Abbreviation or Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSM</td>
<td>Modular Switchgear Monitoring</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
</tbody>
</table>
## 7. Revision History

<table>
<thead>
<tr>
<th>Rev.</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial version</td>
<td>06.03.2023</td>
</tr>
</tbody>
</table>