

rotork®

Keeping the World Flowing
for Future Generations

rotork® *Master Station* Full configuration manual



CE UK
CA

Network Systems



rotork® Master Station



Table of Contents

Section	Page
1. Introduction	4
Interface and Configuration	5
2. The User Interface	6
3. Menu Structure	16
Host Communications	31
4. Ethernet Communications to the Rotork <i>Master Station</i>	32
5. Serial Communication to the Rotork <i>Master Station</i>	45
6. Hot Standby	51
Field Networks	52
7. <i>Pakscan</i> Classic Field Network	53
8. Modbus Open Field Network	64
Modbus Technical Information	72
9. Host Modbus Specification	73
10. Modbus Database – Generic and Honeywell EPLCG	75
11. Modbus Database – Yokogawa and Honeywell SI	96
12. Data Interpretation (All Modbus Databases)	119
Glossary of Terms	125

1. Introduction

This manual provides instruction on the configuration, operation and analysis of the *Master Station* and connected devices.

This manual should be read in conjunction with PUB059-050 *Master Station Safe Use, Installation and Maintenance Manual* supplied with the *Master Station*.

The *Master Station* must be installed as per instructions provided in PUB059-050.

Section 2 provides information to gain a full understanding of the *Master Station* interface and how information is presented. It is important to be familiar with interface behaviour described in this section before proceeding through the manual.

Section 3 explains the menu structure of the *Master Station*.

Section 4 provides information for Ethernet host communication to the *Master Station*.

Section 5 provides information for serial host communication to the *Master Station*.

Section 6 explains behaviour of a hot standby *Master Station*.

Section 7 provides information for the *Pakscan* Classic field network AIM and connected FCUs.

Section 8 provides information for the Modbus Open field network AIM and connected FCUs.

Section 9 details the Modbus specification for host communication to the *Master Station*.

Section 10 defines Modbus Database – Generic and Honeywell EPLCG.



Section 11 defines Modbus Database – Yokogawa and Honeywell SI.

Section 12 provides information for interpreting data from the *Master Station* and connected FCUs.

Glossary of Terms provides descriptions for acronyms or technical terms used throughout PUB059-052.

SOME FUNCTIONS DETAILED IN PUB059-052 REQUIRE USER OR ADMIN LEVEL ACCESS.

Interface and Configuration

Section		Page
	2. The User Interface _____	6
	2.1 Getting Started _____	6
	2.2 General User Interface Functions _____	10
	3. Menu Structure _____	16
	3.1 Profile _____	16
	3.2 Loop Map _____	17
	3.3 Alarms Page _____	18
	3.4 Devices Page _____	20
	3.5 Interfaces Page _____	22
	3.6 <i>Master Station</i> Page _____	23
	3.7 Utilities _____	24



2. The User Interface

2.1 Getting Started

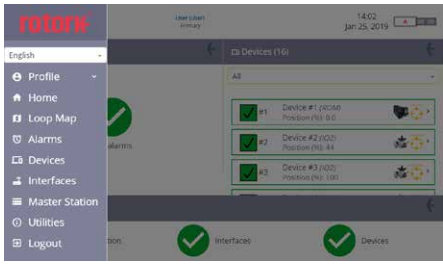
The user interface can be accessed using the local touch screen or via the built in web pages using a web browser. In both cases the screens that you see are identical, except the web page drop down menu list is displayed on the screen at all times (subject to screen resolution). For the purposes of this manual, all settings shown will be from the local touch screen display.

The menu structure of the user interface is intuitive, therefore little training or direction is required to be able to navigate to the areas of interest to the operator.

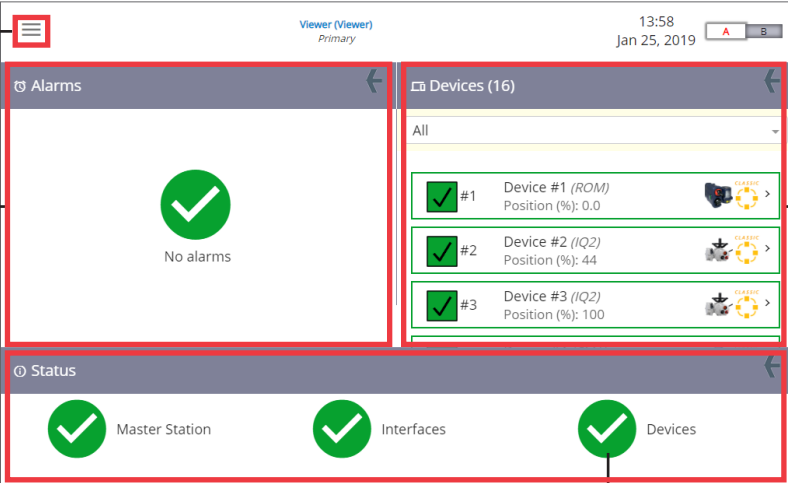
2.1.1 Home Display

Home display on the local touch screen:

Touching ☰ brings up the menu bar:



Devices Area:
Any Field devices that are connected to the *Master Station*, communicating or not, are shown here. From here the list of devices can be scrolled through and individual devices selected. Selecting the banner
☰ Devices () ←
takes you to the dedicated Devices page.



Alarms Area:
Any alarms that are still present or have not been accepted (acknowledged) are shown here. From here the list of alarms can be scrolled through, selected and accepted. Selecting the banner
☰ Alarms ←
takes you to the dedicated Alarm page.

Status Area:
An overview status of the *Master Station*, interfaces and field devices is shown here.

- ✔ A tick indicates that the status of that item is all healthy.
- ! An exclamation mark indicates that there is an alarm or error. Touching the banner has no function, but dedicated pages for each item are selected by touching the tick or exclamation mark.



2.1.2 Main Banner

Click to open the menu bar.

The top line shows the Tag name of the *Master Station*, the tag name can be different for Side A and Side B.
 The second line shows the login level in the form **Username (Login Level)**.
 The bottom line shows whether the *Master Station* is in primary or standby mode.

The active side of the *Master Station* is shown in red with a raised profile. A white background shows the primary side and a grey background shows the standby side.

☰

Left
 Admin (Admin)
Primary

09:53
 Feb 11, 2019

A
B

Clicking on the time will bring up the time change settings, it will only appear if the Admin level login has been used:

Left
Admin (Admin)
Primary
08:33
Mar 11, 2019

←

Format 12hr 24hr
 NTP disabled. Enable through Master Station settings.
 Date
 Time :
 UTC Offset :

Save
Cancel

Time format is configurable for 12 or 24 hour. NTP can be enabled for automated time and date or manual adjustment is possible through the date and time fields. It is important to set the correct UTC offset for the *Master Station* location to ensure that data logs from the *Master Station* have the correct time. The NTP settings are found within the *Master Station* setting pages.



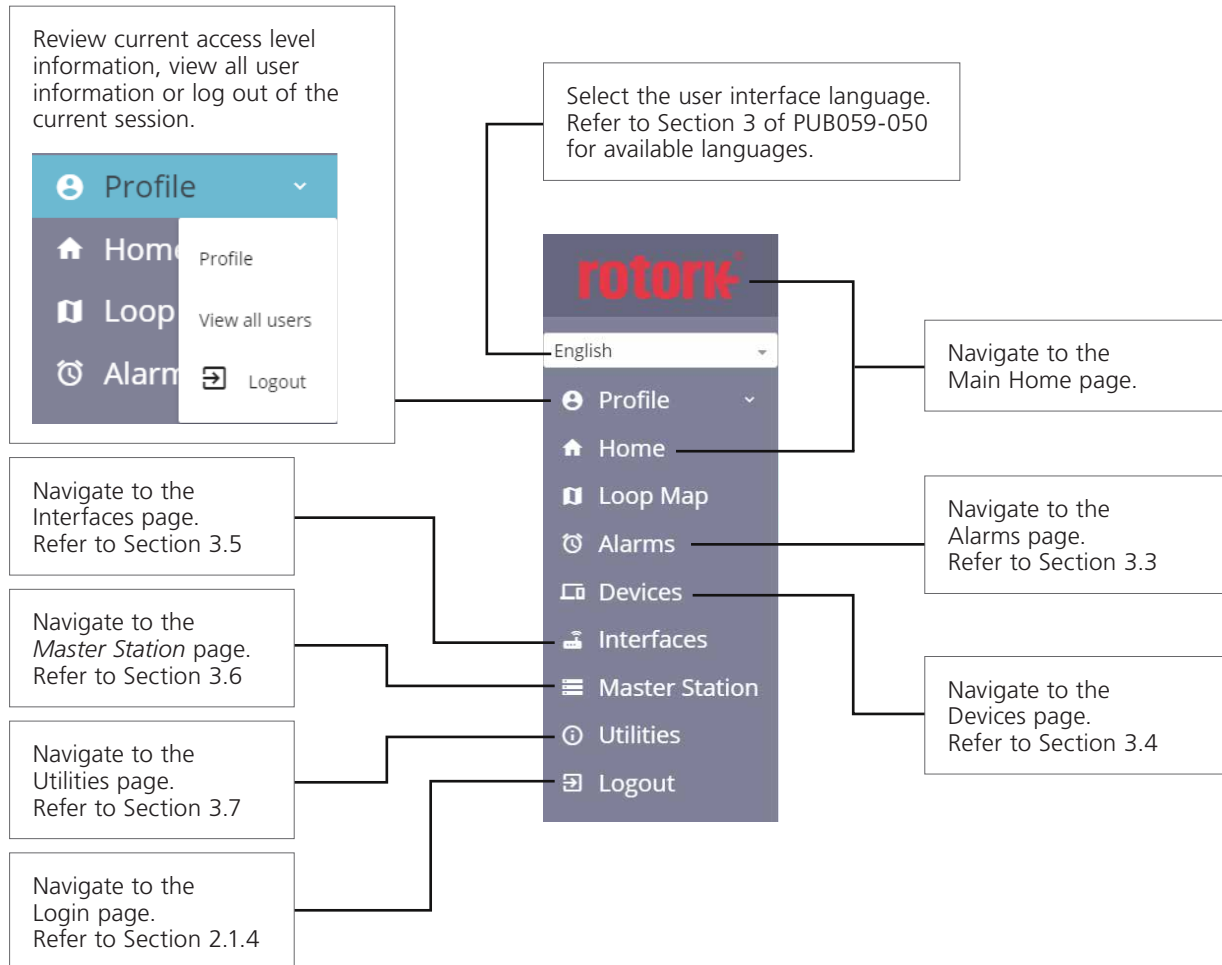
For hot standby *Master Stations*, the standby side top bar is shaded grey.



2. The User Interface *continued*

2.1.3 Menu Bar

The menu bar will appear if you select the ☰ icon.



2. The User Interface *continued*



2.1.4 Logging into the *Master Station*

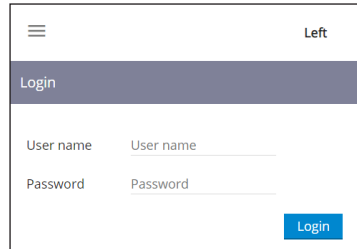
The *Master Station* has 3 access levels:

- Viewer – data can only be viewed and not modified
- User – data can be viewed and some field unit settings can be modified
- Admin – full access to view and modify all settings

Refer to Section 3.1 Profile of this manual for information on *Master Station* operator accounts. To complete the operation required, the operator may need to log in.

Viewer access is always available at the local display however a password must be entered for the same access through a web browser.

Select Login from the menu bar and enter the appropriate login details.



The main banner will indicate the login level after the correct details are entered.

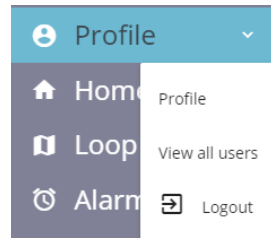


The top line shows the Tag name of the *Master Station*, the tag name can be different for Side A and Side B.

The second line shows the login level in the form **Username (Login Level)**.

The bottom line shows whether the *Master Station* is in primary or standby mode.

It is possible to log out via the menu bar, or the profile drop down box. Admin access level can add and remove users.





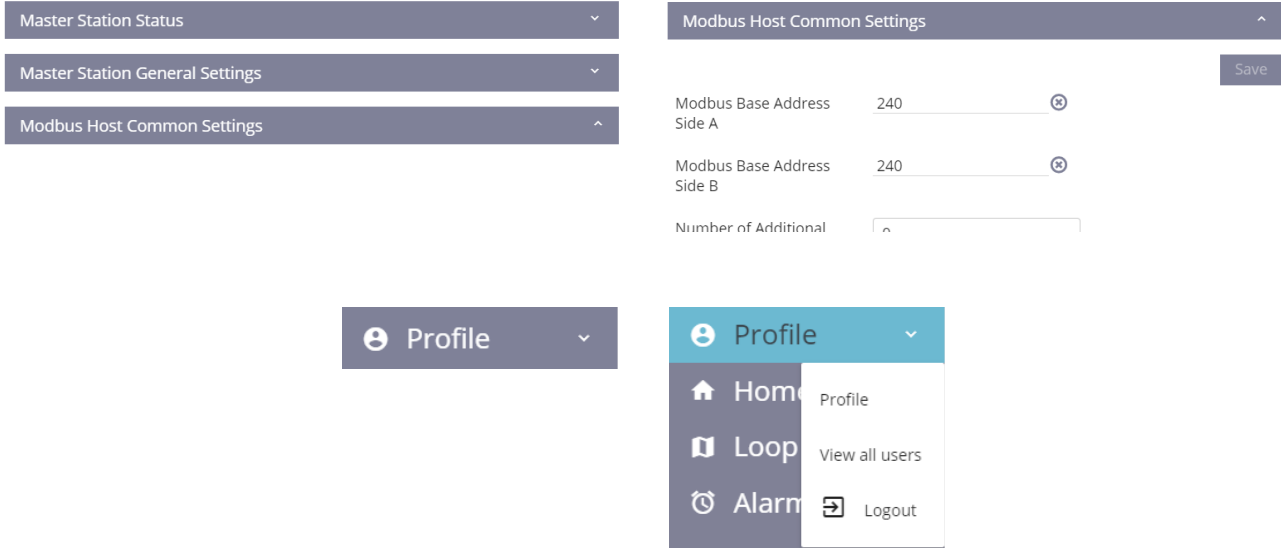
2. The User Interface *continued*

2.2 General User Interface Functions

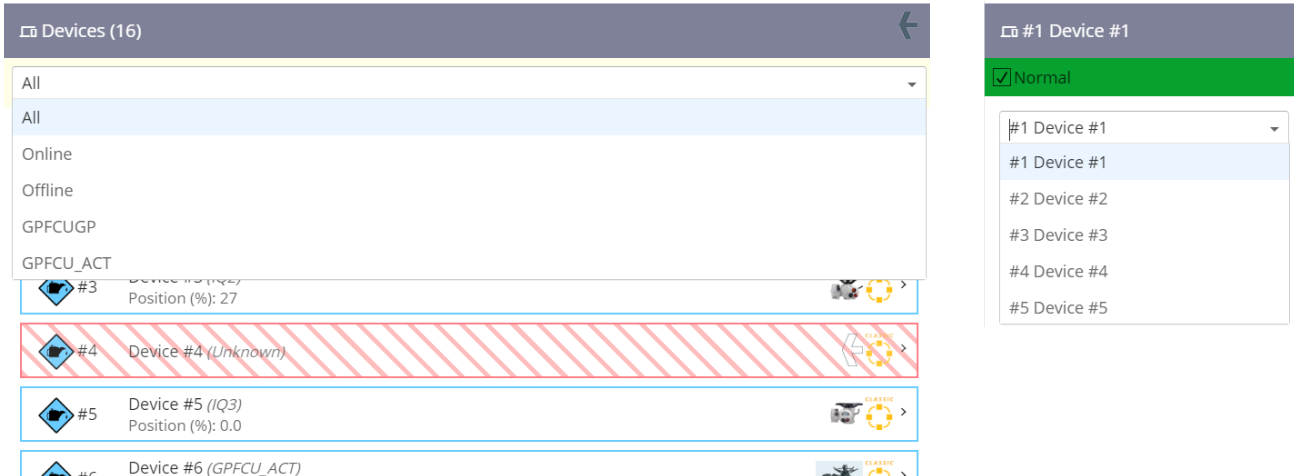
The user interface has a number of different behaviours to show or hide data, edit setting values or perform actions.

2.2.1 Down and Up Arrows

A down arrow indicates the presence of an expandable menu or drop down box. Click anywhere on a banner showing a down arrow to expand the menu.



An expanded banner will show an up arrow. Click anywhere on the banner to collapse the menu. Click anywhere on a drop down box to expand the list.



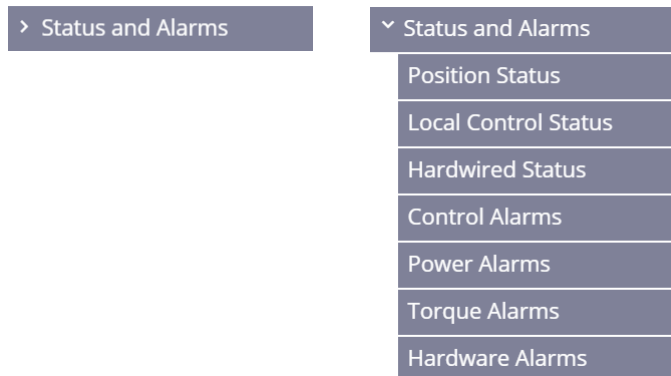
Drop down boxes will disappear when an item is selected from the list or another part of the screen is selected.



2.2.2 Right Arrows

A right arrow indicates an item with sub menus below it.

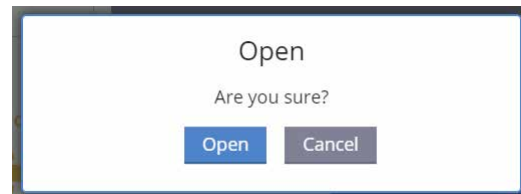
Selecting 'Status and Alarms' reveals a list of pages below it containing specific data.



The arrow changes to a down arrow to indicate that the list can be minimised.

2.2.3 Buttons

Buttons trigger operation commands that require confirmation on the pop up warning window.





2. The User Interface *continued*

2.2.4 Text and Edit Boxes

Text boxes permit alphanumeric data for settings such as Valve Tag. Edit boxes only allow set data types depending on the setting. Text box example containing letters and numbers:

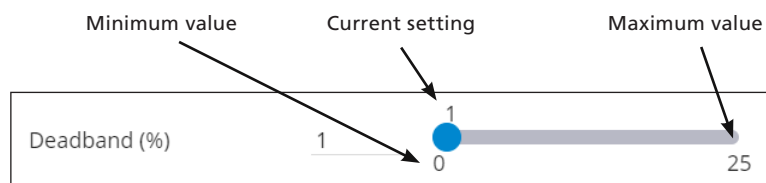
Valve Tag MOV_456_1 ✕

Edit box example containing numbers only:

Deadband (%) 3.2

2.2.5 Slider Bars

Slider bars display and edit settings that have fixed ranges. The bar shows the current setting for the item and the minimum and maximum range setting.



2.2.6 Radio Buttons

Radio buttons display settings that can only have one state. Editing a radio button setting will only permit selection of one option.

Hot Standby Module Disabled Enabled



2.2.7 Changing Settings

Unsaved setting changes will cause the section banner to change colour to yellow and the individual setting to highlight yellow. Select 'Save' to confirm the changes or select 'Reset' to revert settings to the previously saved values.

Setting	Value	Range
Time Parameters last retrieved	2019-3-19 13:19:14	-
Min Span Position (%)	0	0 to 100
Max Span Position (%)	100	0 to 100
Deadband (%)	2	0 to 25
Hysteresis Band (%)	0.5	0 to 25

Navigating away from the page will cause a pop up to be displayed. Selecting 'Stay on page' will remove the pop up window and remain on the current page with unsaved changes. Selecting 'Leave' will leave the page and any unsaved settings will revert to the previously saved values.

Unsaved changes
You have made changes on this page - leave without saving?

Leave **Stay on page**

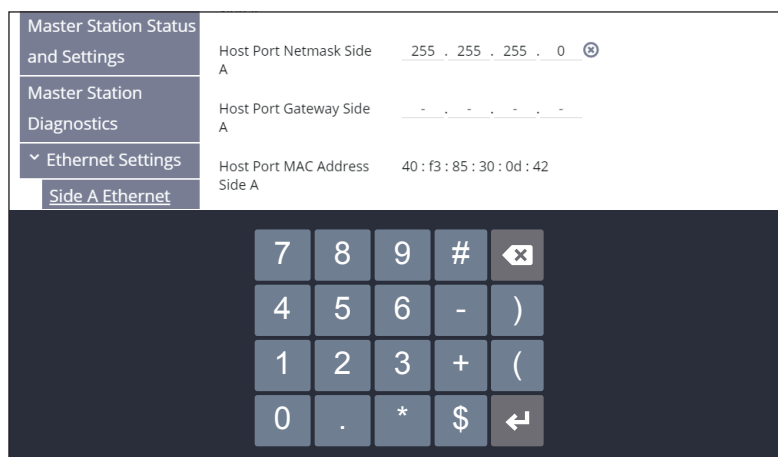
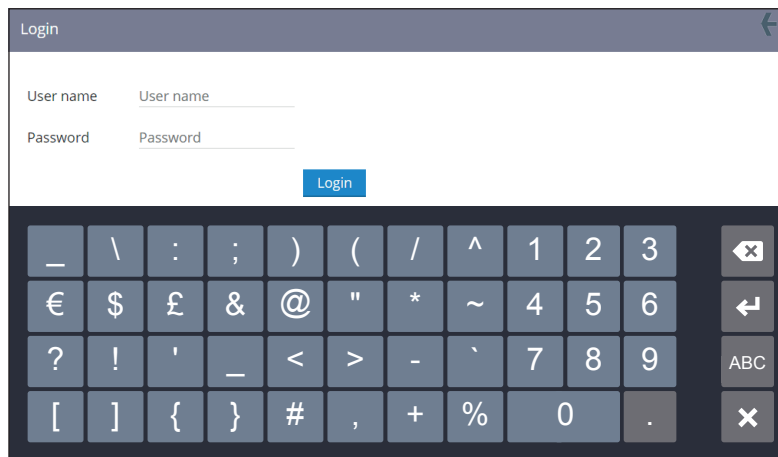
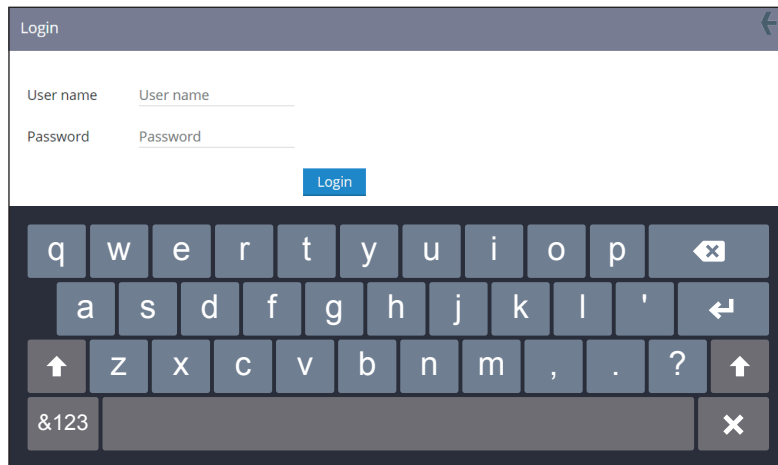
Settings are ONLY changed if the Save button is selected



2. The User Interface *continued*

2.2.8 Local Display Pop Up Keyboard

The *Master Station* local display includes a touch keyboard that appears whenever a text or numeric setting is selected. The keyboard will vary depending on the type of data permitted.

