Keeping the World Flowing
for Future Generations

Master Station

Security

System and Security Overview

Contents

Section Page

System and Security Overview 3
- Security strategy 3
- System architecture: *Master Station* and Interfaces 4
- Physical protection 4

Security Management 5
- Identification of threats and mitigation measures 5
- Security set-up and control 5
- OEM security contact details 6
- Anti-virus measures in place 6
- System hardening applied 6
- System and network monitoring in place 6
- Interfaces and integration with existing/other systems 6

Section Page

Change Management 7
- System maintenance requirements 7
- Security patch management 7
- Back-up and disaster recovery 7

Security Data 7
- List of usernames and passwords 7
- Firewall rules 7
- Ports, protocols, programs 7
- Whitelisting 7
- Wireless security rules 7
- List of licenses and software 7
- Anti-virus and patch installation log 7

System and Security Overview

Security strategy

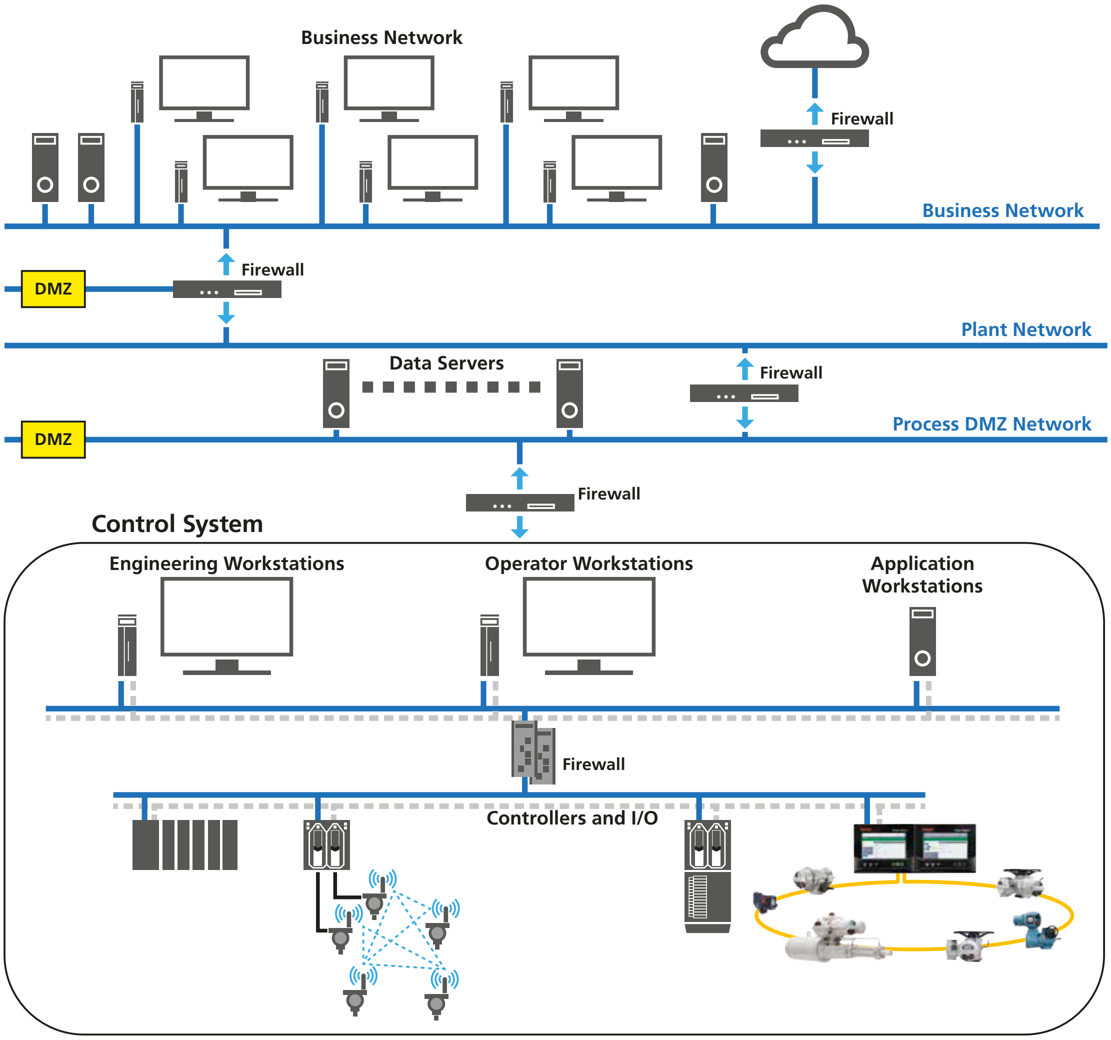
The Rotork *Master Station* (RMS) has several security issues that need to be addressed. Although many of these are dependent on the overall network configuration of the devices and any upstream systems (such as a PLC or SCADA system), there are several features that can be configured from the RMS, itself.