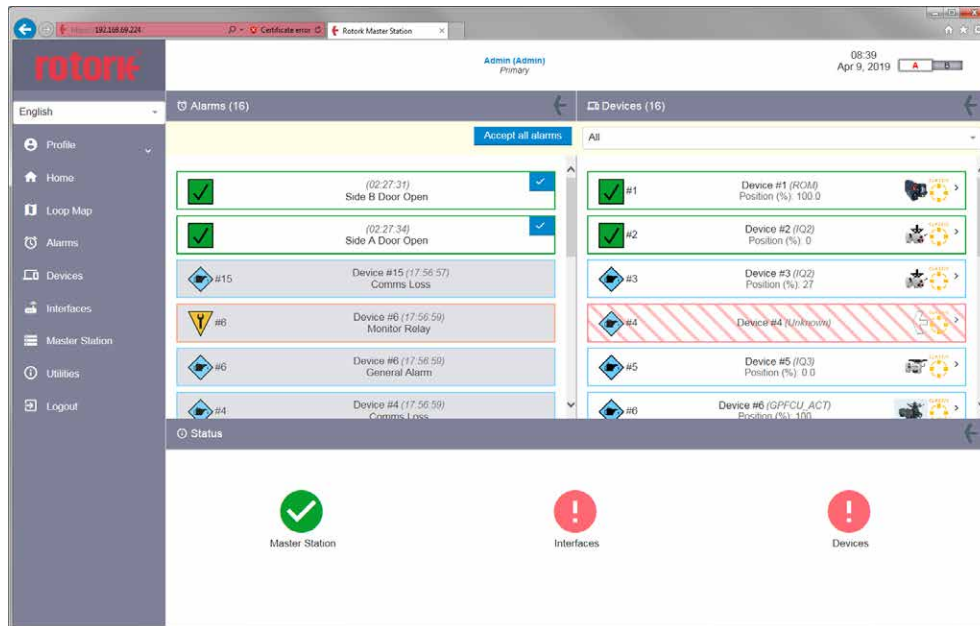


2. The User Interface *continued*



2.2.9 Web Page Screen Size

The *Master Station* web browser interface will dynamically resize depending on screen resolution and browser window size.





3. Menu Structure

Menus in this section follow the structure of the menu bar when is selected.

3.1 Profile

The User Details page shows the user name and access level for the logged in account. To change the Password, input the old password and then input a valid new password. The new password must be entered in two separate fields to avoid typing errors.

Selecting 'View all users' navigates to the Users page.

The Users page permits password and account changes to all accounts with equal or lower access rights.

- Viewer access only permits changes to viewer accounts
- User access permits changes to viewer and user accounts
- Admin access permits changes to all accounts including creation and deletion

Changes to account passwords always require entry of the old password. Deleting an account will trigger a warning message to confirm the action. One Admin account will always remain active on the *Master Station*.

User Interface Session Timeout

After 15 minutes of inactivity, the *Master Station* will automatically end the current session and the user will be logged out.

Password Complexity

Master Station account passwords must be between 8 and 100 characters long and must include at least one upper case, lower case, numeric digit and special character. Special characters are:

!@#£\$%^~&* _+(){}[];':",.<>/?-`\\€



Forgotten Passwords

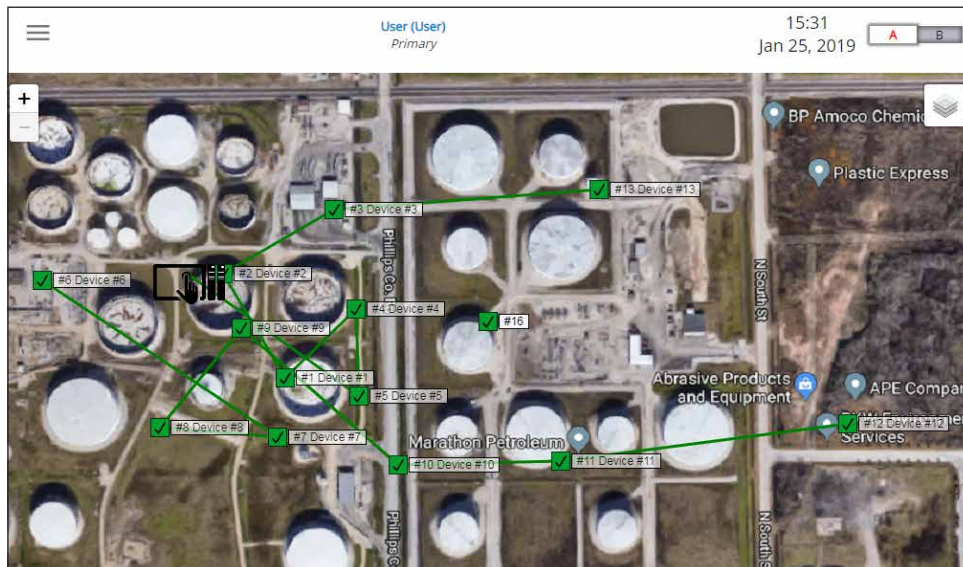
Forgotten passwords cannot be reset but Admin level access permits deletion and creation of new accounts. If a password is lost, Rotork recommends deleting the account and recreating the account with a new password.

Contact Rotork if all Admin account credentials have been lost or forgotten. You will be required to verify your identity, authority and provide the *Master Station* unique ID (accessible within the *Master Station* settings or on the *Master Station* test certificate) plus the password reset code (obtained using the Request Reset Password Code in the Utilities menu, refer to Section 3.7.4). Rotork will then be able to provide reset instructions for the *Master Station*.

User Interface Login Retries

Entering incorrect login credentials will trigger a back off delay timer to prevent a brute force repeat entry attack. Each successive failed attempt will increase the period until the next attempt can be performed. Access to the *Master Station* with correct login credentials will be blocked when the back off timer is active. Rotork recommends waiting up to five minutes before re-entering correct login credentials.

3.2 Loop Map



The Loop Map page is designed to show a satellite view of network devices. A background image of the site can be uploaded in the general *Master Station* settings so devices can be positioned at their approximate install locations.

The Loop Map image must be .PNG format and 1024 x 520 pixels. Images in different formats or sizes will not successfully upload to the *Master Station*.

FCUs on a Modbus Open Loop Map will appear in the same order as the Device File.

Rotork recommend using a Loop Map image with light colours so that network devices are clearly visible.



3. Menu Structure *continued*

3.3 Alarms Page

The Alarms page shows any recorded alarms from network devices, the host controller or the *Master Station*. Alarms remain visible until they are accepted by the user.

If an accepted alarm remains visible, the alarm condition is still active.

Alarms are split into different categories depending on the type of alarm.

Accepting all alarms will clear the alarm log. Any remaining alarms are still active but will no longer be shown as new.

Alarms can be accepted and cleared individually. An alarm that remains is still active but will no longer be shown as new.

Icon	Device	Time	Alarm Type	Action
🔧	#4	01:00:07	General Alarm	✓
⚠️	#4	01:00:07	Monitor Relay	✓
⚠️	#4	01:00:07	Local Stop	✓
✅	#5	01:00:45	Monitor Relay	✓
✅	#5	01:00:45	General Alarm	✓

Certain events can trigger multiple alarm conditions. Device 4 in the above example shows three different alarms, all triggered by the Local Stop action.

The icon against an alarm indicates the type and current state of the alarm.

- ❌ Failure
- ✅ Device healthy
- 🔧 Maintenance required
- ⚠️ Control inhibited

3. Menu Structure *continued*



Accepted alarms will disappear if the alarm condition is no longer present. If the alarm condition is still active, the alarm will remain and be shaded grey.

The screenshot displays the 'Alarms (15)' interface. At the top, it shows the user 'Admin (Admin) Primary' and the time '10:55 Apr 12, 2019'. A yellow banner at the top right contains the text 'Accept all alarms'. Below this, a list of alarms is shown, each with a device icon, device ID, and description. The 'Local Control' alarm for Device #5 is highlighted with a blue checkmark, indicating it has been accepted. Other alarms include 'General Alarm' for Device #5, 'Comms Loss' for Device #15, and 'General Alarm' for Device #3.

Device	Time	Description	Status
#5	20:02:06	General Alarm	Active
#5	20:02:06	Monitor Relay	Active
#5	20:02:06	Local Control	Accepted
#15	20:02:08	Comms Loss	Active
#3	20:02:08	General Alarm	Active
#3	20:02:08	General Alarm	Accepted



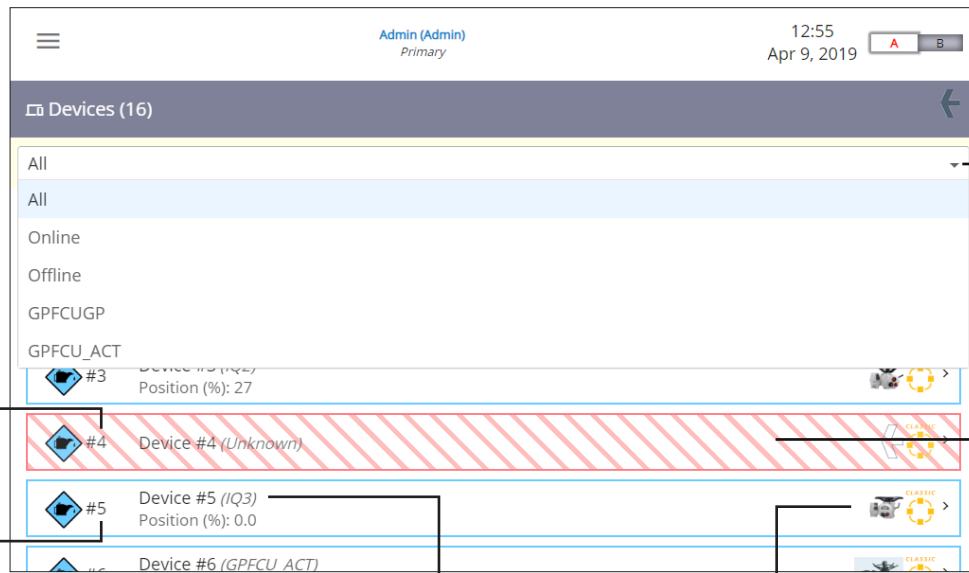
3. Menu Structure *continued*

3.4 Devices Page

The Devices page lists all FCUs configured to communicate with the *Master Station*. This includes any FCUs not currently communicating with the *Master Station*.

Every device is shown with its assigned FCU address.

The drop down box enables filtering of the list by device type or connection status.



Device tag is shown here if one is set. The default name shows the device FCU address.

The type of field device is shown in brackets and represented with a picture of the device.

Selecting any part of the device banner will navigate to the status page for that device.



Device banners with hashing on, indicate communication has been lost with the field network.



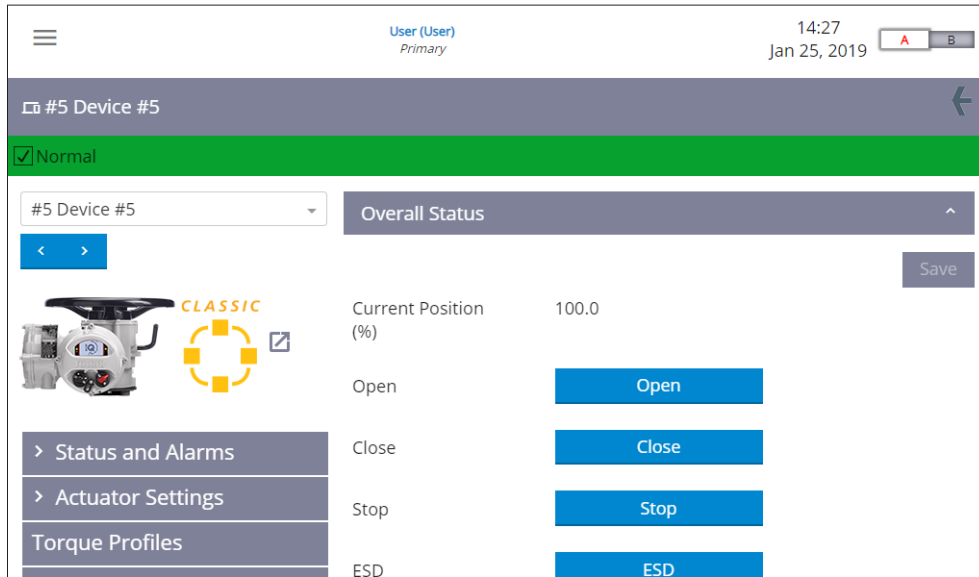
The icon against a device number indicates the current state of the device.

- Failure
- Device healthy
- Maintenance required

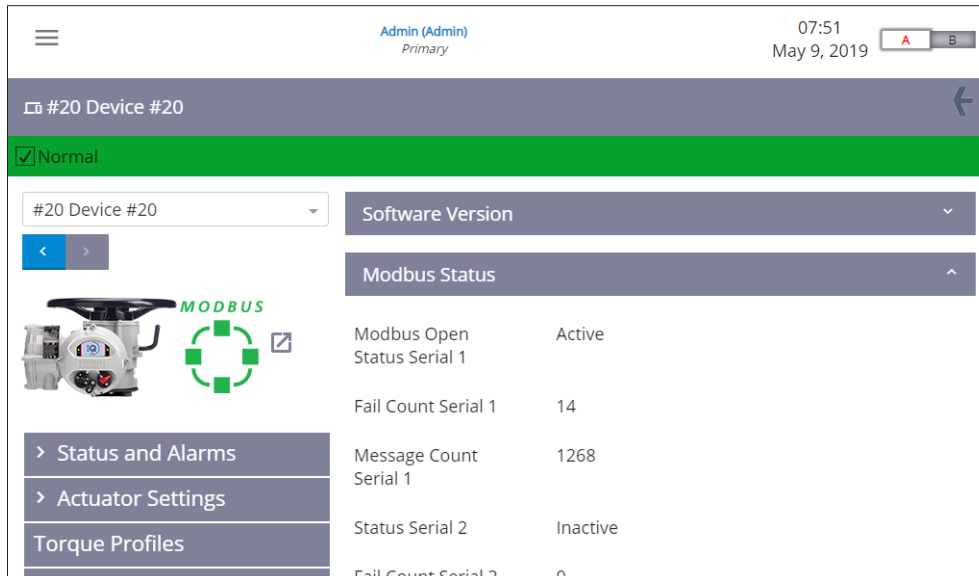


3.4.1 Device Detail

Selecting a device from the Devices page will show detailed status and configuration information for the selected device. Limited control commands are available if the connected device state permits operation.



Device information is accessible through the left side menu structure. Status and setting items will appear in the right side section of the display and may require scrolling or expanding a collapsed banner to view. Device information will vary for different device types and different network types.

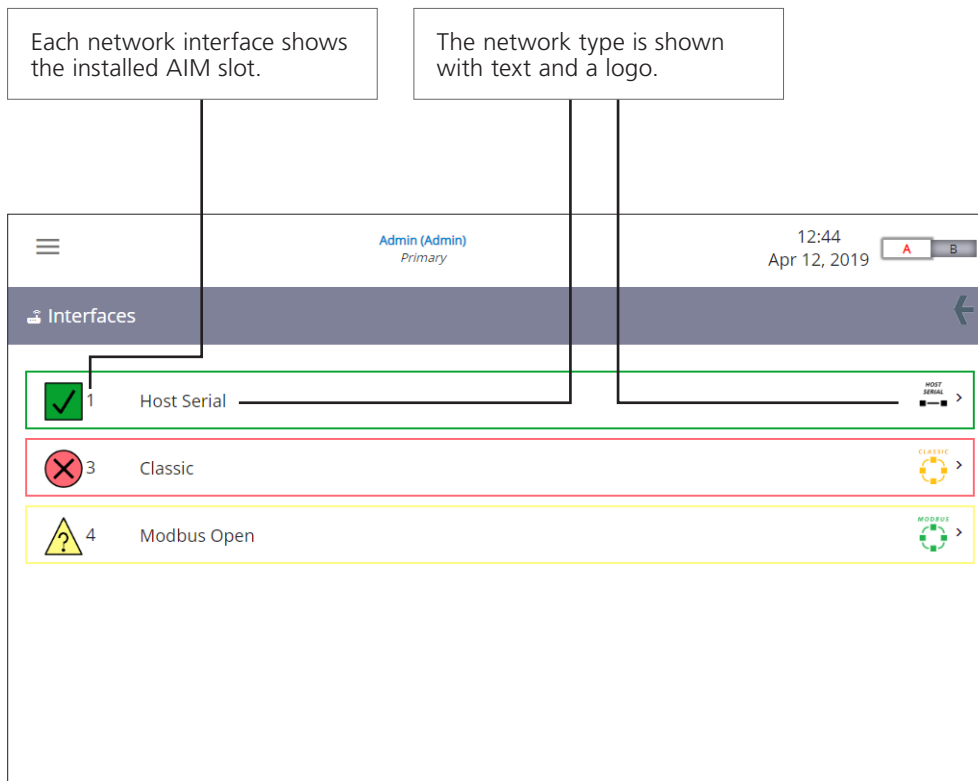




3. Menu Structure *continued*

3.5 Interfaces Page

The Interfaces page lists all of the networks installed to the *Master Station*.



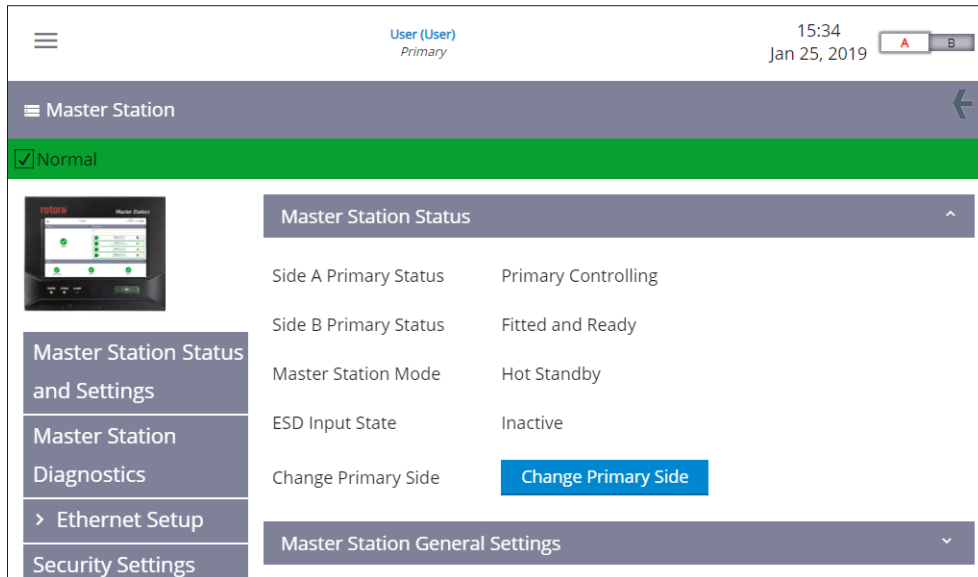
The icon against a network type indicates the current state of the network.

- Failure
- Healthy
- Maintenance required
- Out of specification



3.6 Master Station Page

All settings that impact behaviour of the *Master Station* are accessible from the *Master Station* page. Status, settings, diagnostics, communication settings and security are all configurable within the left menu structure. Visible information may vary depending on the *Master Station* type and installed AIMS.



The icon and status bar below the *Master Station* banner indicates the current state of the *Master Station*.

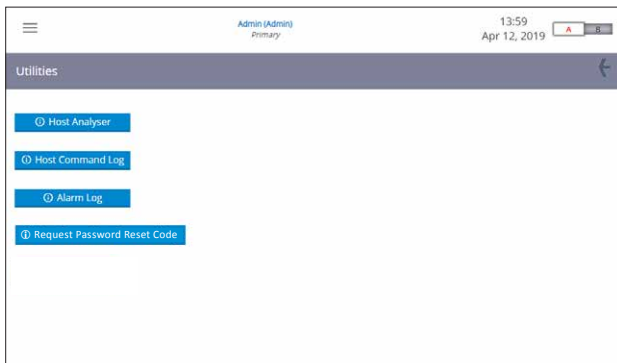
- Failure
- Normal
- Maintenance required
- Out of specification



3. Menu Structure *continued*

3.7 Utilities

Rotork *Master Station* includes a number of utility tools for data analysis and manufacturer support. The features available for users vary depending on login level and access method to the *Master Station*.







Local display interface



Web browser interface

All utility logs include a common set of action buttons to interact with the log information.

Action buttons perform the following functions:

-  Navigate between pages
-  Refresh the log to include new messages
-  Download the log as CSV file
-  Delete all logged messages



3.7.1 Host Analyser Page

The Host Analyser is a real time system analyser for monitoring and troubleshooting Modbus host communication through the Ethernet or Host Serial ports.

The analyser will record up to 10,000 messages (requests and responses) in the Host Analyser Log for each of the interfaces (Ethernet, RTU1 and RTU2) and it is useful for debugging host control system issues. Visibility of the messages ensures correct formatting and access to the necessary data can be checked.

The Host Analyser Log only shows the latest 10,000 messages for the selected port at the time of selection. The Host Analyser is a circular buffer which means the oldest messages expire as new messages appear. The display is not dynamic. Pressing the Refresh button will show the latest messages.

The Host Analyser data can be downloaded as a CSV file for further analysis or recording purposes. Please note the Host Analyser is continually updating, therefore the data downloaded as a CSV file is likely to include new data not shown on the display.

Only one interface can be selected at a time.

The screenshot shows the 'Host Analyser' page in a web browser. At the top, it displays 'Admin (Admin) Primary' and the time '13:40 Apr 12, 2019'. Below the title bar, there are navigation arrows and a 'Detail' link. The interface selection area shows three options: 'Ethernet' (checked), 'RTU1', and 'RTU2'. Below this is a table of messages with columns for 'Address', 'Timestamp', and 'Message'. The table contains seven rows of data, alternating between TxSideA and RxSideA messages.

Address	Timestamp	Message
<input type="checkbox"/> TxSideA[10.200.1.123:502]	2019-04-09 07:44:25.904	F0:01:02:8C:60
<input type="checkbox"/> RxSideA[10.200.1.123:502]	2019-04-09 07:44:25.903	F0:01:00:00:00:10
<input type="checkbox"/> TxSideA[10.200.1.123:502]	2019-04-09 07:44:25.902	F0:03:78:60:8C:00:10:00:04:78:E3:00:0...
<input type="checkbox"/> RxSideA[10.200.1.123:502]	2019-04-09 07:44:25.901	F0:03:00:00:00:3C
<input type="checkbox"/> TxSideA[10.200.1.123:502]	2019-04-09 07:44:25.901	F0:04:78:80:00:00:00:00:24:00:02:00:2...
<input type="checkbox"/> RxSideA[10.200.1.123:502]	2019-04-09 07:44:25.900	F0:04:06:A0:00:3C
<input type="checkbox"/> TxSideA[10.200.1.123:502]	2019-04-09 07:44:25.900	F0:02:02:08:18



3.7.2 Host Command Log Page

The Host Command Log has a similar structure and user interface as the Host Analyser Log; however only Modbus write commands sent to the *Master Station* are logged. The Host Command Log is a circular buffer that will record the most recent 10,000 messages for each of the interfaces (Ethernet, RTU1 and RTU2). The display is not dynamic. Pressing the Refresh button will show the latest messages.

The screenshot shows the 'Host Command Log' interface. At the top, it displays 'Admin (Admin) Primary' and the date/time '08:24 May 10, 2019'. Below the title bar, there are navigation arrows and a 'Detail' view on the right. The main area contains a table of log entries with columns for 'Address', 'Timestamp', and 'Message'. The table is filtered to show 'Ethernet' messages. The entries are as follows:

Address	Timestamp	Message
<input checked="" type="checkbox"/> RxSideA[10.200.1.123:502]	2019-05-01 07:55:36.086	F0:06:00:05:00:01
<input checked="" type="checkbox"/> RxSideA[10.200.1.123:502]	2019-04-26 13:45:29.219	F0:06:00:05:00:01
<input type="checkbox"/> RxSideA[192.168.248.149:502]	2019-04-16 09:19:27.074	F0:10:0A:9C:00:05:0A:07:D0:0F:A0:1F:4.
<input type="checkbox"/> RxSideA[192.168.248.149:502]	2019-04-16 09:19:26.018	F0:0F:0C:F3:00:05:01:7F
<input checked="" type="checkbox"/> RxSideA[192.168.248.149:502]	2019-04-16 09:19:24.763	F0:10:0A:9C:00:05:0A:07:D0:0F:A0:1F:4.
<input type="checkbox"/> RxSideA[192.168.248.149:502]	2019-04-16 09:19:23.706	F0:0F:0C:F3:00:05:01:7F
<input type="checkbox"/> RxSideA[192.168.248.149:502]	2019-04-16 09:19:18.373	F0:0F:0C:F3:00:05:01:7F

The detail view on the right shows expanded information for the selected entry, including the full timestamp and message details.

The Host Command Log can be downloaded as a CSV file for further analysis or recording purposes. Please note the Host Command log is continually updating, therefore the data downloaded as a CSV file is likely to include new data not shown on the display.



3. Menu Structure *continued*

3.7.3 Alarm Log Page

All device, network and *Master Station* alarms are recorded in the Alarm Log. Alarm events are shown in chronological order from newest to oldest. The log can be filtered by alarm type using the appropriate checkboxes or filtered for a specific device using the drop down box. The Alarm Log can record 1,000 alarms in a circular buffer where older entries are overwritten by incoming newer ones.

Selecting the icon next to the address will navigate to the applicable device or AIM page.

The screenshot shows the Alarm Log interface. At the top, there is a user profile 'User (User) Primary' and the date '15:27 Jan 25, 2019'. Below the title 'Alarm Log', there is a filter section with a dropdown menu 'Select...' and several checkboxes for alarm types. A table of alarm events is displayed below, with columns for Time, Address, Type, Side, Level, and Alarm. The Level column contains various icons representing different alarm types. A callout box points to the icon next to the address '10000' in the first row.

Time	Address	Type	Side	Level	Alarm
2019-01-25 15:12:18	10000		Side B	✓	Side B Door Open
2019-01-25 15:08:38	10000		Side B	⚠	Side B Door Open
2019-01-25 14:52:00	2	IQ2	Side A	✓	General Alarm
2019-01-25 14:52:00	2	IQ2	Side A	✓	Monitor Relay
2019-01-25 14:51:57	2	IQ2	Side A	🔧	General Alarm
2019-01-25 14:51:57	2	IQ2	Side A	⚠	Monitor Relay
2019-01-25 14:51:56	2	IQ2	Side A	✓	Comms Loss
2019-01-25 14:51:52	1	ROM	Side A	✓	General Alarm
2019-01-25 14:51:52	1	ROM	Side A	✓	Monitor Relav

The Alarm Log can be downloaded as a CSV file for further analysis or recording purposes.

The icon in the Level column indicates the type of alarm according to NE107.

- ✓ Normal
- ⚠ Function check
- 🔧 Maintenance required
- ⚠ Out of specification
- ✗ Failure



3.7.4 Request Password Reset Code

The Request Password Reset Code feature is only accessible through the *Master Station* local display interface.

Every effort should be made to ensure *Master Station* Admin login credentials are not lost. It is the users responsibility to monitor and maintain user accounts according to their site security policies.

If all Admin login credentials have been lost, the Rotork *Master Station* includes a feature to restore access. Pressing the Request Password Reset Code button will generate a unique code. Follow instructions in Section 3.1 to use this code.

 Request Password Reset Code

 Request Password Reset Code

Your Admin Reset Code is: !#~*<?\\€



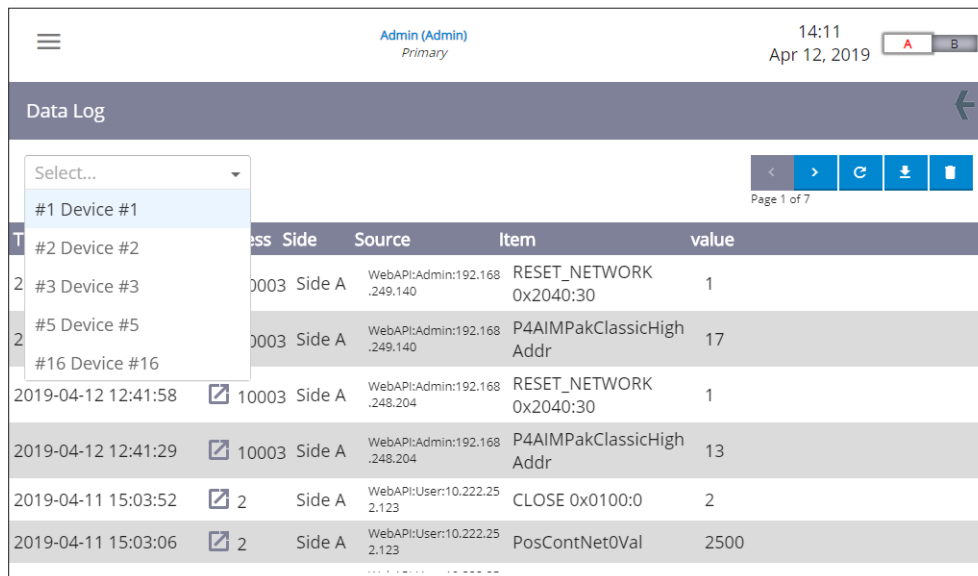
3. Menu Structure *continued*

3.7.5 Data Log Page

The Data Log is only accessible for Admin level operators through the *Master Station* web browser interface.

Events are recorded when accessing the *Master Station* through the web browser interface. Web API events do not appear in the Host Analyser or Host Command log as they are not in Modbus format.

The Data Log shows time and date stamped web API events in chronological order from newest to oldest. The log can be filtered by specific device using the drop down box. The Data Log can record 10,000 events.



Each event includes the address, *Master Station* side, source (IP address), item (setting) and the new item value.

Addresses within the 10000 range indicate an event occurring with a *Master Station* AIM. Other addresses relate to a device connected to the *Master Station*.

Address	Message
10000	CPU
10001	AIM slot 1
10002	AIM slot 2
10003	AIM slot 3
10004	AIM slot 4

Selecting the icon next to an address will navigate to that specific device or AIM page.

The Data Log can be downloaded as a CSV file for further analysis or recording purposes.




3.7.6 Download Syslogs

The Download Syslogs feature is only accessible for Admin level operators through the *Master Station* web browser interface.

Clicking the Download Syslogs button will cause a .TGZ file to download from the *Master Station*. Rotork will advise when to use this feature.

[Download Syslogs](#)

Host Communications

Section	Page
 4. Ethernet Communications to the Rotork <i>Master Station</i> _____	32
4.1 Default Host Ethernet Settings – Host Ports (Ethernet 1 and 2) _____	33
4.2 Setting Up the Ethernet Comms – Host Ports (Ethernet 1 and 2) _____	33
4.3 Setting Up the Ethernet Service Port _____	36
4.4 Ethernet Security _____	37
 5. Serial Communication to the Rotork <i>Master Station</i> _____	45
5.1 Serial Connection to the <i>Master Station</i> _____	46
5.2 Host Serial – Port Function _____	50
5.3 Host Serial – RS-485 Termination _____	50
 6. Hot Standby _____	51
6.1 Hot Standby Change Over _____	51



4. Ethernet Communications to the Rotork Master Station

The *Master Station* CPU module includes three Ethernet ports for communication by Modbus TCP/IP to a host connection or by https to web pages. Ethernet 1 and Ethernet 2 are dedicated host communication ports, and are intended for permanent host communication connection. The service port is intended for temporary connection for configuration and troubleshooting. The service port requires the display to be lifted for use, the display can be closed while the host ports are in use. Both host ports will have the same IP settings, the service port should be set to different IP settings such that it is isolated from the host network.

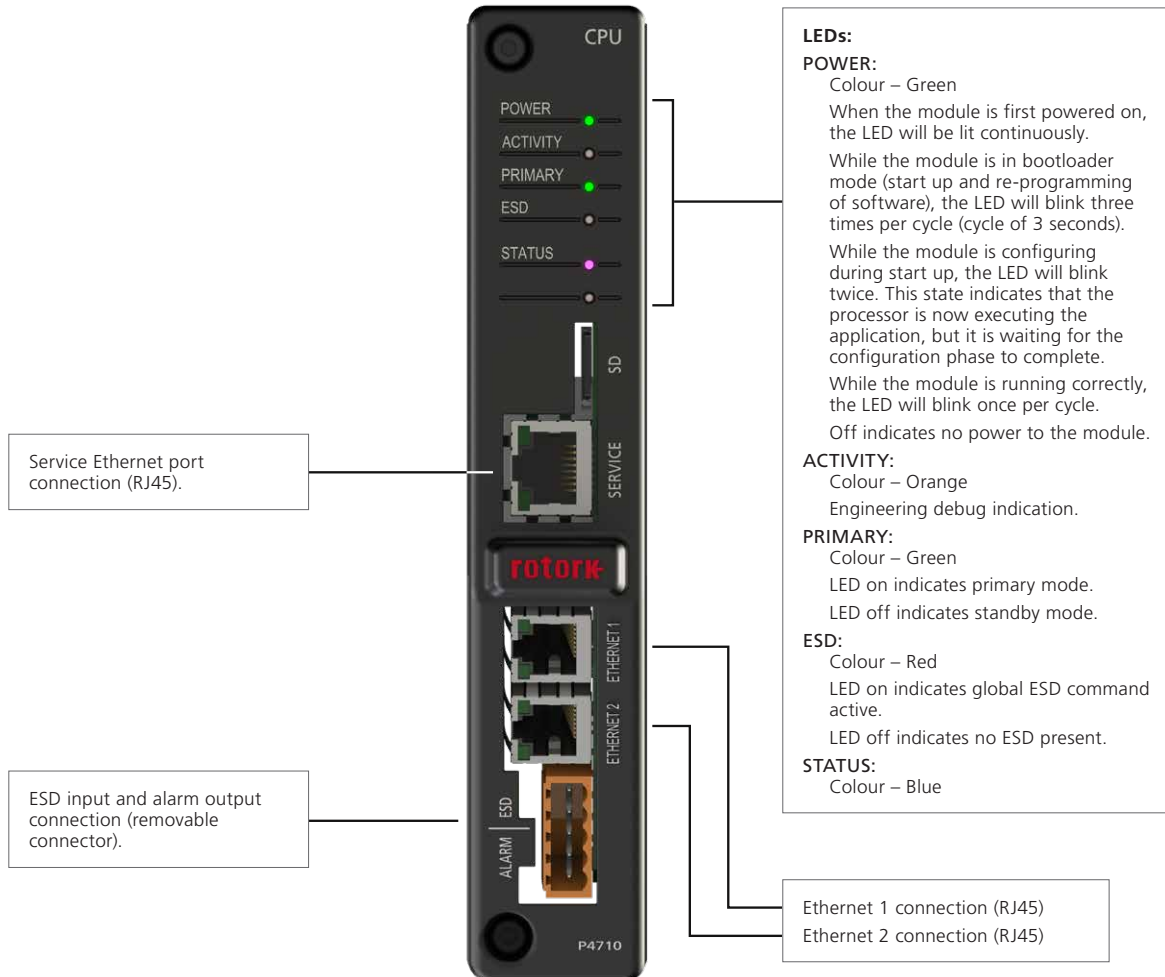


Fig 4.1: CPU module front face

A hot standby *Master Station* will include two CPU modules, one each side, with two Ethernet host communication ports per module. A total of four Ethernet communication ports are available for host connection.



4.1 Default Host Ethernet Settings – Host Ports (Ethernet 1 and 2)

The *Master Station* is ready to connect to a DCS via Ethernet for control and monitoring data from FCUs. The IP address is already set to a default value, but can be changed at any point within the *Master Station* Ethernet Setup menu.

Default Ethernet port settings

The default Ethernet parameters for the host ports of each CPU module are given below:

Default IP address (Side A)	10	200	1	1
Default IP address (Side B)	10	200	1	2
Default Subnet mask	255	255	255	0
Standby action (hot standby only)	Active			

The IP address settings are static, the address cannot be set dynamically.



Ensure the service and host networks are on different subnets.

4.2 Setting Up the Ethernet Comms – Host Ports (Ethernet 1 and 2)

Ethernet connections require 10/100/1000BaseT Ethernet switches to connect the system together. Patch cords connect the ports on the *Master Station* to the switches. Independent highways are possible by using separate switches on each highway.

Side A is the primary side by default when a hot standby *Master Station* is powered up.

Automatic change over of standby to primary will occur if both Ethernet connections to the primary are disconnected. Refer to Section 6.1 for setting details that control hot standby changeover.

It is possible to change the IP address on either side, but the two ports of each CPU module always have the same address. If Side A and Side B both use the same IP address and are connected to the same highway, it is important to set the *Standby Action* to *Passive*.

The two Ethernet inputs are logically combined within the *Master Station*. An alarm read over either highway is effectively read over both and there is only one alarm database.

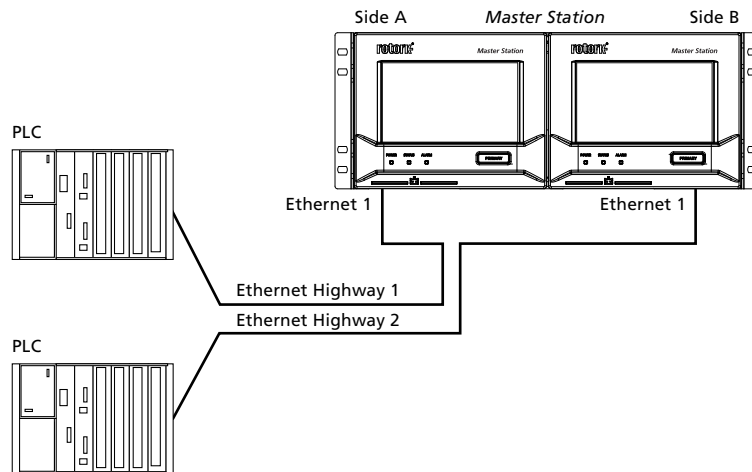


4. Ethernet Communications to the Rotork *Master Station* continued

There are various topologies for connecting to Ethernet networks. The diagrams show a hot standby *Master Station* configuration but a single *Master Station* topology can be visualised by removing the connections to Side B.

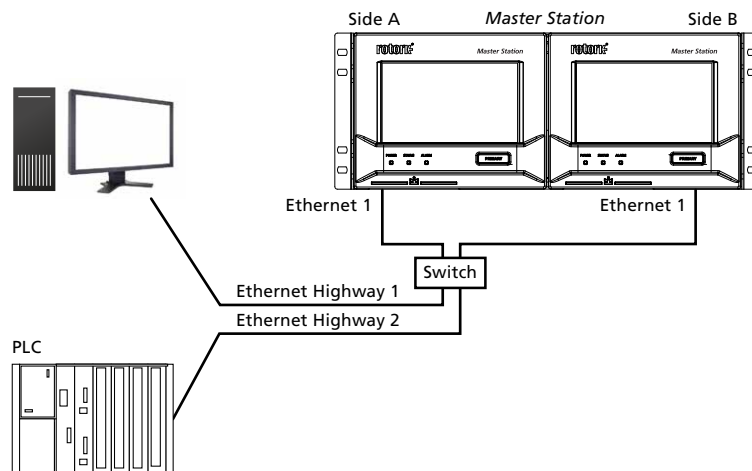
Separate LAN Connections

Comprising two separate LAN connections, one to either side of the *Master Station*. The IP address for each side of the *Master Station* can be the same or different. Host devices can only communicate to Side A or Side B if they have a physical connection. *Standby Action* can be configured to *Active*.



Partial Redundancy

Comprising two LAN connections linked together with an Ethernet switch. The IP address for each side of the *Master Station* can be the same if *Standby Action* is configured to *Passive*. Host devices can communicate to either side of the *Master Station*.

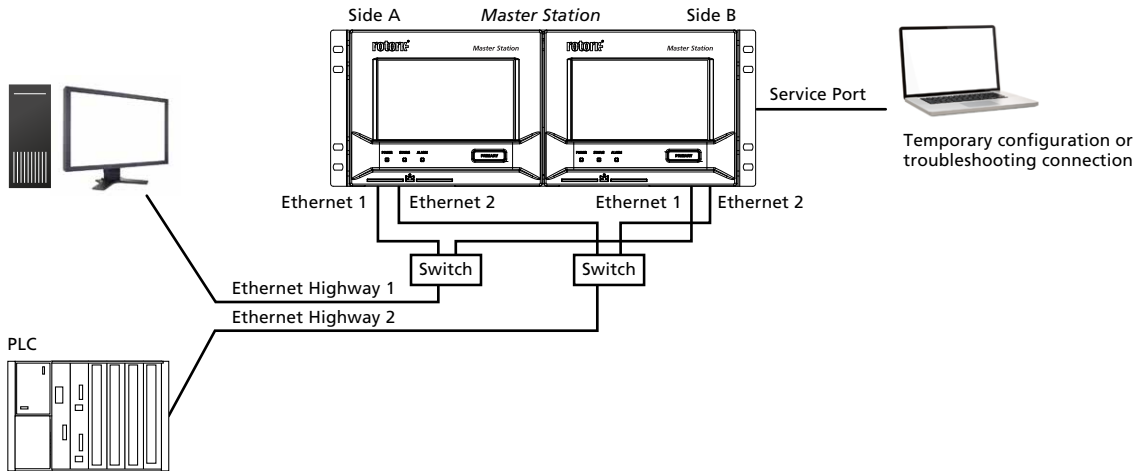




Full Redundant Host Connection

Comprising two separate LAN connections, each linked to both sides of the *Master Station* through a managed Ethernet switch. Managed Ethernet switches must support rapid spanning tree protocol. Managed switches of this type prevent Ethernet broadcast storms, where messages are re-circulated continuously.

The IP address for each side of the *Master Station* can be the same if *Standby Action* is configured to *Passive* or different if *Standby Action* is configured to *Active*. Host devices can communicate to either side of the *Master Station*.



The above arrangement ensures either host can always communicate with the *Master Station* in control of the loop.

Ethernet switches must be a managed type and support either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).



4. Ethernet Communications to the Rotork *Master Station* *continued*

4.3 Setting Up the Ethernet Service Port

Each *Master Station* CPU has a dedicated Ethernet service port that is physically and logically isolated from the host Ethernet ports. Isolation permits a service or maintenance user connection to the *Master Station* for diagnostics purposes without connecting to the host LAN. The service port has separate settings to prevent conflicts with the host Ethernet ports.

The default service port Ethernet parameters are shown below:

Default IP address (Side A)	10	201	1	1
Default IP address (Side B)	10	201	1	2
Default Subnet mask	255	255	255	0

The IP address settings are static, the address cannot be set dynamically.

Service and host Ethernet ports must be configured to operate on different subnets.

Configuring the service and host Ethernet ports for the same subnet will cause the following issues:

- If they are physically connected to different Ethernet networks the *Master Station* would not know which port to reply on
- If they are physically connected to the same Ethernet network the *Master Station* would not know which port to reply on. The reply message will still reach the destination however this network configuration is not advisable

The same subnet mask can be used for host and service Ethernet (255.255.255.0) however different networks (subnets) are necessary. For example: 10.**200**.1.1 to 10.**200**.1.255 for host and 10.**201**.1.1 to 10.**201**.1.255 for service.



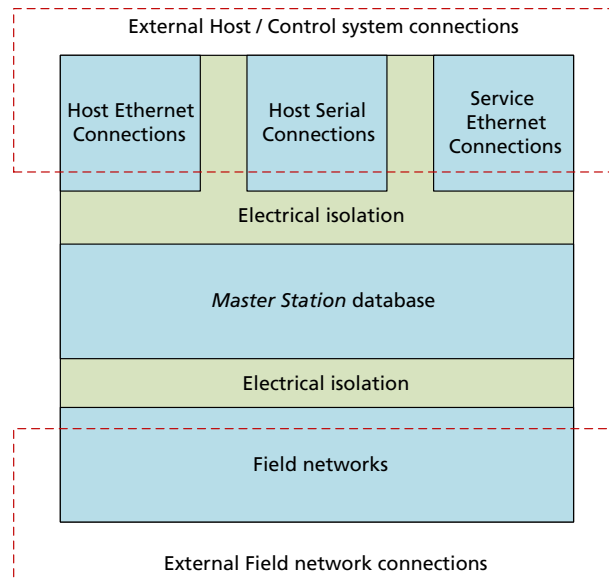
4.4 Ethernet Security

Always consider security of the *Master Station* when connecting it to an Ethernet network.

The user should ensure the Ethernet infrastructure is able to protect the *Master Station* from unauthorised access.