Note that, as with all IT-based systems, Rotork cannot guarantee that the RMS can be protected against currently known and future threats. However, following the guidelines and procedures in this document will significantly reduce the risk.

rotork®
Master Station

System and Security Overview

System architecture: *Master Station* and Interfaces



The diagram above shows an example plant with cyber security protection. Segmentation of networks forms separate security zones that are important to protect the control system. Security zones use firewalls and other security devices to only allow authorised network traffic between the zones.

The firewall at the top of the control system network only allows traffic from the servers in the process demilitarised zone (DMZ) network to the control system and blocks traffic coming directly from the plant network – preventing a direct attack from the business network. Devices in the plant network that require access to control system data must access the servers in the DMZ. The firewall above the servers only allows the plant network workstations to connect to the servers.

Examples of DMZ applications in this context include OPC data servers, SCADA systems, web servers and secured computers.

The RMS allows you to configure the key Ethernet settings. For a dual or hot standby *Master Station* the left and right side modules are labelled A and B. When entering the Ethernet settings, the MAC addresses of the A and B *Master Stations* are hard coded during CPU production and cannot be changed. However the Side A and Side B IP addresses, their subnet masks and their host port gateway IP addresses need to be specified.

Physical protection

Each RMS should be placed in a locked cabinet, with keys allocated only to personnel responsible for operation and maintenance of the RMS.

Security Management

Identification of threats and mitigation measures

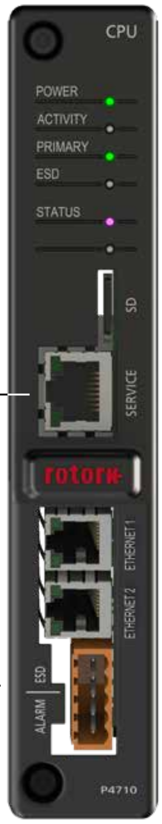
Physical access to the RMS should be controlled by a lock and key (*see Physical protection, Page 4*).

Access to upstream systems, such as SCADA systems is via TCP and UDP (*see Interfaces and integration with existing/other systems, Page 6*). Access from these systems is controlled using a firewall, as shown on *System architecture: Master Station and Interfaces, Page 4*. Whilst this guarantees a high degree of cyber security, Rotork recommends that you install up-to-date security patches on the firewall (*see Security patch management, Page 7*).

Connections to the webserver are via HTTPS protocol.

A service Ethernet port is available for an authorised engineer to access the RMS. This requires physical access to the RMS and uses the same username and strong password as the two host Ethernet ports.

Interfaces to downstream systems are via the Modbus protocol over secure TCP ports. Modbus is not vulnerable to general viruses that corporate networks and home devices are.



Service Ethernet port connection (RJ45).

ESD input and alarm output connection (removable connector).

LEDs:

POWER:
- Colour – Green
- When the module is first powered on, the LED will be lit continuously.
- While the module is in bootloader mode (start up and re-programming of software), the LED will blink three times per cycle (cycle of 3 seconds).
- While the module is configuring during start up, the LED will blink twice. This state indicates that the processor is now executing the application, but it is waiting for the configuration phase to complete.
- While the module is running correctly, the LED will blink once per cycle.
- Off indicates no power to the module.

ACTIVITY:
- Colour – Orange
- Engineering debug indication.

PRIMARY:
- Colour – Green
- LED on indicates primary mode.
- LED off indicates standby mode.

ESD:
- Colour – Red
- LED on indicates global ESD command active.
- LED off indicates no ESD present.

STATUS:
- Colour – Blue

Ethernet 1 connection (RJ45)
Ethernet 2 connection (RJ45)

Security set-up and control

The customer is responsible for setting up and maintaining their corporate IP network and incorporating each RMS into it.

All control systems must be segmented from the business network using a firewall and a DMZ network. Communications between the host SCADA systems, DCS and PLC and the RMS, are via Modbus. Configuration settings are sent using Rotork firmware (RFW) files via the Ethernet ports. These have a proprietary format and are highly resistant to malicious action. Viruses cannot be sent via Modbus.

It is possible to perform security configuration from the RMS using the RMS's HMI (human machine interface). The same operations can be performed using a service port from the RMS to an engineer’s laptop. This service port can be enabled or disabled.

If configured as enabled, a whitelist lists the IP addresses and/or MAC addresses that can connect to the RMS. This would normally contain details of the engineers’ laptops. If whitelisting is not enabled, it would not prevent any unauthorised users from connecting to the RMS. Note, however, that physical security and password security still operate as countermeasures.

Security Management

OEM security contact details

All enquiries should be made to your local Rotork office.