The *Master Station* has a number of security features that can be employed to harden the system against cyber threats, these are described in this section along with the security features expected from the overall network into which the *Master Station* is installed.

The *Master Station* is the interface between the plant control system and field units. The field units are connected to field networks that are physically (electrically) isolated from the control system network. Host connection to the *Master Station* is via Ethernet (or optional serial connection).



Master Station security features form a small part of the overall security strategy of the plant.

It is important to involve the local plant or site IT department in conversations about security of control system networks. The local IT department should be involved with securing access between the business network and the control system network. IT professionals will already be utilising cyber security measures to protect the business networks.

Coordination between IT and the control system team is important to ensure cyber security is managed properly and functions for all networks on site. Security policies may require modification if the exact same policy is not appropriate for the control system and business network.

For example, IT departments can use remote access to periodically maintain and update devices on the business network, these routine updates could disrupt the control system network. Control system updates to software and configuration must be strictly controlled and remote connection like this could introduce security risks to the control system.

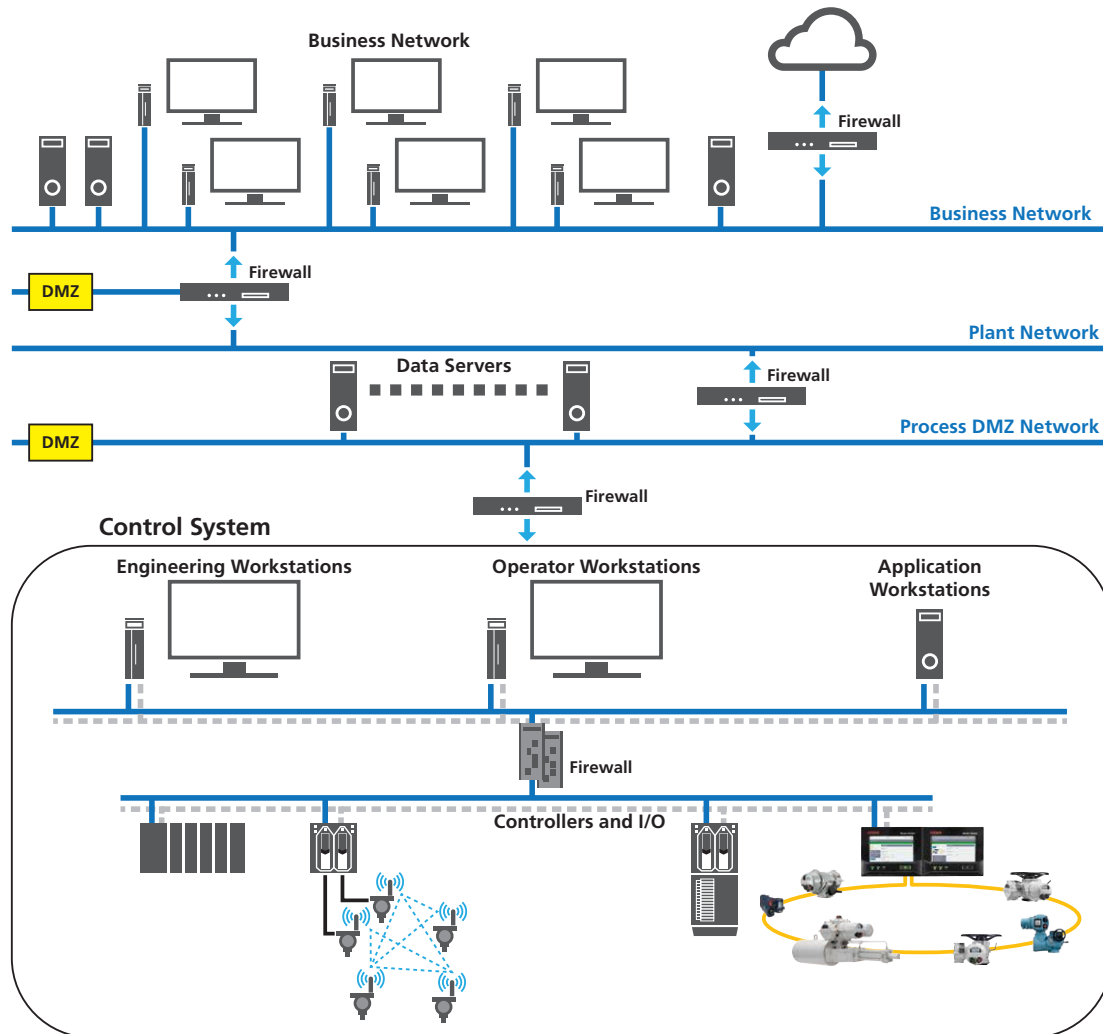
The traditional priority for an IT department managing a business network is confidentiality, integrity and availability of data in the system. The same priority list is reversed for a control system network as availability of the data is the most important. The security of the system should not adversely affect the availability of data to users that need it. Confidentiality is less important as most of the control system data means nothing outside of the system.

The security guidance in this document is intended to help the user implement and maintain reasonable security of the *Master Station*, however, no security implementation can guarantee to protect against all existing, new or previously unknown threats. Rotork does not guarantee that adherence to these and any other security recommendations will protect the *Master Station* from security breaches and any subsequent impact on process in which the *Master Station* and associated ancillary components are involved with.



4. Ethernet Communications to the Rotork Master Station *continued*

4.4.1 Control System Architecture



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 DMZ (demilitarised zone) 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 have to do this by accessing 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, historians, web servers and secured computers.

Examples of security policies that can be employed on site:

- All control systems must be segmented from the business network using a firewall and a DMZ network

Recommendation: All control systems must be segmented from the business network using a firewall/UTM (Unified Threat Management) device which has built-in Intrusion Prevention, Intrusion Detection System and a two-tier DMZ network

- All users should be trained on the site security procedures and policies
- Different job and responsibility level users should have different user names and passwords, preferably per individual

Recommendation: Each user should have an individual user account with a strong password (minimum of 8 characters using a mix of upper case and lower case alphanumeric characters)

- Default passwords for user accounts must be changed during system installation or site acceptance tests

Recommendation: The end-user should always change the default password to a suitable strong password

- Security events should be logged in a security audit file, these include invalid logins and changes to user accounts



4.4.2 Security Environment Expected for the *Master Station*

The *Master Station* should be installed in an environment with suitable IT security protection to safeguard against internet attacks.

Protection should include (but not limited to) DMS and firewalls between the *Master Station* control system network and the plant network. A DMZ is an effective method of protection by separating networks.

Direct connection between the *Master Station* and control system host is expected. Therefore, a DMZ and firewall is not required between these devices.

4.4.3 Defence in Depth

A defence in depth strategy utilises multiple layers of security so that a threat has to overcome more than one security mechanism. Defence in depth has 3 fundamental types of security safe guards:

- 1) Physical controls – the physical access of a device and the protection of the device. Normally achieved through protective measures such as site perimeter fences, locked control rooms and cabinets plus deterrence measures such as CCTV.
- 2) Technical controls – content access restriction of the system or device.
- 3) Administrative controls – policies and procedures of the organisation.

Physical Controls

Physical security intends to prevent unauthorised users accessing and tampering with networked devices, like a *Master Station*. The *Master Station* host Ethernet connections, service Ethernet connection and micro SD card slot are all accessible when the *Master Station* display is lifted. There is no lock on the *Master Station* to prevent the display from being lifted, therefore, external physical security measures must be employed.

The *Master Station* should be installed in a locked enclosure (cabinet) or an access controlled location (secure room). Access control to the enclosure or location would typically take the form of locks, fences, identity badges for personnel and general security awareness of the personnel.

Personnel should be wary of their surroundings when viewing data and entering user account details.

Restricting access to network cabling outside of the protected area is strongly advised. The topology of the network connections should be reviewed to ensure there is no easy connection point for unauthorised users.

The network topology should ensure that only authorised devices can connect to the network and connectivity of those devices is restricted to the appropriate network segment.

Correct labelling of control system components aids in preventing the accidental connection of unauthorised equipment.

Technical Controls

Technical controls prevent access by unauthorised users to the contents or data of the *Master Station*. These controls include:

- 1) Limiting the types of connections that may be established
- 2) Disabling Ethernet ports
- 3) Whitelisting of IP and MAC addresses
- 4) Use of HTTPS for web pages
- 5) Web page login security
- 6) Appropriate access levels for different users.
- 7) Restrict ICMP flooding, over sized ICMP packets and TCP floods by configuration policies on the Firewall/UTM devices.
- 8) Configure IPS/IDS settings to restrict scanning attacks, enumeration and Dos/DDos attacks.
- 9) In the customer network, if Modbus Port is listening on TCP 502, please disable other non-standard ports (i.e. 50000 series ports).
- 10) User audits should be conducted at least once a month. This is required to double check who has access to Rotork *Master Station* systems.
- 11) Internet connections to the *Master Station* must be established using a secure VPN tunnel.
- 12) The client system used when connecting to the *Master Station* must have the latest operating system security patches installed, up-to-date anti-virus software and up-to-date web browser software. The end-user should not access the *Master Station* using a non-standard or legacy web browser.



4. Ethernet Communications to the Rotork *Master Station* continued

Modbus TCP

Modbus TCP has no inherent security features and therefore relies on other methods for protection. Security methods can include industrial network firewalls that allow only Modbus TCP protocol traffic to the device and the whitelisting feature within the *Master Station*. Deep Packet Inspection (DPI) is a form of network traffic filter that can be used to examine the data part of a packet as it passes an inspection point, this could be employed for Modbus TCP inspection but would be external to the *Master Station*.

Accessible TCP and UDP Ports

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the core protocols utilised 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 following TCP and UDP ports are accessible over *Master Station* Ethernet connections:

Application	Protocols	Ports	Comments
HTTP: <i>Master Station</i> webserver	TCP	80	HTTP interface will not do anything other than redirect to the HTTPS interface.
HTTPS: <i>Master Station</i> 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 <i>Master Station</i> .

No other ports are available.

Ethernet Port Security Settings

The physical Ethernet ports (host and service) can be enabled or disabled within the *Master Station* security settings. Host port settings act on Ethernet 1 and Ethernet 2 at the same time. Enabling will cause both to be operational, disabling will prevent operation on both ports.

Disable the Ethernet ports if no Ethernet connections are required for the *Master Station*. The service port can be disabled independently from the host Ethernet ports. Host and service Ethernet ports are identical however the service port (if enabled) is always available and will not cause a primary side switch when unplugged from the primary side of a hot standby *Master Station*.

There are separate settings for whitelisting the IP and MAC addresses for the host and service ports, whitelisting can be enabled and disabled for IP and MAC addresses as appropriate.

Host Ethernet Ports Security Setup
^

Save

Enable Host Ethernet Ports Enabled Disabled

Enable Host Ports IP Address Whitelist Enabled Disabled

Enable MAC Address Whitelist Security Enabled Disabled

Service Port Security Setup
^

Save

Enable Service Ethernet Port Enabled Disabled

Enable Service Port IP Address Whitelist Enabled Disabled

Enable Service Port MAC Address Whitelist Enabled Disabled

4. Ethernet Communications to the Rotork *Master Station* continued



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.

Service Port Security Setup^

Save

Enable Service Ethernet Port	<input checked="" type="radio"/>	Enabled	<input type="radio"/>	Disabled
Enable Service Port IP Address Whitelist	<input type="radio"/>	Enabled	<input checked="" type="radio"/>	Disabled
Enable Service Port MAC Address Whitelist	<input type="radio"/>	Enabled	<input checked="" type="radio"/>	Disabled
IP Address		- . - . - . -		
IP Address		- . - . - . -		
IP Address		- . - . - . -		
IP Address		- . - . - . -		
IP Address		- . - . - . -		
MAC Address		- : - : - : - : - : -		
MAC Address		- : - : - : - : - : -		
MAC Address		- : - : - : - : - : -		
MAC Address		- : - : - : - : - : -		
MAC Address		- : - : - : - : - : -		

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.

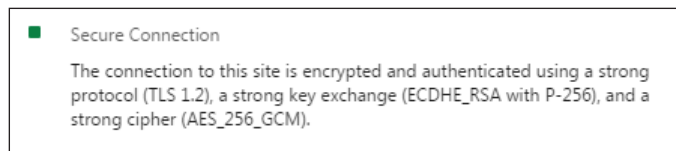
Service and host ports that are not connected to the same physical network must be configured for different IP subnets to avoid routing issues.

Security Certificate

On the internet, an SSL certificate is primarily used to verify that a site is genuine. This means the website can be trusted. Certificates are obtained from certificate authorities and can be self-signed, publically signed (by third party companies), or privately signed (internally by a company).

Advice should be taken from the plant or site IT department on how to obtain a certificate if required.

Even without a certificate installed, *Master Station* data access through a web browser is still encrypted as shown by this output from Google Chrome:



If you are unable to install a certificate specific to the *Master Station*, then you must acknowledge the risks involved, and proceed through your browser's warnings. If the connection is physically one to one between the *Master Station* and the PC, risk is inherently low as the connection route is known.

Operators using Mozilla Firefox may encounter time out errors when loading *Master Station* web pages. The time out error occurs if multiple *Master Station* security certificates are cached in the browser. Rotork advise using an alternative browser. If this is not possible, contact Rotork for guidance to resolve the Mozilla Firefox time out issue.



4. Ethernet Communications to the Rotork *Master Station* continued

Web Page User Account Management

Web browser access to the *Master Station* interface is via user accounts. Management of the user accounts forms an important part of securing the *Master Station*.

There are three access levels for the *Master Station* interface:

- Viewer
- User
- Admin

Viewer – default access on the local *Master Station* display, no password required. Web browser access requires login credentials for all levels of access including viewer level. Viewer permits read only access to some *Master Station* settings and status information. Not all settings are visible at Viewer level. Viewer accounts are only intended for operators that need to check status of the *Master Station* or connected FCUs.

User – password protected on the local *Master Station* display and web browser interface. User permits read only access to all *Master Station* settings plus operation and configuration of connected FCUs. User accounts are intended for operators that need control of FCUs or change device configurations.

Admin – password protected on the local *Master Station* display and web browser interface. Admin permits write access to all settings within the *Master Station*. Admin accounts are intended for *Master Station* commissioning and control system management only.

At least one admin level account must be present on the *Master Station*.



Only use Admin level access when required to perform an Admin level task. Always use the appropriate permission level access for the activity being performed.



Always log out of the *Master Station* after use. There is an automatic session timeout feature after a period of inactivity but it is more secure to manually log out after every session.



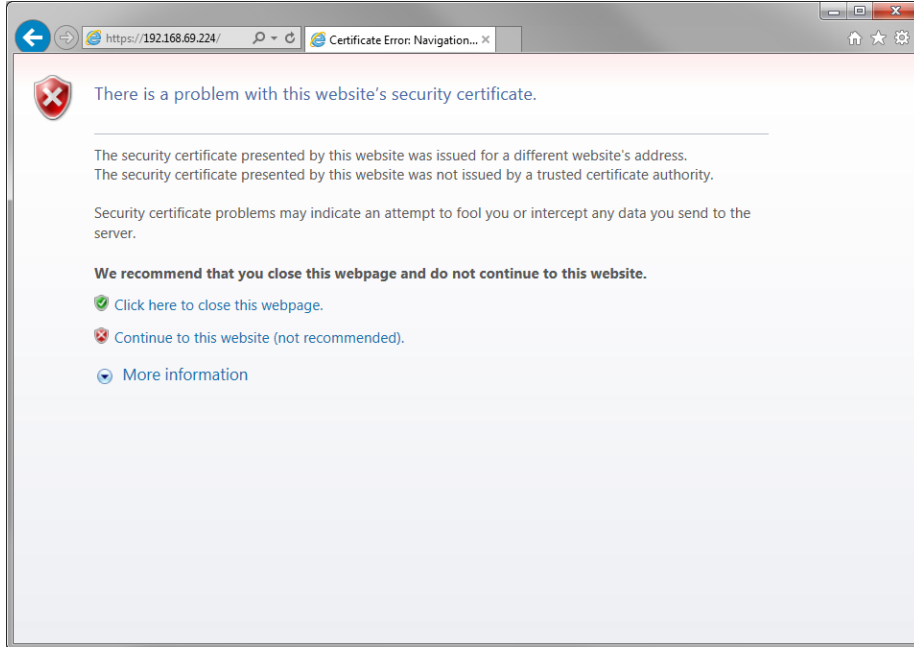
Accessing the *Master Station* through a web browser relies on authentication via security token. The token is issued when logging in and removed when refreshing the browser window or logging out. Refreshing the browser is not necessary as any dynamic information will automatically update periodically.



Accessing the *Master Station* through Web Browser

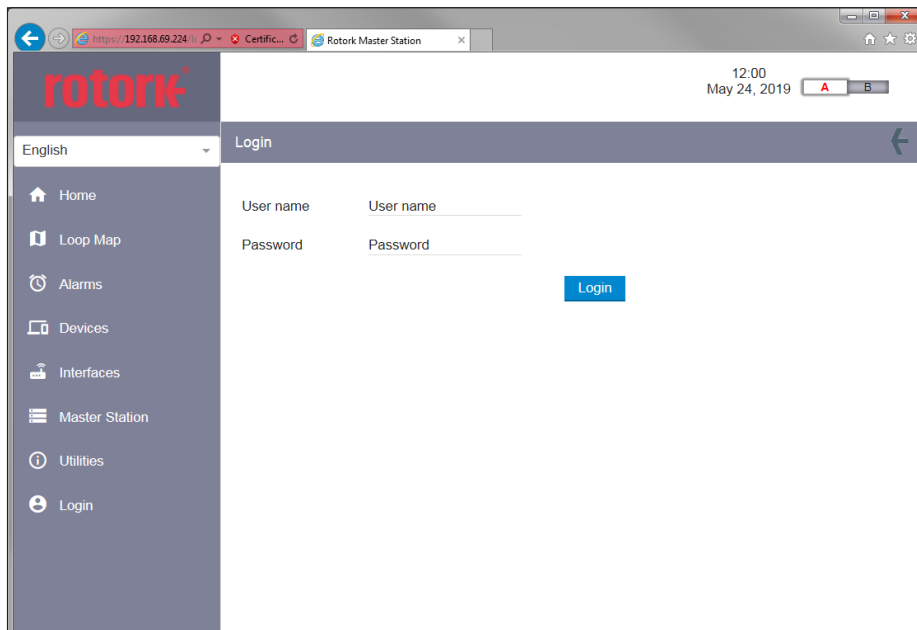
The web interface will work with most modern web browsers, this includes IE 9 and later, Firefox 2.0 and later, and all versions of Google Chrome.

Open a web browser and enter the IP address of the *Master Station* in the address field. If you have not loaded the security certificate you may be presented with a warning like this:



Only continue to the website if you are confident connection to the correct *Master Station* is made.

With the security certificate authenticated or the browser warning accepted, the login page of the *Master Station* will be visible.



Incorrect login credentials will show a warning message:





4. Ethernet Communications to the Rotork Master Station *continued*

Login Security

There is no default Admin account password for the *Master Station*. Each *Master Station* has a unique user name and password programmed at the factory. The user name and password is shown on the *Master Station* test certificate, supplied with the unit.

Rotork Controls Ltd
Bath,
England
BA1 3JQ


rotork

MASTER STATION TEST CERTIFICATE

Serial Number: Z123456789 **Test Date:** 08.05.2019
Customer: CUSTOMER
Order Number: PO12345

MASTER STATION SPECIFICATION

SIDE A		SIDE B	
Power Supply	PSU (100-240v AC)	Module 5	P4720 PAKSCAN CLASSIC FIELD NETWORK
Module 1	P4720 PAKSCAN CLASSIC FIELD NETWORK	Module 6	NOT FITTED
Module 2	NOT FITTED	CPU	60 CHANNEL
CPU	60 CHANNEL	Module 7	P4724 MODBUS FIELD NETWORK
Module 3	P4724 MODBUS FIELD NETWORK	Module 8	P4727 MODBUS HOST SERIAL
Module 4	P4727 MODBUS HOST SERIAL	Power Supply	PSU (100-240v AC)



BUILD CODE
3 1 1 B 1 4 7 1 B 1 4 7 1

MASTER STATION TYPE
(HOT STANDBY MASTER STATION)

BUILD DETAILS

Module	Module Serial Number	SW Version	Module	Module Serial Number	SW Version
PSU (A)	4018B.A0630001501=154295	---	Module 5	1840B.A0630001601=154255	209
Module 1	1840B.A0630002101=154255	209	Module 6	NOT FITTED	---
Module 2	NOT FITTED	---	CPU (B)	4118B.A0630001601=154224	V034
CPU (A)	4118B.A0630008701=154224	V034	Module 7	4818B.A0630004502=12401	105
Module 3	4818B.A0630003302=12401	105	Module 8	1840B.A063000401=154307	105
Module 4	1840B.A0630004501=154307	105	PSU (B)	4018B.A0630001601=154295	---
Backplane	2417B.A0630009903=142051	---			

DEFAULT LOGIN INFORMATION


Side	Username	Password
SIDE A	Z123456789	LEq4Sen2~
SIDE B	Z123456789	LEq4Sen2~

CPU UNIQUE ID

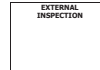
Side	Unique Identification
SIDE A	e8b346815052604
SIDE B	c1386c913189104

Tester ID: GSTA1

This Rotork Master Station has been manufactured within the Rotork ISO 9001:2008 Approved Quality System



PRODUCTION COMPLETE



EXTERNAL INSPECTION

DOCS136-1 03/17

DEFAULT LOGIN INFORMATION

	Username	Password
SIDE A	Z123456789	LEq4Sen2~
SIDE B	Z123456789	LEq4Sen2~

The example above is not a real user name and password.

It is important to change the default Admin login credentials during system installation or site acceptance tests to maintain the security of the *Master Station*.

Rotork keeps a record of the original user name and password for every *Master Station*. Rotork does not have an overriding password to gain access to a *Master Station*. Rotork cannot access the *Master Station* if a user changes the password and does not communicate the change to Rotork.

5. Serial Communication to the Rotork Master Station



The Modbus Host Serial AIM (P4727) is required for host serial communications. Host Serial is an optional AIM that should be ordered as part of the *Master Station*. It is possible to retrofit this AIM.

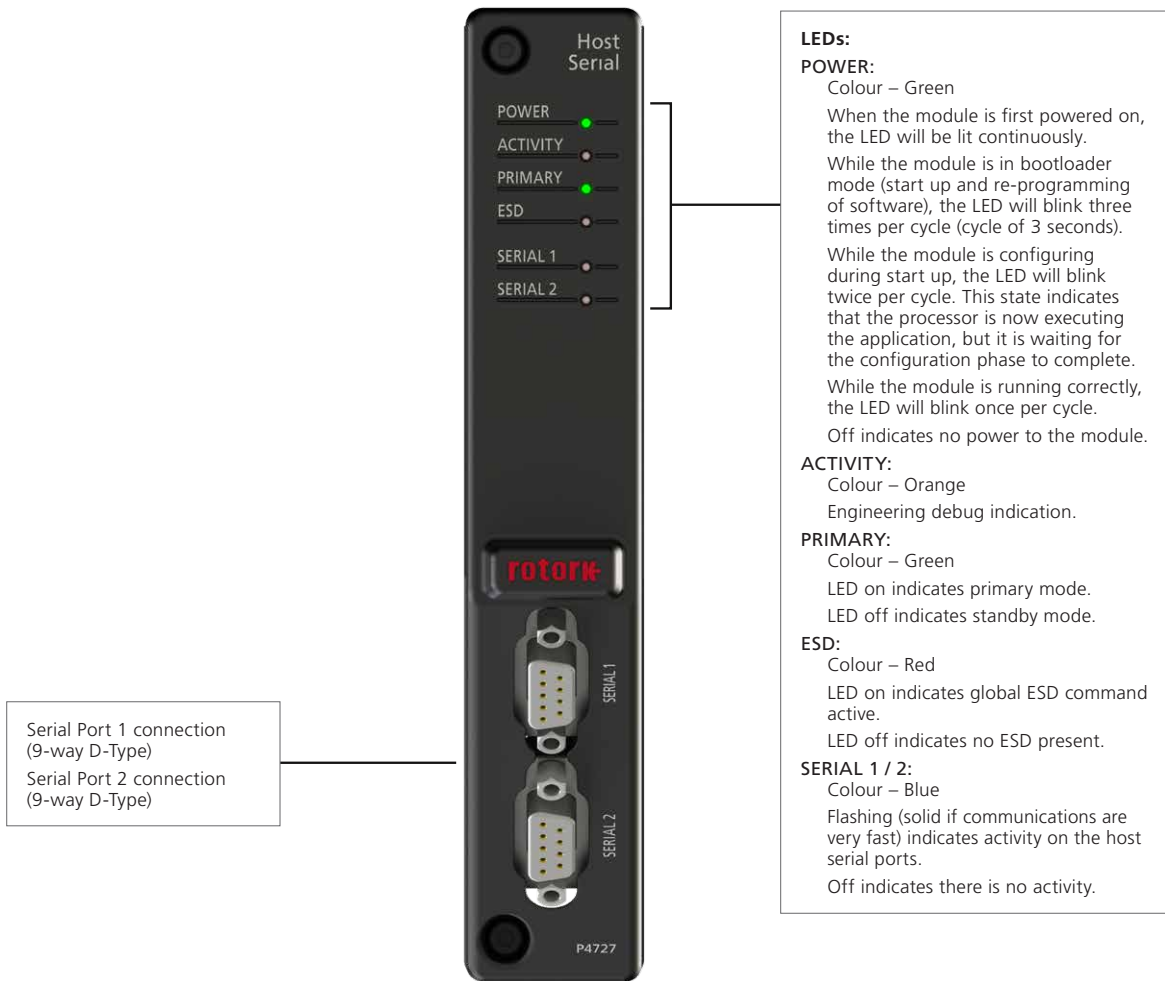


Fig 5.1: Host Serial module front face

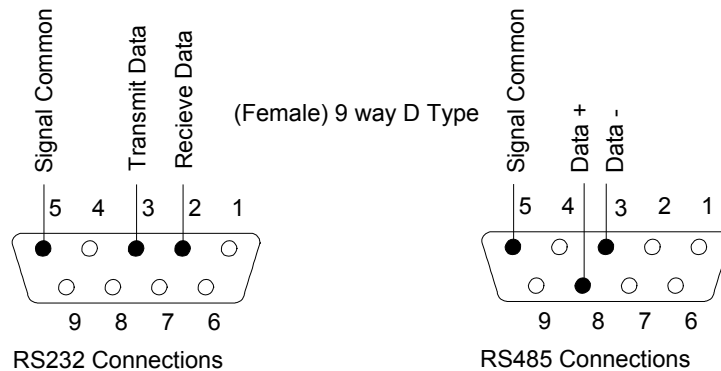


Fig 5.2: Master Station serial communications connections



5. Serial Communication to the Rotork Master Station *continued*

The Host Serial AIM includes two serial communication ports for connection to the host system. Each port can be configured for RS-232 or RS-485 using the DIP switches included on the Host Serial AIM. For instructions on AIM removal and changing DIP switch position, refer to PUB059-050.

A hot standby *Master Station* will include two Host Serial AIMs, one for each side, providing four serial port connections in total. DIP switch setting for Serial 1 must be the same for both sides. DIP switch setting for Serial 2 must be the same for both sides.

Serial communication is half-duplex.

RS-485 is a 2-wire system with configurable line termination. Biasing and termination resistors can be switched in from the Host Serial setting menu on the *Master Station*. Termination is 120 Ω passive with 1 k Ω biasing.

5.1 Serial Connection to the *Master Station*

Suggested serial port settings for a single (also applicable for each side of a dual) and each side of a hot standby *Master Station* are shown below:

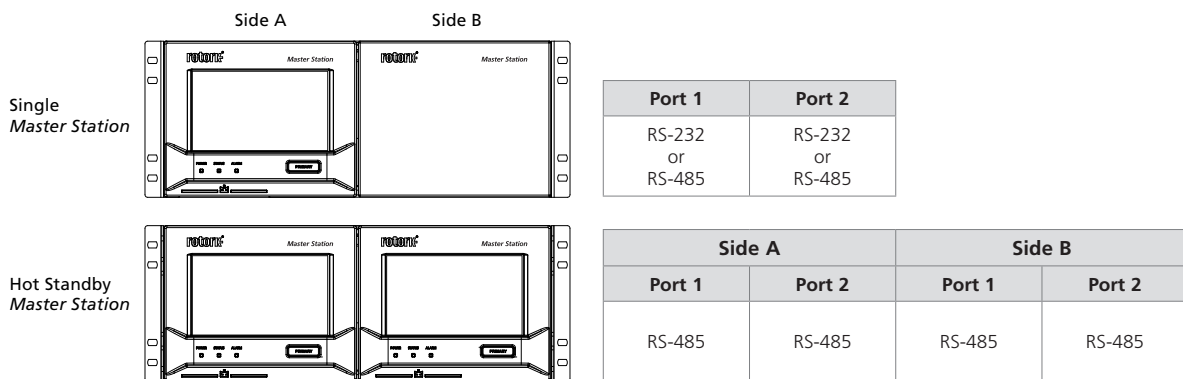


Fig 5.1.1: *Master Station* serial communications

Serial communication to a single *Master Station* can be linked to the host system as shown below. Hot standby *Master Station* configurations require more complex connection arrangements.

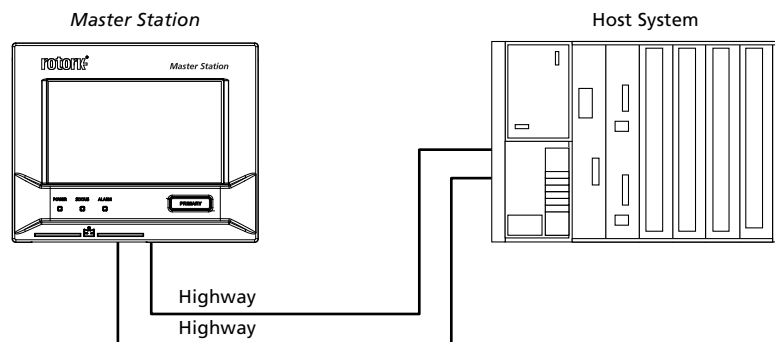


Fig 5.1.2: *Single Master Station* serial communications

Single or redundant communications can be used on either multi-drop or dedicated highways. Database information remains the same.

When redundant communications are employed (see Fig 5.1.2); the two highways access Serial 1 and Serial 2. The data behind these ports is designed to allow communication to two separate host systems or a single host on redundant highways. The two ports are effectively handled by two independent data bases each fed with information from the connected FCUs. Care must be taken when handling latched alarms in the *Master Station* databases. Either link the two ports by setting Port Alarms to *Linked* in the Modbus Host Common Settings or ensure that all alarms are accepted on both highways.



- **Single Host - RS-485 (2-wire) communications**

RS-485 enables multi-drop communication to multiple devices on one data highway. One host system can be connected to 32 *Master Station* RS-485 ports (more are permitted with repeaters). The *Master Station* only supports 2-wire RS-485, a single pair of wires for transmitting and receiving data. Highway extension is achieved external to the *Master Station* using additional cabling.

Wiring a hot standby *Master Station* to a multi-drop highway will send data to Side A and Side B. It is important to set Serial 1 Standby Mode and Serial 2 Standby Mode on each side to *Passive* to prevent duplicate replies corrupting data.

If a Serial Host AIM fails, primary control will automatically switch to the standby side. Automatic switching will not occur if the communication highway from the host system to *Master Station* is broken. Control of any *Master Station* beyond the failure point is not possible.

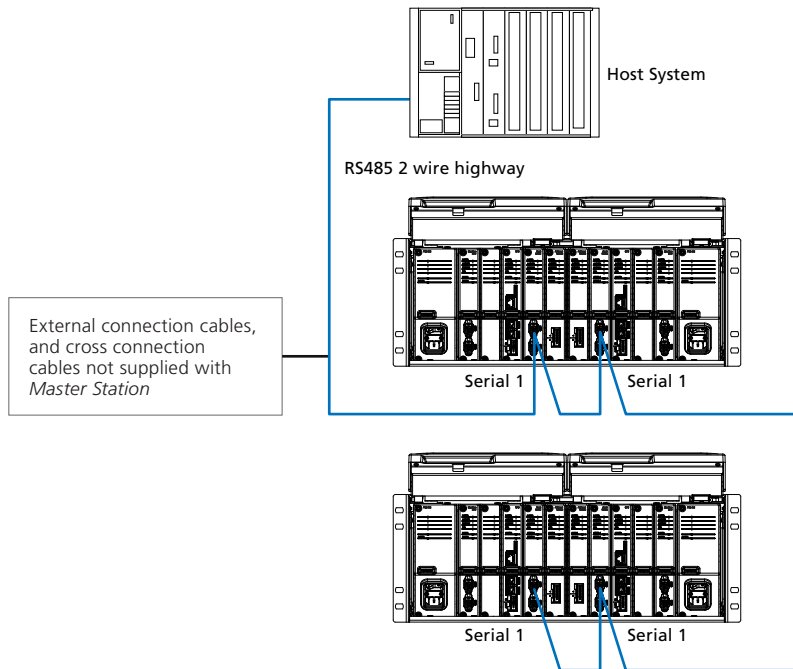


Fig 5.1.3: 2-wire RS-485 single highway



5. Serial Communication to the Rotork Master Station *continued*

- **Twin host – RS-485 (2-wire) communications**

Sometimes two host systems (e.g. PLC and In-Vision) are connected to one or more hot standby *Master Station* units. Two hosts offer redundancy of the host controller and the *Master Station* units. Two RS-485 highways are required for redundancy, independently connected to Serial 1 and Serial 2 of each Host Serial module. Highway extension is achieved external to the *Master Station* using additional cabling.

Serial 1 Standby Mode and Serial 2 Standby Mode on each Host Serial AIM should be set to *Passive* to avoid duplicate reply messages. If a host system or the communication highway between the host and *Master Station* fails, communication will be lost. The second host will continue communication with the *Master Station*. As each host requires full access to present alarms, Port Alarms should be set to *Separate*.

Commands from either host system (PLC or In-Vision) are not prioritised and therefore have equal weighting.

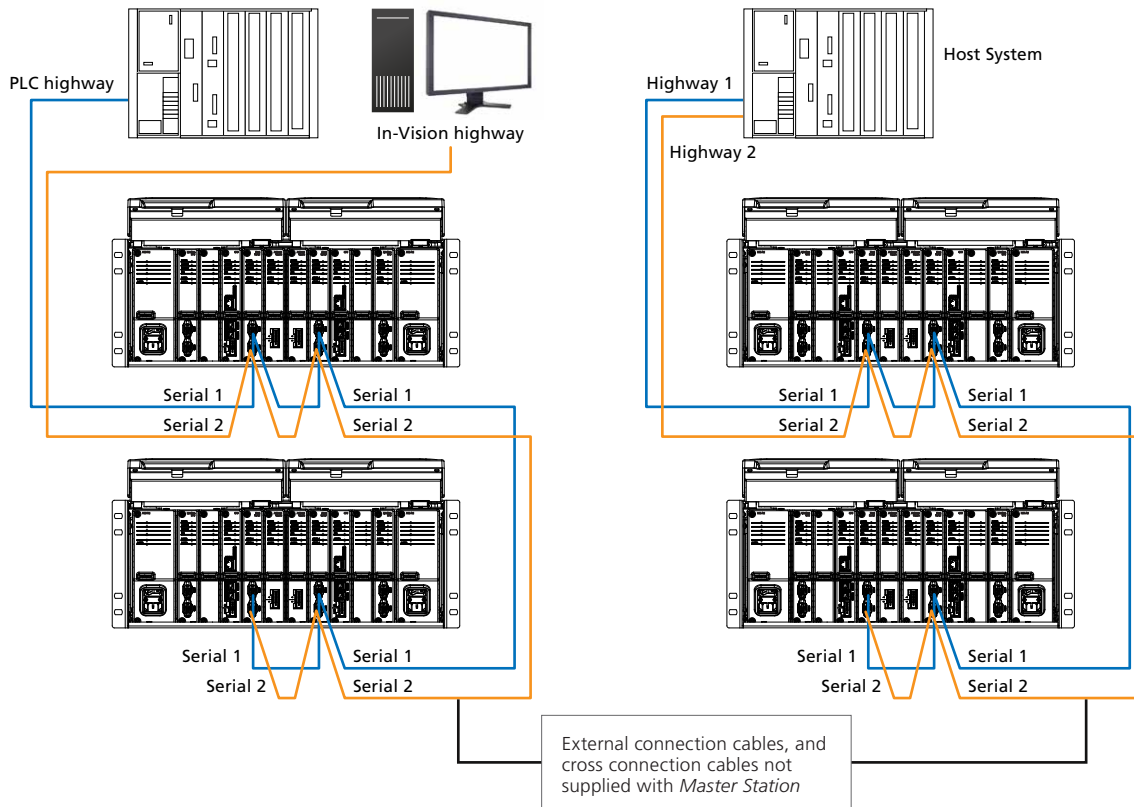


Fig 5.1.4: Twin host, single RS-485 comms

Fig 5.1.5: Single host, dual redundant RS-485 comms

- **Single host – dual redundant RS-485 (2-wire) communications**

A single host connected with two separate highways offers true redundancy for the *Master Station*, host interface and serial communication cabling. Serial 1 Standby Mode and Serial 2 Standby Mode on each Host Serial AIM should be set to *Passive* to avoid duplicate reply messages and data corruption. Port Alarms should be set to *Linked* to prevent repeat collection of alarms when changing communication highway.



- **Single host – dual RS-232 communications**

RS-232 is a point to point means of communication. One port on the host system must connect to one port on the *Master Station*. Two RS-232 data highways from the host system are required for a hot standby *Master Station*. One highway should connect to Serial 1 of Side A and the second highway should connect to Serial 1 of Side B. RS-232 should only be used if a single field network and *Master Station* need to be supervised. RS-232 does not permit multi-drop communications to more than one *Master Station*.

The host system determines which output port and highway to use, therefore defining which side of the *Master Station* to communicate with. Serial 1 Standby Mode should be set to *Active* for Side A and Side B of the *Master Station* to ensure an answer is always returned to the host system. Only the side in primary mode will action commands issued by the host system.

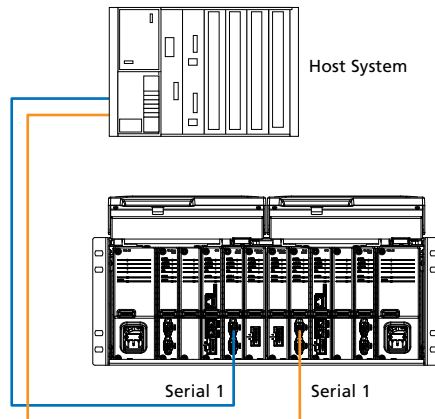


Fig 5.1.6: Single host, dual redundant RS-232 comms

If a Serial Host AIM fails, primary control will automatically switch to the standby side. Automatic switching will not occur if the communication highway from the host system to the *Master Station* primary side is broken. The host system must read *Master Station* data to determine which side is in control and then issue a command to change the primary side if required.

General guidance	
1.	Side A and Side B must have the same settings, especially Serial 1 and 2 Standby Mode set as <i>Passive</i> or <i>Active</i> .
2.	RS-485 highways must always be terminated at both ends and only at the ends.
3.	The primary side can be switched by sending a suitable command to either Side A or Side B.



5. Serial Communication to the Rotork Master Station *continued*

5.2 Host Serial – Port Function

DIP switches are used to configure the serial port type. The Host Serial AIM must be removed to change DIP switch settings. For instructions on AIM removal and changing DIP switch position, refer to PUB059-050.

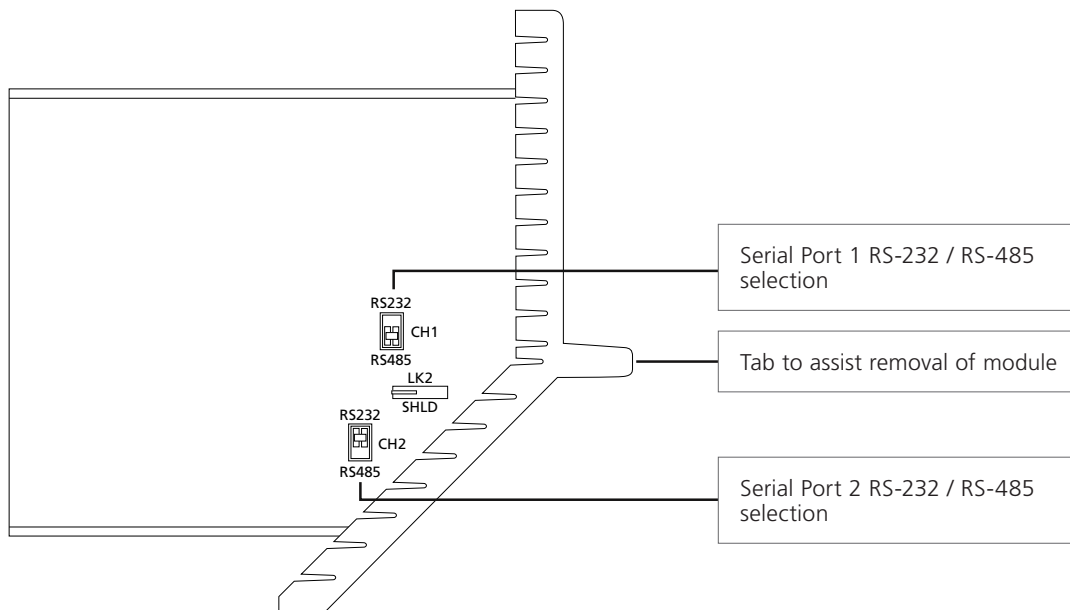


Fig 5.2.1: Serial port DIP switches shown in default position

The two DIP switches allow each port to be set for RS-232 or RS-485. The default setting for CH1 is RS-485 and CH2 is RS-232. Slide the switch up (RS-232) or down (RS-485) for the desired type. Ports can be configured independently. Do not move LK2 from the default position shown above.

To access the DIP switches, unscrew the two hex head bolts from the top and bottom of the module with a 2.5 mm Allen (hex.) key. Pull the front tab away from the *Master Station* to release the Host Serial AIM and access the DIP switches.

Refitting the Host Serial AIM is the reverse of removal. Care should be taken to ensure the AIM connectors align correctly with the *Master Station* backplane connector.



It is possible to adjust the DIP switches without fully removing the Host Serial AIM. This is useful when the *Master Station* display door cannot be fully extended outwards.

5.3 Host Serial – RS-485 Termination

The *Master Station* includes settings to switch in line termination and biasing resistors. All RS-485 highways must be terminated at each end of the highway. Multi-drop highways may include more than one *Master Station*. Only switch in termination and biasing resistors if the *Master Station* is at the end of the highway. Biasing resistors help eliminate data errors caused by reflection at the end of a highway.

Line termination and biasing resistors are disabled by default.

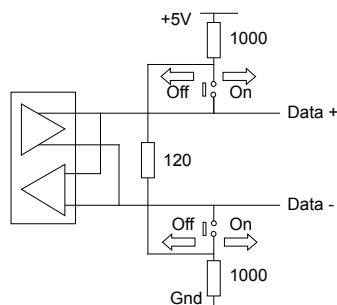


Fig 5.3.1: Port termination switches shown in off position

Settings to enable termination are in the Host Serial interface menu for each applicable side. Relay contacts connect end of line termination and biasing resistors to the RS-485 highway. Each serial port can be terminated independently.



6. Hot Standby

6.1 Hot Standby Change Over

The hot standby *Master Station* configuration provides *Master Station* redundancy through a primary side and standby side. The standby side is a complete duplicate of the primary side. The standby side remains fully operational at all times but it cannot control any connected FCUs. Each side has an independent database to collect FCU status data. The standby side is ready to take primary control at any time.

The mechanisms for primary and standby change over are:

- Power loss from primary side
- Host system Modbus command to switch primary and standby
- Operator selection of primary using the physical *Master Station* PRIMARY button*
- Operator selection of primary through the *Master Station* local or web browser interface
- Removal of one or both of the Ethernet host connectors at the *Master Station*, if the feature is enabled
- Communications over Modbus TCP stop on one or both of the Ethernet host connections, if the feature is enabled
- Communications over Modbus RTU stop on one or both of the serial host connections, if the feature is enabled

*The physical PRIMARY button can place the *Master Station* into forced primary mode which prevents change over from any other mechanism. This mode is optimised for maintenance where it is critical that change over does not occur. Forced primary mode is set by holding the physical PRIMARY button in for 3 seconds. The button will flash when forced primary mode is active. To exit forced primary mode, hold the same physical PRIMARY button in for 3 seconds.

The primary side controls the field networks and the standby side monitors performance of the primary side. Either Side A or Side B can be primary while the other is standby.



Each side of the *Master Station* has multiple host communication ports. Behaviour of the host communication ports when the side is in standby mode is configurable to *Active* or *Passive*. Ethernet 1 and Ethernet 2 share the same standby mode setting. Serial 1 and Serial 2 on the Host Serial AIM have independent standby mode settings.

When standby mode is set to *Active*, the communication port will respond to messages from the host in primary or standby mode. It is important that operation commands are addressed to the primary side as the standby side cannot control the field network.

When standby mode is set to *Passive*, the communication port will only respond to messages from the host in primary mode. The standby side will not respond to host messages.

The only message actioned by a standby side in Active standby mode is the switch sides command (Ethernet and Serial). In Passive standby mode the switch side command is actioned, but only if the command is received over the Host Serial network.