Anti-virus measures in place

The following measures are implemented by the Rotork *Master Station*:

- Where possible, the RMS System shall implement password protection to PLCs and other upstream systems
- The RMS System shall use a unique default password per System
- The RMS System shall implement a whitelist for IP and MAC addresses of devices permitted to communicate with the RMS. *See Whitelisting, Page 7*
- The RMS System shall close all network services that are not required for System operation
- The RMS System shall implement a service interface that is logically isolated from the main control interface

System hardening applied

The general principles of system hardening are as follows:

1. Install security updates and patches: These are communicated via service bulletins
2. Use strong passwords
3. Bind processes to localhost
4. Implement a firewall: This is the customer's responsibility
5. Keep things clean: This is the customer's responsibility. Ensure there are no log files that grow unchecked
6. Security configurations: *see System architecture: Master Station and Interfaces, Page 4*
7. Limit access: RMS is supplied with one unique admin username and password on the test certificate
8. Monitor your systems: There are no specific monitoring requirements for RMS
9. Create backups (and test!): *see Back-up and disaster recovery, Page 7*
10. Perform system auditing: There are no specific auditing requirements for RMS

System and network monitoring in place

- The RMS System shall implement an alarm if it detects hardware has been tampered with, for example, if a cover is opened

The RMS monitors and records host communications, Modbus read request and write command messages, along with all commands issued via the web pages or HMI screen. Any failure of communications to the RMS can cause an alarm to be raised.

Interfaces and integration with existing/ other systems

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the core protocols used in a LAN and computer networking. Within these networks a port is an endpoint to a logical connection, not to be confused with the physical port.

Only the TCP and UDP ports shown in the table below are accessible over *Master Station* Ethernet connections:

Application	Protocols	Ports	Comments
HTTP: *Master Station* webserver	TCP	80	HTTP interface will not do anything other than redirect to the HTTPS interface.
HTTPS: *Master Station* webserver	TCP	443	Encrypted user interface and API.
Modbus	TCP	502	Standard port for Modbus TCP.
Modbus	TCP	50003 50004 50005 50006 50007 50008 50009	Additional ports available for Modbus TCP.
NTP: Network Time Protocol	UDP	123	Time synchronisation, it is not possible to query the time from the *Master Station*.

Change Management

System maintenance requirements

There are no periodic maintenance requirements for the RMSs.

Security patch management

Patches are communicated to Rotork's regional offices via service bulletins.

Back-up and disaster recovery

The configuration file, which contains all the RMS modules' settings, is used as a backup. This is stored on the RMS's CPU and can only be extracted via the RMS's webpages. It should be saved to the commissioning engineer's laptop hard drive following completion of commissioning and a copy sent electronically to the customer for their records.

The other backup files to save are:

- The "User Configuration" which contains the CPU's user names and passwords in an encrypted format
- Tag files which contain names and IP addresses of connected devices

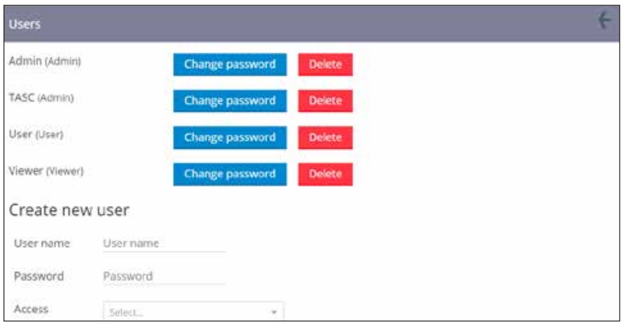
Every time any setting is changed one of these files will change and a new backup file will need to be saved.

The configuration settings, tag files and/or the user configuration can be restored from the engineer's laptop.

Security Data

List of usernames and passwords

Each RMS is delivered with an administration account and unique password, detailed on its test certificate. Rotork recommends that you change this password and save the user configuration. You can create new users, delete users and change passwords.



Users

Admin (Admin)

TASC (Admin)

User (User)

Viewer (Viewer)

Create new user

User name: User name

Password: Password

Access: Select...

Firewall rules

The firewall is the responsibility of the customer.

Ports, protocols, programs

See Interfaces and integration with existing/other systems, Page 6.

Whitelisting

If whitelisting is enabled for the IP address, only devices with a listed IP address can communicate with the *Master Station* via Ethernet connection. Access to the web pages or Modbus database is prohibited if the device IP is not listed.

If whitelisting is enabled for the MAC address, only devices with a listed MAC address can communicate with the *Master Station* via Ethernet connection. Access to the web pages or Modbus database is prohibited if the device MAC address is not listed.

If whitelisting is enabled but no IP or MAC addresses are listed, Ethernet connectivity to the *Master Station* is effectively disabled. At least one valid address must be defined in the list for whitelisting to function correctly.

Service and host ports that are not connected to the same physical network must be configured for different IP subnets to avoid routing issues.

Up to 10 IP and 10 MAC addresses can be defined in the whitelist for the host ports. Up to 5 IP and 5 MAC addresses can be defined in the whitelist for the service port.

Rotork recommends that IP addresses are used in preference to MAC addresses.

Wireless security rules

As the RMS does not use wireless communications, this section is not applicable.

List of licenses and software

We do not use licensed software on our system, so this section is not applicable.

Anti-virus and patch installation log

Rotork keeps a paper log of these installations.

www.rotork.com

A full listing of our worldwide sales and
service network is available on our website.

Rotork plc
Brassmill Lane, Bath, UK

tel +44 (0)1225 733200
email mail@rotork.com

As part of a process of on-going product development, Rotork reserves the right to amend and change specifications without prior notice. Published data may be subject to change. For the very latest version release, visit our website at www.rotork.com