Primary side	Standby side <i>Active standby mode</i>	Standby side <i>Passive standby mode</i>
Controls the field network	Does not control the field network	Does not control the field network
Responds to all host messages and actions all commands	Responds to all host messages, does not action any commands	Does not respond to any host messages, does not action any commands
Will switch to standby side if commanded	Will switch to primary side if commanded	Will switch to primary side if commanded via Host Serial connection

Section	Page
 7. <i>Pakscan</i> Classic Field Network _____	53
7.1 Scan Times & Network Distances _____	55
7.2 Loop Fault Tolerance _____	56
7.3 Supported Field Control Units _____	57
7.4 Connecting Up _____	58
7.5 Loop Checks _____	59
7.6 <i>Master Station</i> Classic Loop Wiring Schematics _____	60
7.7 Commissioning the <i>Pakscan</i> Classic Field Network _____	62
7.8 Verifying FCU Identity _____	63
 8. Modbus Open Field Network _____	64
8.1 Highway Variants _____	66
8.2 Termination _____	68
8.3 Modbus Open Device Files _____	69
8.4 Modbus Open Settings _____	70
8.5 Modbus FCU Control _____	71
8.6 Troubleshooting _____	71

7. Pakscan Classic Field Network



The information in this section relates to the *Pakscan Classic* field network AIM (P4720). All information within applies to a single AIM. The *Master Station* can support up to two *Pakscan Classic* field network AIMs per side. A hot standby *Master Station* can therefore include up to four *Pakscan Classic* field network AIMs in total. Only the primary side AIM is in control of the network. The standby side AIM will be in standby mode ready to take over if required.

Quick specification:

- *Pakscan Classic* Protocol
- Redundant current loop topology
- Does not require external repeaters or external termination
- Network total length up to 20km
- No limitation for distance between devices within the 20km limit
- A single network can control 240 devices
- Data transfer via robust current loop network
- Network baud rate range 110 to 2,400
- Network scan rate (60 devices on 4km loop) less than 1 second
- Twisted pair instrumentation cable (1 pair)
- Communications parameters set up using handheld tool via network or using FCU settings
- Ideal for isolating duty applications



Fig 7.1: *Pakscan Classic* network loop

Automatic Expansion

When additional FCUs are connected to the *Pakscan* network, the system automatically locates and identifies them for data reporting. There is no need to reconfigure the system or modify the internal database; simply change the number of FCUs in the *Pakscan Classic Master Station* settings.



7. Pakscan Classic Field Network *continued*

The *Pakscan Classic* field network AIM fits into one of the four AIM slots of a *Master Station* and facilitates connection to *Pakscan Classic* FCUs using a daisy chain topology. Most intelligent Rotork actuators have an integral *Pakscan Classic* interface option. Devices that do not have an integral *Pakscan Classic* interface option can still be monitored and controlled via *Pakscan* using a General Purpose Field Control Unit (GPFUC).

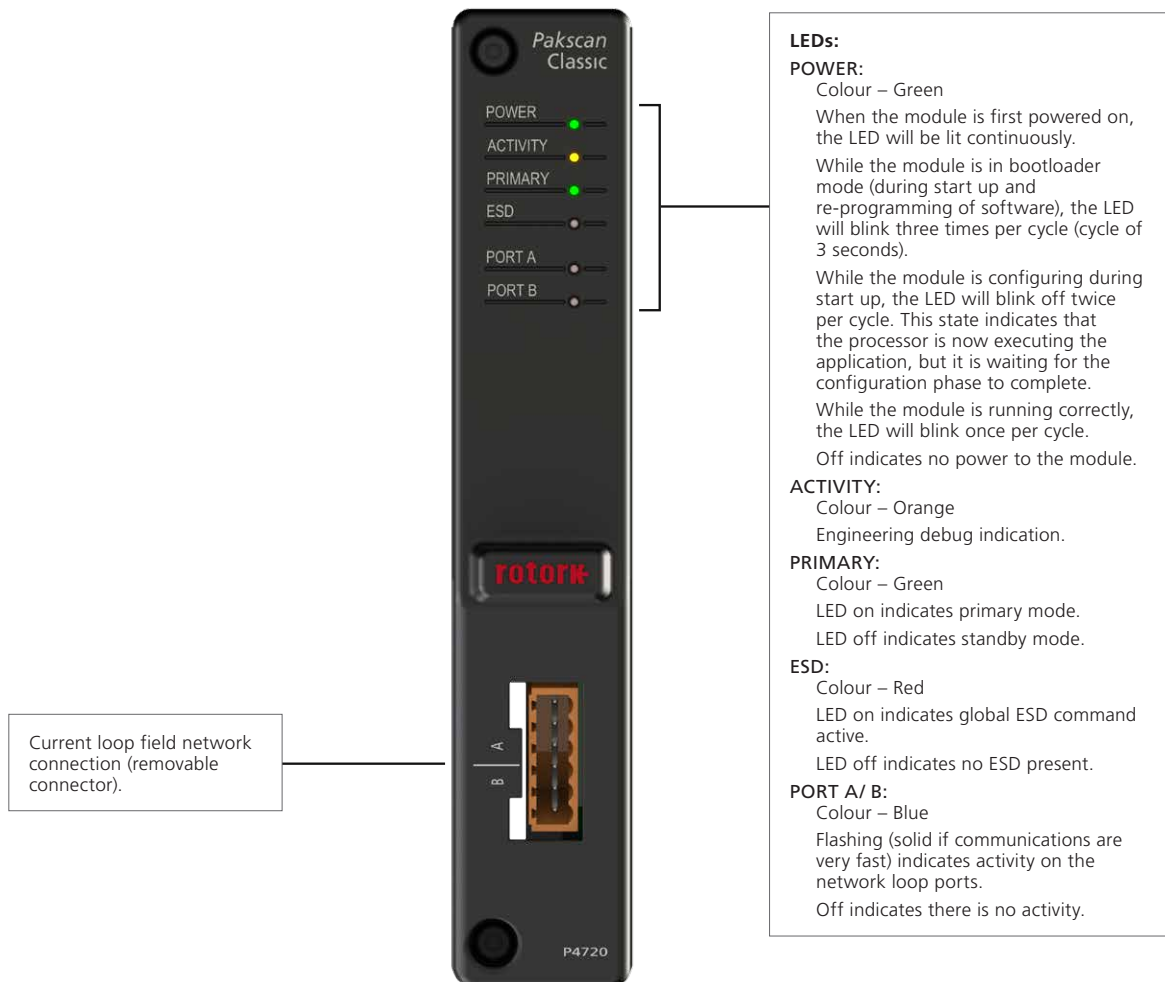


Fig 7.2: *Pakscan Classic* module front face



7.1 Scan Times & Network Distances

The *Pakscan Classic* network uses a unique proprietary protocol that achieves very fast update times with relatively low data transmission rates. Compressing the data field to a minimum length allows more data to pass over the network in a given time. The result is a system that can handle long transmission distances and a large number of FCUs, without repeaters, while still maintaining quick and efficient communication.

FCUs are scanned in turn by the *Master Station* and report their current status back in compressed code messages, minimising the transaction period.

The field cable used for the *Pakscan Classic* network is typical instrumentation cable. A simple twisted pair plus overall screen using polyethylene insulation will suffice.

The use of low transmission speeds allows the current loop to achieve long distance communication with FCUs without the need for repeaters. Where the loop distance is shorter, higher speeds can be used.

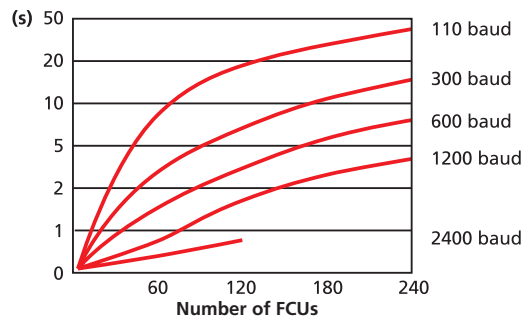
Instructions sent from the *Master Station* to FCUs have priority on the communication protocol.

Commands are considered more important than reports so the routine polling of the FCUs is momentarily suspended when a command is issued. The infrequent nature of command instructions means there is a negligible effect on the scan time for the system.

The scan time in the table shown below assumes that only one FCU has new data or a new event to report during each scan cycle. The loop protocol uses a report-by-exception technique to minimise the message lengths. The FCU does not repeat the data sent once it receives confirmation of receipt by the *Master Station*. If the scan time is short then the probability of more than one FCU with a new event to report is very small and the figures given will be accurate.

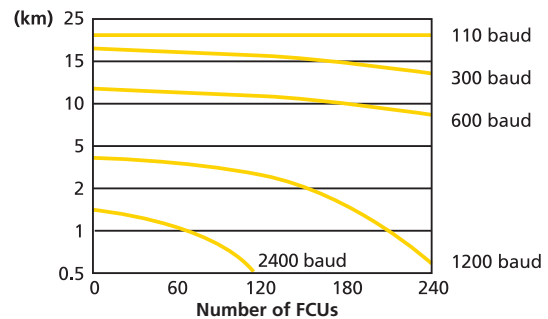
Scan Time (seconds)*

Baud Rate	Number of FCUs			
	60	120	180	240
110	8.4	19.3	31.1	42.9
300	3.1	7.1	11.4	15.8
600	1.6	3.6	5.7	7.9
1200	0.8	1.8	2.9	3.9
2400	0.4	0.9	N/A	N/A



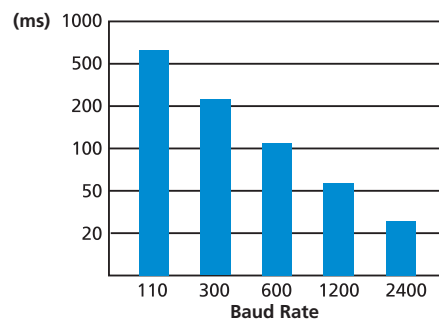
Loop Distance (km) with 1.5 mm² cable

Baud Rate	Number of FCUs		
	60	120	240
110	20.3	20.3	20.3
300	17.1	15.9	13.7
600	12.2	11.1	8.8
1200	4.1	2.9	0.6
2400	1.5	0.3	N/A



Time to issue a command (ms)*

Baud Rate	Time
110	614
300	230
600	110
1200	60
2400	30

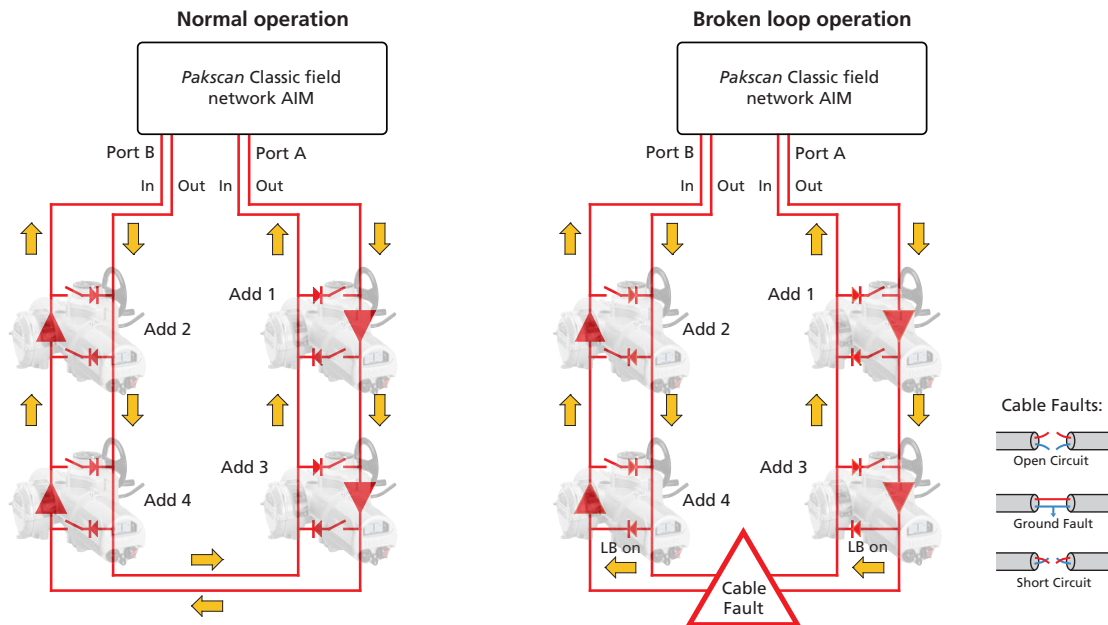


* Figures with *Doubling* enabled.



7.2 Loop Fault Tolerance

The Pakscan Classic current loop network is a single fault-tolerant redundant loop. A hot standby *Master Station* utilises a 'Y' loom to connect Side A and Side B to the same network loop. Only the primary side can control the Pakscan Classic loop.



The Loop System

The two wires are connected to each FCU in turn. They originate from and return to the *Master Station* to create a single twisted pair 2-wire loop. Each FCU is accessible from either direction forming a redundant communication path. Pakscan Classic utilises the redundant communication path in the event of a cable fault.

Cable Fault Tolerance

Integrity of the 2-wire cable is continuously checked while the system is running. In normal operation Port A is a transceiver and Port B is a receiver. The 20mA loop current passes from Port A out to Port B in and back from Port B out to Port A in. Port B can monitor communications from Port A. If communication fails, transmission from the *Master Station* stops and all FCUs go into loopback mode. Loopback closes all the switches on the diagram above. The *Master Station* then begins communication from Port A to each FCU in turn, removing loopback. Progressively, the current loop is extended until the fault location is revealed.

Port B reconfigures as a transceiver and the procedure is repeated from Port B. Once the process is complete, the fault location and nature will be known. Communication will also be restored with all FCUs from either side of the current loop.

The loopback feature allows the system to have two communication routes without the need for two cable runs. It also allows the system to cope with cable breaks, short circuits or ground faults.

High Integrity Data Transmission

Message transmission on the network is controlled by the *Master Station*. FCUs are only permitted to respond to requests from the *Master Station*. All data messages and commands are verified by framing and CRC checks.

Non-catastrophic failures due to noise are handled by the *Master Station* on a repeat as necessary basis. All messages require a response within the timeout period. If the timeout period expires, the *Master Station* will repeat the message up to three times before indicating that the field unit is out of communication.

Fault Indication

The *Master Station* can identify the location and type of cable fault should a cable fault occur. FCUs shown in loopback mode will be adjacent to the cable fault.

FCUs should have unique addresses on the network. If a duplicate address is found, the *Master Station* will indicate which FCUs share the duplicate address. The *Master Station* will never issue a command to a duplicate address.



7.3 Supported Field Control Units

Actuator Field Control Units

Pakscan Classic FCUs contained within Rotork actuators provide the same environmental protections offered by the actuator. Variable parameters such as address and baud rate are configured using a connected Paktester or through the actuator setting menus. Refer to the specific actuator manual for setting details.



FCUs operating on the network can have all their *Pakscan Classic* parameters changed by the *Master Station* apart from the address. The address must be unique to the FCU. All FCU settings are retained in the actuator if power is lost. IQ actuators and their variants, such as IQT and SI4, use Common Protocol cards to communicate with the *Master Station*.

Pakscan Classic FCUs can be positioned in any order on the network loop with addresses in any order.

FCUs include an automatic bypass to maintain loop continuity in the event of power loss. Network communication will continue with the remaining FCUs and the *Master Station* will automatically detect the isolated FCU is no longer present on the network. The missing FCU data can be returned to zero (unknown) or kept in its last known state.

Every FCU will automatically identify its FCU type to the *Master Station*. FCU type determines the information shown for the FCU in the *Master Station* interface.

Standard actuator local and remote control may be used in addition to *Pakscan Classic* control.

General Purpose Field Control Unit

Modern plants often require additional equipment such as transmitters, solenoids or other sensors to be integrated into the site control system. *Pakscan Classic* can facilitate integration of these devices using a General Purpose Field Control Unit (GPFCU).

The GPFCU controls and monitors digital or analogue inputs and outputs and reports them on the network loop. GPFCU can be supplied in multiple forms; 19" rack mount (shown below), watertight IP65 enclosure or fully certified hazardous area enclosure.

Network variables for GPFCU are configured using a Paktester. Refer to PUB059-021 for GPFCU instructions.



Noise Protection

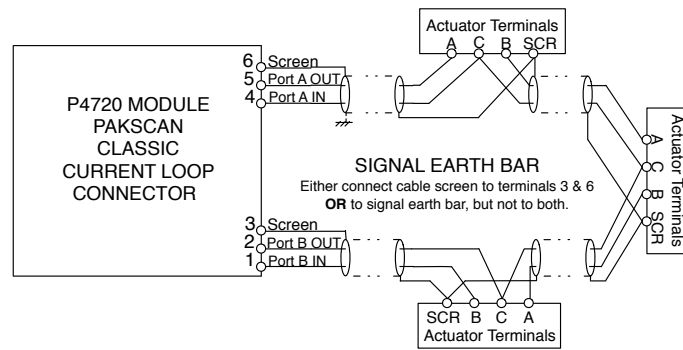
Pakscan Classic provides good protection against electrical interference due to the nature of current loops. Using a 20mA current loop offers low impedance to noise currents and prevents voltage spikes as a result of noise currents. If a voltage spike does occur, it is quickly clamped with high speed surge arresters fitted to each FCU and the *Master Station*.



7. Pakscan Classic Field Network *continued*

7.4 Connecting Up

Wire the network cable to the 6 way connector fitted to the *Pakscan* Classic field network AIM or the Y loom connector for a hot standby *Master Station*. Wiring details are shown below:



Pakscan Classic will operate on standard instrumentation cable with the following recommended parameters:

Cross Section (mm ²)	Resistance Ω /km	Capacitance pF/m
0.5 solid	36.8 Ω /km	115 pF/m
0.5 flexible	39.7 Ω /km	115 pF/m
1.0 solid	18.4 Ω /km	115 pF/m
1.5 stranded	12.3 Ω /km	115 pF/m



7.5 Loop Checks

Cabling and connection of the network loop must be correct for *Pakscan Classic* to operate. Loop resistance and capacitance must be known to determine the maximum communication speed possible. Operate at the lowest loop speed if loop resistance and capacitance are unknown.

Loop Continuity

Network loop continuity must be checked with all FCUs connected and powered OFF. Measure and record the resistance of each cable core. Network loop resistance (R) is the sum of the resistance of both cable cores. Periodic measurement, recording and comparison to previous resistance records could indicate a cable fault or degradation.

Screen Continuity

Screen continuity must be continuous between each end of the network loop. The screen must be connected to either a signal earth bar at only one point on the network or to terminals on the *Master Station* network loop connector. Pin 6 connects to the enclosure earth and pin 3 connects to the enclosure earth via an internal capacitor, preventing an earth loop. Both screens must be connected to the terminals provided on the *Master Station* network loop connector to meet the EMC European Directive.

Cable Capacitance

Capacitance (C) between the cable cores is critical to system performance. Maximum capacitance varies with baud rate. If capacitance exceeds the baud rate maximum, communication will be poor or fail. Measure and record the capacitance between the cable cores if a suitable meter is available.

Maximum Loop Speed

Cable resistance must not exceed 500 Ω (250 Ω per core) and the total capacitance must not exceed the maximum value for the applicable speed shown below. Total capacitance is the sum of cable capacitance and FCU capacitance which can be calculated using the FCU figure below. Use the table below to determine what loop speed should be used.

Baud Rate	R max (Ω)	C max (μF) ¹
110	500	4.5
300	500	2.1
600	500	1.54
1200	500	0.6
2400	500	0.3

¹ Each FCU will add a capacitance of 2.2nF. C max is the maximum value for network capacitance (cable capacitance plus FCU capacitance).

Test Equipment

An accurate multimeter with capacitance test facility is suitable for testing loop resistance and capacitance.

Under no circumstances should high voltage test equipment, such as insulation Megger testers, be used when the cable loop is connected to a *Master Station* or FCU. High voltages generated by such equipment may damage *Pakscan* components.



7. Pakscan Classic Field Network *continued*

7.6 Master Station Classic Loop Wiring Schematics

The connected *Pakscan* Classic loop should match the diagram below for a single or dual *Master Station*. Review wiring if it does not match the diagram.

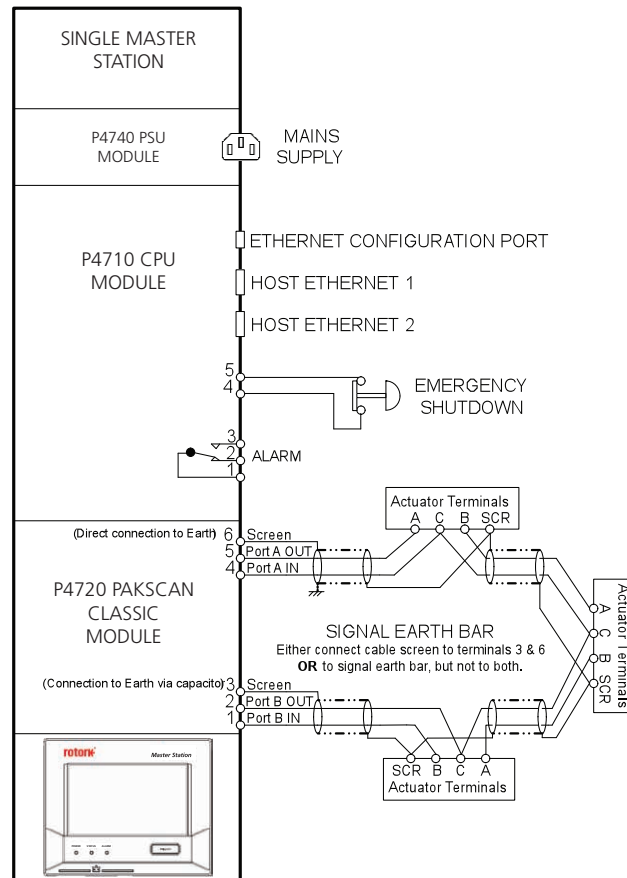


Fig 7.6.1: Single and dual Master Station current loop block diagram

A link is fitted at the factory from pin 4 to pin 5 on the CPU module. The link prevents an unexpected ESD action if the ESD function is enabled on the *Master Station*. If ESD is required, the link should be removed and replaced with appropriate wiring.

7. Pakscan Classic Field Network *continued*



The connected *Pakscan Classic* loop should match the diagram below for a hot standby *Master Station*. Review wiring if it does not match the diagram.

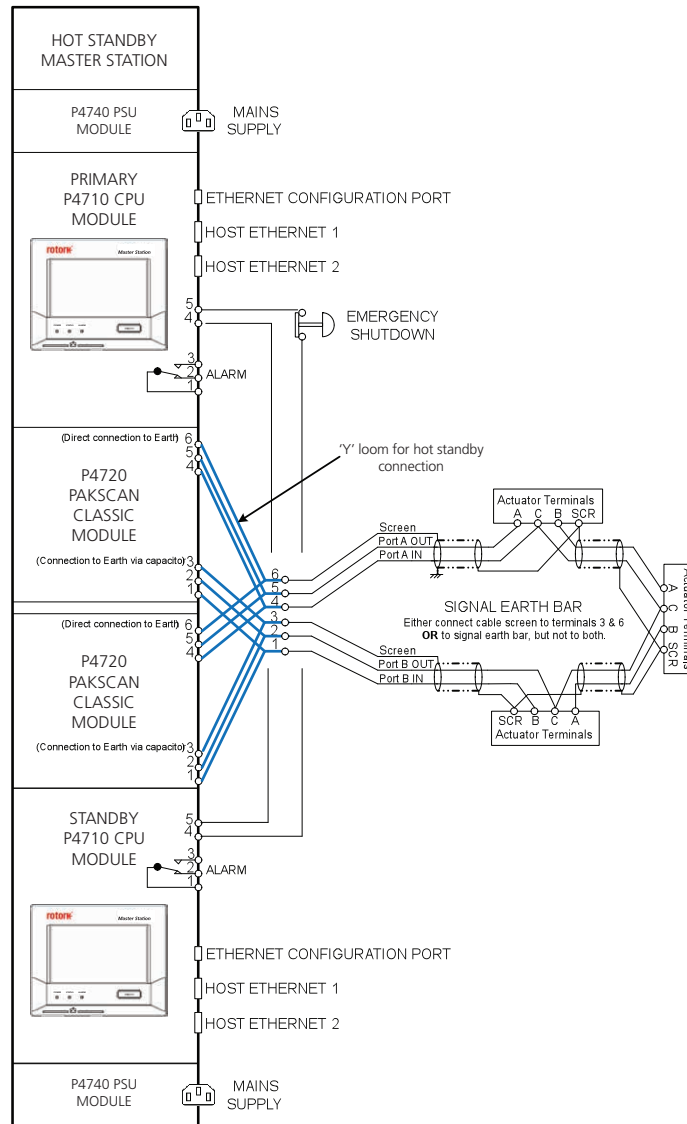


Fig 7.6.2: Hot standby Master Station current loop block diagram

A link is fitted at the factory from pin 4 to pin 5 on the CPU module. The link prevents an unexpected ESD action if the ESD function is enabled on the *Master Station*. If ESD is required, the link should be removed and replaced with appropriate wiring.



7. Pakscan Classic Field Network *continued*

7.7 Commissioning the Pakscan Classic Field Network

The *Pakscan Classic* network loop must be commissioned in order to identify all FCUs on the network. Baud rate must be configured in the *Master Station* to permit communication. Each FCU must be available, have a unique network address and be set for the same baud rate as the *Master Station*.

The *Master Station* parameter for highest field network address should be set to the highest address configured in the FCUs and the *Master Station* parameter for lowest field network address should be set to the lowest address configured in the FCUs.

Parameter	Value
Lowest FCU Scan Address	1
Highest FCU Scan Address	5
Loop Speed	1200
Loop Speed Doubling	disabled
DV Convert	disabled
Port A Drive Strength (%)	1200
Port B Drive Strength (%)	51

Perform the following steps to commission the current loop and validate communication to FCUs.

- 1) Ensure all connected FCUs are in a non-responsive state (LOCAL or STOP mode) before commencing commissioning or fault finding on the system.
- 2) Disconnect wires from Port B on the *Master Station* and ensure power is ON for all FCUs.
- 3) Navigate to the *Pakscan Classic Status* page on the *Master Station* interface. Select *Reset Network* and confirm the reset to begin polling network addresses from the *Master Station*.
- 4) Verify all FCUs appear on the *Master Station* device list. This confirms communication is possible to each FCU from the *Master Station* through the connected port.
- 5) Reconnect wires to Port B and disconnect wires from Port A on the *Master Station*.
- 6) Repeat steps 3 and 4.
- 7) Reconnect wires to Port A on the *Master Station* and select *Reset Network* a final time.

If an FCU does not appear on the *Master Station* device list; check wiring, FCU configuration and power to the device.

The network loop is now commissioned for communication to all FCUs.



7.8 Verifying FCU Identity

Commissioning a *Pakscan* Classic network loop does not account for physical FCU installation location or FCU configuration errors. It is important to verify each physical FCU appears as expected on the *Master Station* device list to ensure commands are issued to the correct FCU during operation.

The easiest method to verify identity of an FCU is by isolating power from each device in turn and observing results on the *Master Station*. Follow the below set of instructions for each connected FCU.

- 1) Note the expected FCU address of the device (configured in Section 7.3).
- 2) Isolate power to the FCU.
- 3) Observe loss of communication to one FCU within the *Master Station* device list. It may take a moment to report loss of communication with an FCU.
- 4) Confirm the missing FCU is configured with the expected FCU address.
- 5) Return power to the FCU and observe communication with the *Master Station* returns.

Repeat the above process for each FCU on the network loop.

If multiple FCUs lose communication when isolating power, a network cable fault may be present.

If the confirmed FCU address does not match the expected FCU address, reconfigure the FCU settings (Section 7.3).

8. Modbus Open Field Network

The information in this section relates to the Modbus Open field network AIM (P4724). The *Master Station* can support one Modbus Open field network. In a hot standby system there are two AIMs, one on each side. Only the primary side AIM is in control of the network. The standby side AIM will stay in standby mode ready to take over if required.

The Modbus Open field network AIM accommodates three topology options:

- Single RS-485 multi-drop highway
- Dual isolated RS-485 multi-drop highways
- Redundant ring (FCUs have built in repeaters)

Quick specification:

- Open protocol communications
- Redundant dual and ring topologies
- Network baud rate range 9,600 to 115,200
- Ideal for isolating duty applications for multi-drop highway topology
- Up to 240 FCUs can be connected in a ring configuration
- Up to 32 field control units (FCUs) per segment

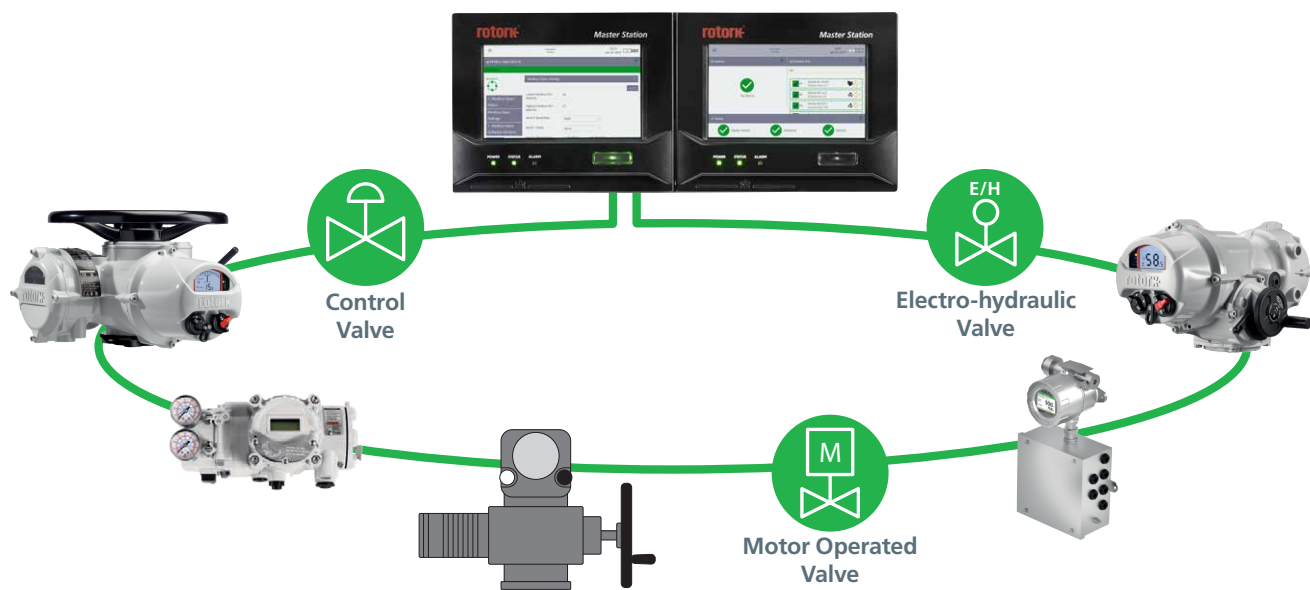


Fig 8.1: Modbus Open redundant ring

The Modbus Open field network AIM fits into one of the four AIM slots of a *Master Station* and facilitates connection to a Modbus FCU using a highway or ring topology. Most intelligent Rotork actuators have an integral Modbus interface option. Third party Modbus FCUs can also be connected to the Modbus Open field network.

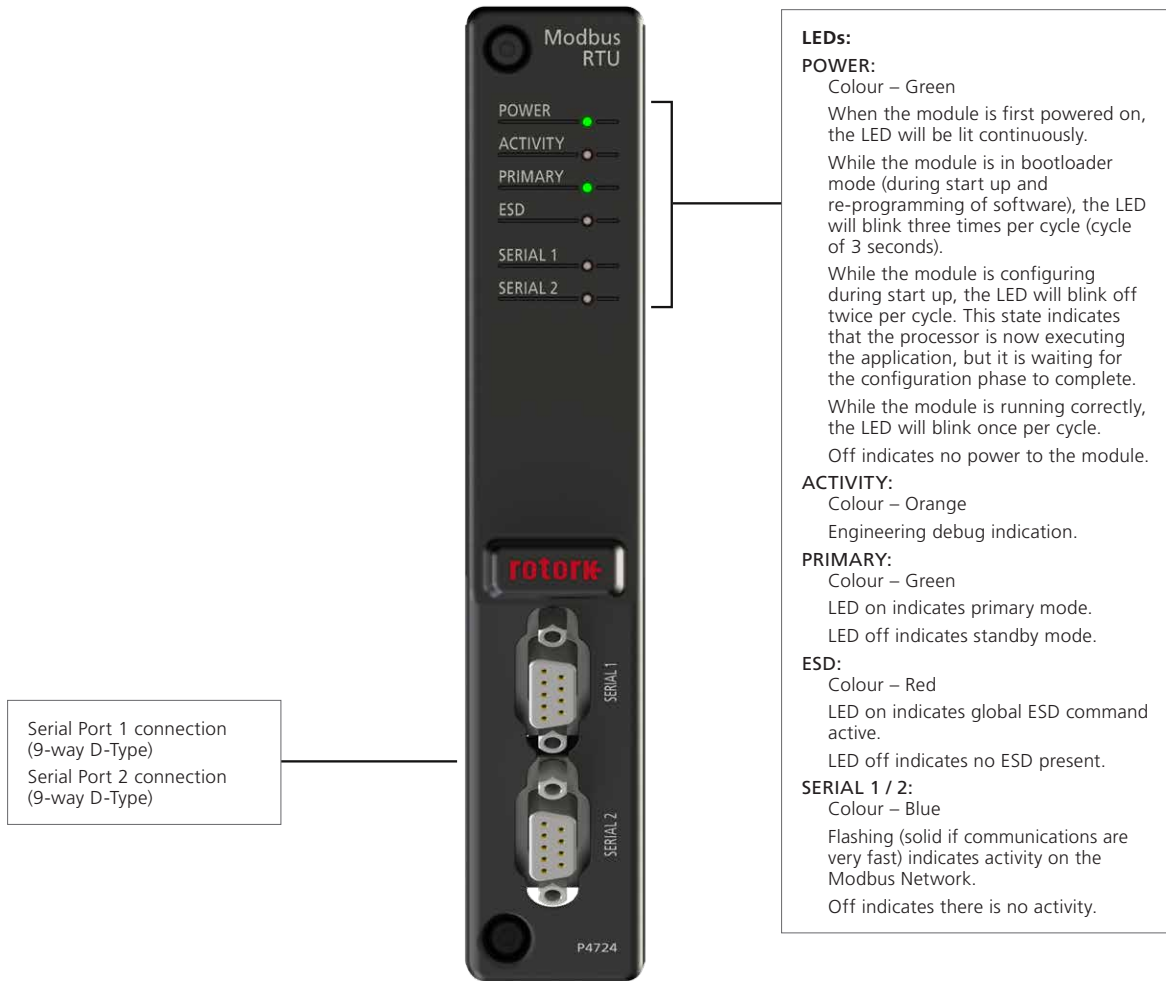


Fig 8.2: Modbus Open module front face

8.1 Highway Variants

The Modbus Open field network AIM accommodates a Single Channel, Dual Channel or Redundant Ring topology. FCUs must be compatible with the configured *Master Station* topology. A Redundant Ring FCU will not function on both channels of a Dual Channel topology.

- A Single Channel highway is ideal for simple networks.
- A Dual Channel highway offers increased integrity by creating a second redundant highway.
- A Redundant Ring topology extends the network distance without external repeaters and also offers redundancy.

The Modbus Open Settings must be adjusted to set the correct serial ports to use for the chosen network. Each side of the *Master Station* can be configured to use either Serial 1, Serial 2, or both serial ports. Serial ports must have Baud Rate, Parity, Termination and Time Out configured for successful network communication.

For a **Single Channel** network topology, only one serial port is used per network. For a single or dual *Master Station*, Serial 1 and / or Serial 2 can be used for the Modbus Network. Each port can have different highway settings however, Modbus addresses must not be duplicated across both highways.

Two different connection topologies can be used for a multi-drop RS-485 highway. The daisy chain method connects the trunk cable directly to each Modbus FCU. The trunk line method connects spur lines from each Modbus FCU to the trunk cable. Spur line tap locations must be positioned as close to the Modbus FCU as possible. All configurations require the total network length to be kept within the permitted maximum for the network speed used. It is good practice to avoid spur lines wherever possible.



Fig 8.1.1: RS-485 Data Highway Topology – Single Channel

For a **Dual Channel** network topology, two highways are used per network. For a single or dual *Master Station*, Serial 1 and Serial 2 ports should be used for the same network. Serial Configuration should be set to Serial 1 / 2 and settings for each serial port must be the same. The highway from Serial 1 must be connected to FCU channel 1 and the highway from Serial 2 must be connected to FCU channel 2.

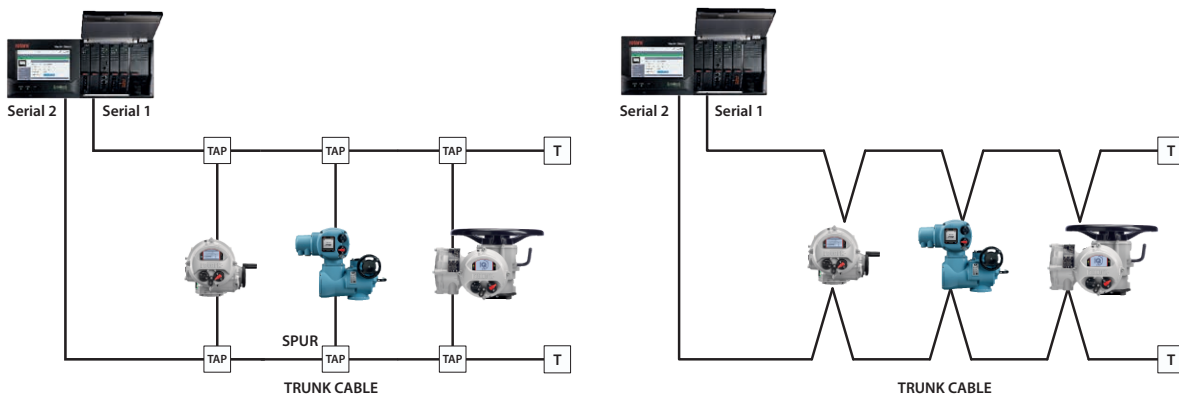


Fig 8.1.2: RS-485 Data Highway Topology – Dual Channel

The maximum trunk length, length of each spur and the cumulative total length are dependent on the system speed in use. The table below suggests the maximum figures for copper cable. Segment Length is the total of the trunk and all spurs added together.

Data Rate (Baud)	Maximum Segment Length (m)	Total Spur Length (m)
9,600	1,500	500
19,200	1,200	500
38,400	1,000	300
57,600	750	200
115,200	500	100

Within each FCU there is a short drop line or stub connection wire from the terminals to the Modbus control option. The length must be included in any calculation for total and individual drop lengths.

A **Redundant Ring** network topology requires each field device to contain a repeater to form the ring. Both Serial 1 and Serial 2 must be used for a Single Channel Repeater highway in a Redundant Ring topology. The ring topology links all FCUs together terminating both ends of the loop at the *Master Station*. Ring topology allows communication in both directions, thereby allowing communication to continue to all FCUs in the event of a broken connection between FCUs, or to all available FCUs in the event of a failed unit. Each FCU must have a bypass facility to ensure the network integrity is maintained should the power to the FCU be removed.

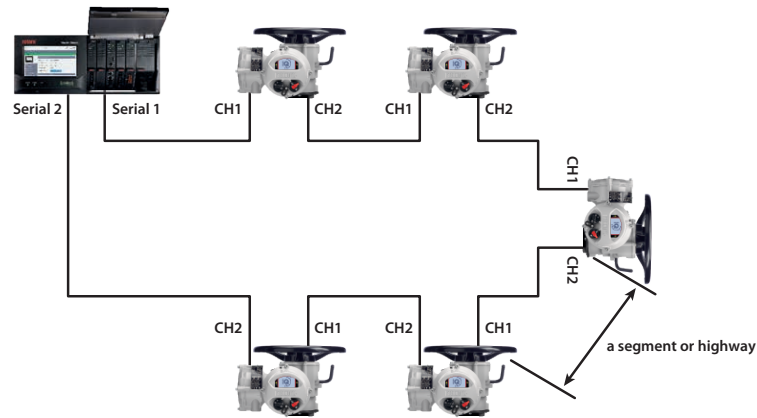


Fig 8.1.3: Ring Topology

The above diagram shows a Redundant Ring topology where the signal from Serial 1 of the *Master Station* connects to channel 1 of the first FCU. Channel 2 is connected to channel 1 of the next FCU. Subsequent FCUs are connected in the same fashion to form a loop. The final FCU terminates the loop at Serial 2 of the *Master Station*.

Communications received on channel 1 are repeated on channel 2. Each repeater has a small propagation delay (< 2 ms).

The connection between each device on the network is known as a segment. Distance rules for network segments apply to the distance between two connected FCUs. For example, at 9,600 baud you can have a distance of 1.5 km between each FCU. It is important to note that should an FCU be powered off, the segment length between the two available FCUs either side of the powered down FCU could exceed the cable length limits and communication may be affected. Rotork recommends at least four FCUs are connected within the maximum segment length limit for the baud rate in use to ensure reliable communications when FCUs are powered off.

Modbus field wiring for hot standby

When using a hot standby *Master Station*, Side A and Side B serial port configurations must be the same. Serial ports from each side must be physically linked to the equivalent serial port from the other side (i.e. Side A serial 1 to Side B serial 1). Linking the serial ports together ensures both sides of the *Master Station* can communicate on the same network.

The below diagrams show how the serial ports are linked for the three network topologies.

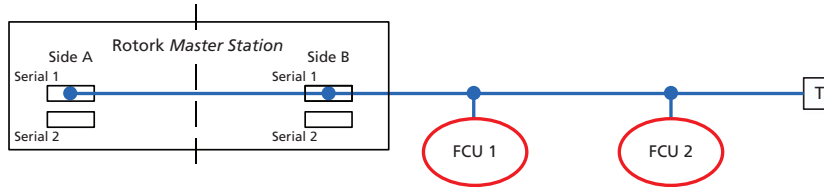


Fig 8.1.4: Single Channel Topology

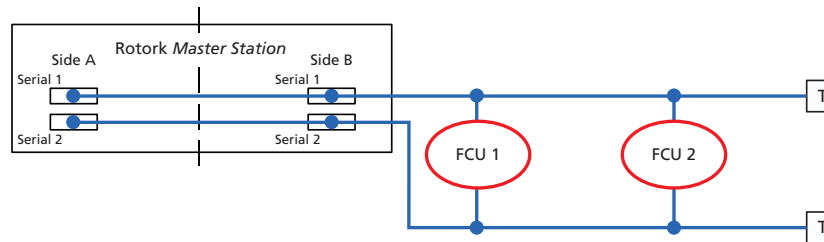


Fig 8.1.5: Dual Channel Topology

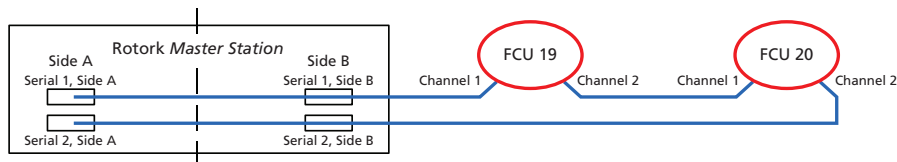


Fig 8.1.6: Redundant Ring Topology

8.2 Termination

The *Master Station* has built in termination resistors (providing termination and biasing) that can be switched in through the Modbus Open *Master Station* settings. Termination of a network prevents issues caused by signal reflections and biasing creates a fixed healthy state when none of the FCUs are transmitting on the network. If termination is not correctly implemented, network communications could be adversely affected.

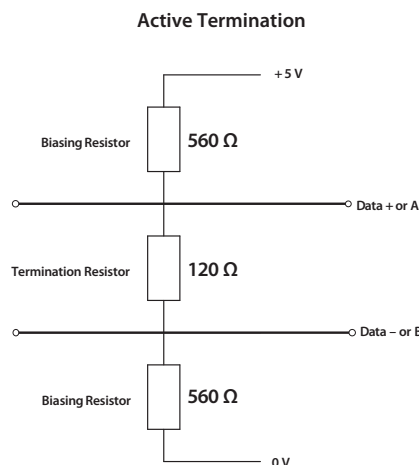


Fig 8.2.1: Active Termination for RS-485 highway. Biasing resistor values are typical

Termination for Redundant Ring segments is handled automatically within Rotork FCUs.

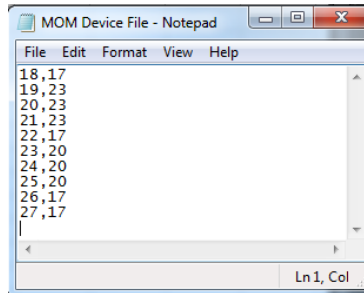
End of line termination for Single Channel and Dual Channel topologies can be achieved within Rotork FCUs or separately with a suitable resistor (120Ω, 0.5 Watt rating) connected between data line A and data line B.

8. Modbus Open Field Network *continued*

8.3 Modbus Open Device Files

In order for the *Master Station* to identify Modbus FCUs, a Device File must be created that defines the FCU type code against the Modbus address of each FCU.

The Device File is a plain text file in a CSV (Comma Separated Values) format.



A Device File can be created directly in a Text Document editor such as Notepad. Each row of the Device File represents a Modbus FCU. Each row consists of the Modbus FCU address and the applicable FCU Type Code, separated by a comma. The order of Modbus addresses will represent the order that the FCUs appear on the network. The FCU Type Code defines the type of FCU the *Master Station* is communicating with.

All values of the Device File should be in decimal, not hexadecimal.

For large network loops with many FCUs, a Device File can be created using a spreadsheet program such as Excel. Column A should contain the Modbus FCU address and Column B should include the FCU Type Code. Separation with commas is not necessary when using Excel.

One row per Modbus FCU. The file must always be saved as '.csv' format.

Modbus FCU Type Codes are detailed in the following table:

Value (dec)	Value (hex)	Description	Value (dec)	Value (hex)	Description
0	0000	A, AQ or Q Actuator	12	000C	CVL
1	0001	Unknown	13	000D	CVQ
2	0002	Unknown	14	000E	ROMpak
3	0003	GPFCU - ACT	15	000F	Pakscan 3 Wireless
4	0004	GPFCU - GP	16	0010	A Range watertight
5	0005	Flowpak	17	0011	IQ3
6	0006	IQ	18	0012	IQT3
7	0007	IQ Analogue	19	0013	P3W Sensor
8	0008	IQT	20	0014	CMA
9	0009	EH	21	0015	SI3 or SI4
10	000A	Skilmatic	22	0016	K Range or 1600 mk5
11	000B	Multiport	23	0017	Centronik (CKc)

The Device File is uploaded to the *Master Station* from the Modbus Open Settings screen. This is only available in Admin mode.



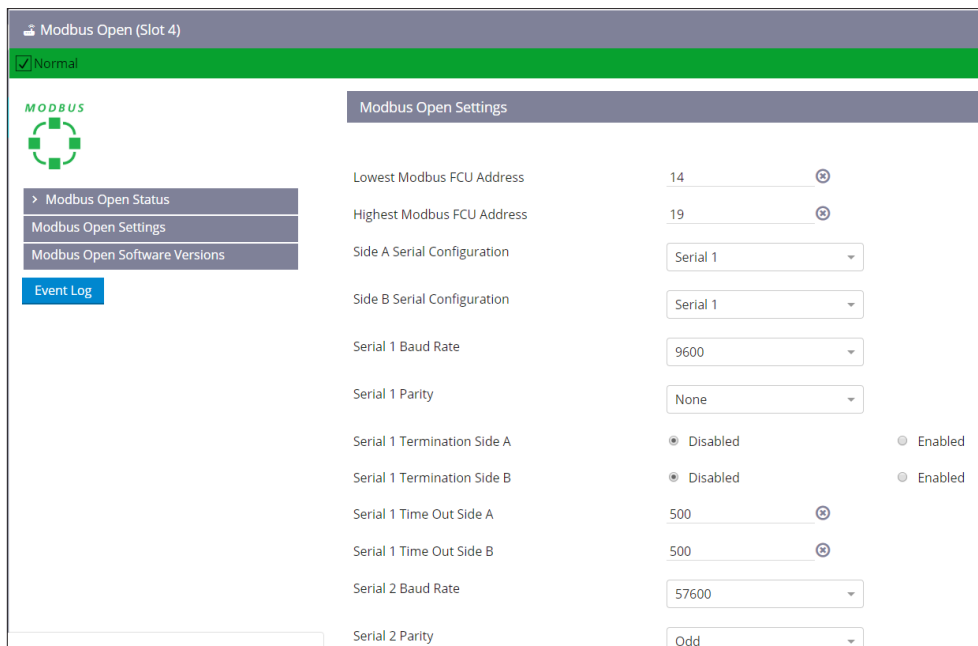
Communication to Modbus FCUs cannot occur until the Device File is uploaded to the *Master Station*. The file will need to be loaded into both sides of a hot standby *Master Station*.

For changes to settings it is advisable to use the Service Port connection (rather than host connections).

8.4 Modbus Open Settings

Settings for the Modbus Open field network are located in the Modbus Open interface menu. The available settings are detailed below.

- **Lowest / Highest Modbus FCU Address:** Defines the address range the Modbus Open field network AIM will scan when communicating with FCUs on the Modbus Open network. FCUs will not communicate with the *Master Station* if their address is beyond the range set here. FCUs must have a unique address that is not already used on another network in the *Master Station*. If an FCU address overlaps another network, a duplicate address alarm will be shown
- **Serial Configuration:** Defines which ports communicate to the Modbus network. This setting is often determined by the Modbus network in use (Single Channel, Dual Channel or Single Channel Repeater)
 - Single Channel networks only require one serial port, either Serial 1 or Serial 2. Side A Serial Configuration and Side B Serial Configuration must match for a hot standby *Master Station*
 - Dual Channel and Single Channel Repeater networks require both serial ports. Serial Configuration must be set to Serial 1 / 2. Side A Serial Configuration and Side B Serial Configuration must match for a hot standby *Master Station*
- **Baud Rate:** Set to an appropriate communication speed for the network loop. Refer to Section 8 and the Modbus RTU specification for guidance on appropriate baud rate setting
- **Parity:** Configure as Even or Odd for error detection. Configure as None to disable parity
- **Termination:** Enable or Disable termination at the *Master Station*. Termination should only be enabled if the *Master Station* is at the end of the network trunk line
- **Time Out:** Set the period a Modbus Open field network AIM will wait for an FCU response (500 to 5000 ms). Communication loss will be reported if an FCU does not respond within the Time Out period
- **Upload Device File:** Upload the CSV file defining the FCUs on the Modbus network. Only available at Admin access level
- **Device File CRC:** Only displayed after upload of a valid Device File. The CRC value is specific to the Device File. A hot standby *Master Station* must have the same Device File uploaded to Side A and Side B. The CRC for Side A and Side B should match



8. Modbus Open Field Network *continued*

Modbus Open Software Versions

Software versions of all connected Modbus Open field network AIMs can be checked on the Modbus Open Software Versions page. Viewer and User logins provide read only access to the Software Version and Changeset Code. Admin login adds functionality to upload a new RFW file (Rotork Firmware) and view upload status of the *Master Station*.

Firmware can only be updated on the connected side of a hot standby *Master Station*. Side A and Side B must be upgraded in turn with the same firmware.

Event Log

The Event Log shows commands received by the Modbus Open field network AIM. A hot standby *Master Station* will show commands to Side A and Side B.

8.5 Modbus FCU Control

Modbus FCUs can be controlled from the *Master Station* by two different means:

- *Master Station* Interface
- Modbus Host Database

Master Station Interface

Control and status information for Modbus FCUs is accessible from the local *Master Station* display interface or via web browser. Each Modbus FCU can be controlled by navigating to the applicable device from the Devices page.

Modbus Host Database

Modbus commands from a host controller can be used to control an individual FCU or groups of FCUs connected to the *Master Station*. Host connection is via Ethernet ports (Modbus TCP) or optional Host Serial AIM ports (Modbus RTU).

8.6 Troubleshooting

1. Modbus Open serial ports are inactive and no Modbus FCUs are appearing on the Devices page or Modbus Loop Map.

Ensure correct high and low address values are entered, serial configuration is correct for the port(s) in use and the correct Device File is uploaded in Modbus Open Settings. Serial port LEDs should begin to flash on the Modbus Open field network AIM to indicate active communication on the port.

If no devices appear on the Loop Map after approximately five minutes, check network connections from the serial port(s) to the Modbus FCUs.

2. Unknown Modbus device appearing.

An unknown device will appear on the Loop Map if it has not been defined by the uploaded Device File. Check the Device File contains all Modbus FCU addresses and every address has a suitable FCU type.


3. Modbus device appears with incorrect image.

The Device File defines the type of FCU connected. Update the FCU type for the applicable Modbus FCU address and upload the Device File to the *Master Station*.

4. The Modbus Loop Map does not represent the real layout of the network.

The order that FCUs appear on the Loop Map matches the order in the Device File. Change the order of FCUs in the Device File to reflect the real connection order on the network.

Modbus Technical Information

Section	Page
M 9. Host Modbus Specification _____	73
9.1 Electrical Specification _____	73
9.2 Outer Protocol _____	73
9.3 Serial Data (Host Serial AIM only) _____	73
9.4 Overview of the Design _____	74
M 10. Modbus Database – Generic and Honeywell EPLCG _____	75
10.1 Modbus Unit Address _____	75
10.2 Modbus Function Code Support _____	76
10.3 Database Access _____	80
10.4 Notes on the use of the Generic and EPLCG Modbus Protocol _____	82
10.5 <i>Master Station</i> Database _____	84
10.6 FCU Database _____	88
10.7 Modbus Messages Examples _____	94
M 11. Modbus Database – Yokogawa and Honeywell SI _____	96
11.1 Modbus Unit Address _____	97
11.2 Modbus Function Code Support _____	98
11.3 Database Access _____	100
11.4 Notes on the use of the Yokogawa and Honeywell SI Modbus Protocol _____	101
11.5 <i>Master Station</i> Database _____	103
11.6 FCU Database _____	104
11.7 FCU Inputs and Outputs Available _____	116
11.8 Modbus Message Examples _____	118
 12. Data Interpretation (All Modbus Databases) _____	119
12.1 <i>Master Station</i> Data _____	119
12.2 FCU Data _____	122

9. Host Modbus Specification

The information in this section relates to the Host Modbus communications.

The Host Modbus interface is available over Ethernet and serial connections. Ethernet connections are available as standard, whereas the serial interface is an optional AIM. Both interfaces use the same Modbus database structures to present information to the host.

The user is able to select one of two basic database formations:

- **Generic and Honeywell EPLCG**

An efficient database with all the info required for controlling a process, best for register reads and writes. Multiple Modbus slave addresses are used to access the devices in blocks of 60. Up to 247 devices can be accessed. Generic and Honeywell EPLCG databases are identical apart from the scaling of analogue values

- **Yokogawa and Honeywell SI**

A condensed database, best for discrete reads and writes, up to 240 devices can be accessed with a single Modbus slave address. Yokogawa and Honeywell SI databases are identical apart from the scaling of analogue values

It is possible to select a different database for the Ethernet and serial ports. Ethernet uses the same database for both ports. Serial permits selection of different databases for each port.

Each database can be used for any PLC, DCS or other host system. Selection of the database will depend in part how the user requires to read data and how much data is required.

9.1 Electrical Specification

Ethernet	10/100/1000 Mbps
Serial data line electrical specification	RS-485 or RS-232

9.2 Outer Protocol

Ethernet	Modbus TCP/IP Server
Modbus Transmission Mode	RTU (8-bit binary data)

9.3 Serial Data (Host Serial AIM only)

Baud Rate	2400, 4800, 9600, 19200, 38400, 57600, or 115200
Number of bits per character:	
Start bits	1
Data bits (LSB first)	8
Parity (configurable)	Odd, Even, None, Always 0
Stop bits	1
Error checking	CRC

The Modbus protocol supports two forms of data access discrete (bit) and register addressing. The function code determines which form of addressing is to be used.

9.4 Overview of the Design

Modbus commands may be transmitted to the *Master Station* via Ethernet, RS-232 or RS-485 physical interfaces. Up to 32 *Master Station* modules may be linked on a single RS-485 highway to one host port. Each *Master Station* permits up to 240 FCUs to be connected to it.

The *Master Station* responds as a MODBUS SLAVE or SERVER to messages from the host. The Modbus address of the *Master Station* and the protocol used on the particular port is set using the *Master Station* local display interface or the *Master Station* web browser interface.

The Modbus slave address is required for communication with the *Master Station* via Modbus TCP and Modbus RTU. The *Master Station* maintains a sectioned database covering all its connected FCUs, and the host reads this data without the need to access FCUs directly. The *Master Station* performs the functions of Data Concentrator and interface whilst the Field AIMS are the field network masters.

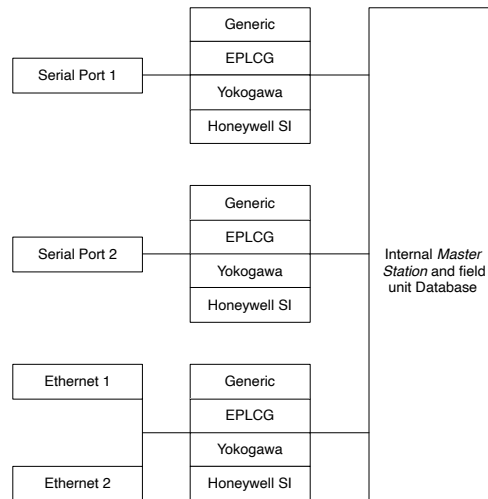


Fig 9.4.1: Database Connections

10. Modbus Database – Generic and Honeywell EPLCG

This section describes the two protocols that most efficiently allow access to the maximum amount of data within the *Master Station* for controlling a process. The tables give locations for the data which may be read from either registers or discrete locations.

Selection of the Modbus database varies depending on the type of connection. The Ethernet database can be set in the Modbus Host Common Settings section on the *Master Station* page (*Master Station* > *Master Station* Status and Settings > Modbus Host Common Settings). The serial databases can be set for each port on the Host Serial Settings page (Interfaces > Host Serial > Host Serial Settings). Select *Generic* for the generic configuration of the database or *Honeywell EPLCG* for the EPLCG version of the database: the difference between these two choices is in the analogue scaling data only. Generic uses 16-bit 2's complement and EPLCG uses a 12-bit value in the register.

Care must be taken to ensure that the correct protocol is routed to the port being used for the application concerned. Rotork's own In-Vision system, for example, uses the *Generic* Modbus database. The Modbus address is used to gain access to the correct section of the database for the FCU whose data is to be collected. The base address for this database does not cover the whole range of FCU addresses. The lowest (base) Modbus address allows access to the first 60 FCUs, the next address accesses the the next 60 FCUs and so on.

10.1 Modbus Unit Address

The first byte of all Modbus message frames is the Modbus Address byte. Modbus supports 248 addresses, of which value 0 is always allocated for broadcast messages. This leaves 247 addresses for use by connected devices on the Modbus data link. Each *Master Station* is configured with a Modbus Base Address, which may be anywhere in the range 1 to 247.

Modbus Address	Function Code	Register or Discrete Address	Number of Registers or Bits	CRC Check
8 bits	8 bits	16 bits	16 bits	16 bits

Fig 10.1.1: Typical Modbus host read request telegram

Each *Master Station* will then respond to between 1 and 4 Modbus addresses depending on how many FCUs it has been configured to support. Physically a *Master Station* is only one unit on the Modbus highway, but logically it can appear to be up to 4 units. Each logical unit supports up to 60 FCUs.

Each unit behaves as an independent Modbus slave. Fig 10.1.2 illustrates this and Fig 10.1.3 correlates the real FCU address with which logical *Master Station* unit it appears to be attached. Users may find that when assigning Modbus addresses for use on the network, configuring the setting of the Base address of the *Master Station* using increments of 4 will ensure future expansion space.

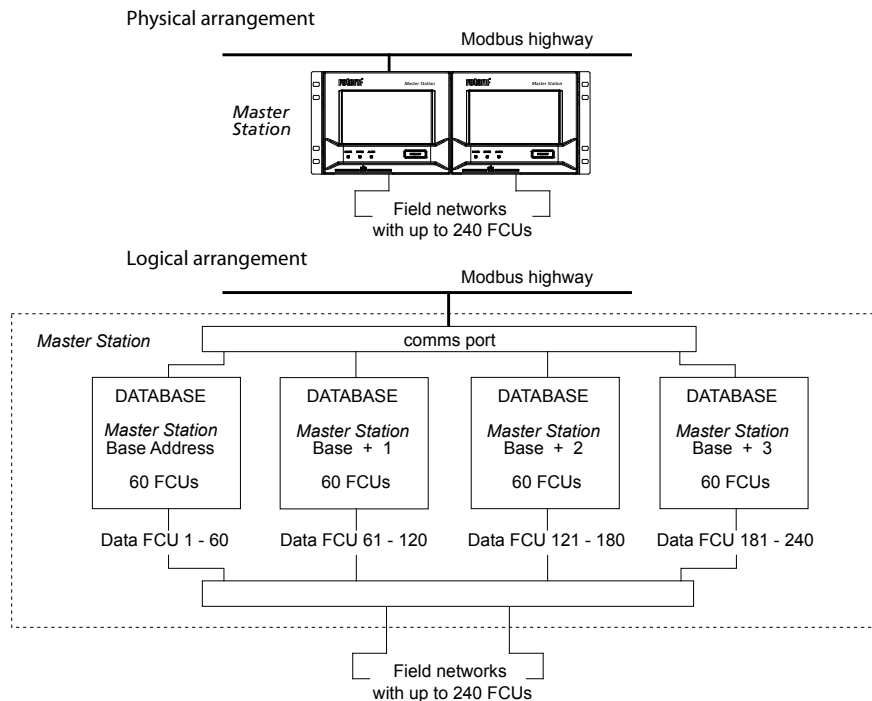


Fig 10.1.2: Master Station model – Modbus Database Generic and Honeywell EPLCG

FCU Address	Number of Modbus Addresses Master Station Responds to	Modbus Address
1 to 60	1	Base
61 to 120	2	Base + 1
121 to 180	3	Base + 2
181 to 240	4	Base + 3

Fig 10.1.3: Modbus address organisation

Examples:

Physical FCU address 10 is accessed as FCU No. 10 within Modbus Base address.
 Physical FCU address 61 is accessed as FCU No. 1 within Modbus Base address +1.
 Physical FCU address 165 is accessed as FCU No. 45 within Modbus Base address +2.

10.2 Modbus Function Code Support

Details of request and reply formats are contained in the Modbus Reference Guide. The following section deals with how *Master Stations* interpret the commands. Fig 10.2.1 lists the supported Modbus commands.

Function Code	Modbus Name	Master Station Meaning	Addressing
01	Read coil status		
02	Read input status	Read <i>Master Station</i> status	Discrete
03	Read holding registers	Read FCU status	Discrete
04	Read input registers	Read <i>Master Station</i> status	Register
05	Force single coil	Read FCU status	Register
06	Preset single register	Discrete output	Discrete
08	Loopback diagnostic test	Register output	Register
15	Force multiple coils		
16	Preset multiple registers	Multiple discrete outputs	Discrete
17	Report slave ID	Multiple register outputs	Register
43	Read device identification		

Error code	Meaning
01	Illegal function code or incorrect message length
02	Illegal data address (Register address invalid)
04	Illegal data value (value in data field out of range)
06	Slave Device Busy
0A	Gateway Path Unavailable (Modbus TCP only)

Fig 10.2.1: Modbus function codes and error codes

The function code to use will depend on whether the data is to be read as single bits or as 16 bit registers and also whether it is FCU or *Master Station* data. For example, code 01 reads *Master Station* data as discrete bits, whereas code 03 reads the same data as registers. Discrete and register access read the same data.

For discrete access, the discrete address field is interpreted as a bit offset into the database. For register access, the register address field is interpreted as a register location address in the database.

• **Function Code 01 - Read Master Station Status**

Function code 01 is used to read discrete (bit) data from the database to obtain information about the *Master Station* itself.

This function code is not generally supported for use in reading data from the database for FCU information. The exception is where the host is set up to read data from the FCU command open or close coils, for example prior to writing data, this is permitted by the *Master Station*. However, the coils do not physically exist and the data read back by the host is the current status of the Open and Close limit switch in the FCU (OAS for an Open command and CAS for a Close command). These signals may not reflect the state of the command coil. For example the FCU may have been opened by a system command to the open coil and then closed manually. The coil for open would be expected to be *on*, but the FCU will report the close coil as being *on* since CAS will be present, and the open coil as being *off*. In addition for FCU control all the write signals become pulsed outputs at the FCU and the actuator responds to these pulse commands itself.

It is possible to force the read back of the coils to always report 0 by enabling *Master Station* setting *Function Code 1 always reports zero*. This may be useful when replacing old Rotork IIE master stations.

• **Function Code 02 - Read FCU Status**

Within the *Master Station*, there are four sections of FCU database, one for each group of 60 FCUs. Access to each section is via a different Modbus slave address.

Function code 02 is used to read discrete (bit) data from the FCU database to obtain information about an FCU or group of FCUs. This function code is not supported for use in reading information about the *Master Station* itself.

• **Function Code 03 - Read Master Station Status and Read FCU Status**

Function code 03 is used to read register (16 bit) data from the database to obtain information about the *Master Station* itself. This function code may also be used to read FCU data as holding registers in the same way as function code 04.

• **Function Code 04 - Read FCU Status and Read Master Station Status**

Within the *Master Station*, there are four sections of FCU database, one for each group of 60 FCUs. Access to each section is via a different Modbus slave address.

Function code 04 is used to read register (16 bit) data from the FCU database to obtain information about an FCU or group of FCUs. This function code may also be used to read *Master Station* data as Input registers in the same way as function code 03.

• **Function Codes 05 and 06 – Write Single Coil or Register Outputs**

Function codes 05 and 06 are used when data has to be written to the *Master Station* either for action by an FCU (such as a command to open a valve) or by the *Master Station* itself (such as accept an alarm).

Although function code 05 is legal for message transactions its effect is to write data in exactly the same locations as function code 06 (all outputs from the *Master Station* occupy a 16 bit location). The calculation to determine the location for a data write using code 05 produces the same resultant location as a calculation for a register write using code 06. There is no support for writing to discrete data locations in the database, all locations are registers.

If a write request is to part of the database containing *Master Station* data, the data is written directly to that register.

If the write request is to part of the database relating to an FCU, the information in the message is translated into a command that the FCU understands and sent to the FCU over the relevant field network. The rate at which instructions are sent to the *Master Station* should not exceed the rate at which they can be sent on to the FCUs.

The sequence of events is:

- (1) - Write command received by the *Master Station*
- (2) - Response sent back to host
- (3) - Write message sent to FCU

A good response to the host indicates that the request was received correctly, the message length is acceptable, and that the addressed FCU is available. It does not indicate that the write to the FCU was successful. Confirmation of a successful write comes when new data is reported as a change in the main database.

In the case of the current loop AIM, if commands are written at too high a rate then the current loop network is prevented from collecting data from the FCUs and the system will appear to slow down. The command filter provides some protection against too high a frequency of write commands. Duplicated commands to the same FCU will be ignored if within the time setting for the filter.

• **Function Code 08 – Diagnostics**

The purpose of the loopback test is to check the communication system between the host and the *Master Station*. Only diagnostic sub codes 00 and 02 are supported.

• **Function Code 08 Sub Code 00 – Return Query Data**

The purpose of this function is to echo the request data, indicating good communications. The data in the request message is copied into the reply message.

• **Function Code 08 Sub Code 02 – Return Diagnostic Register**

The purpose of this function is to return information about the status of the *Master Station* sides; which side is in control and which unit is the back up. The returned data register is decoded as follows:

Register	Value
Low Byte – Right side	0 = Unknown
	1 = Backup and in Alarm
	2 = Backup and OK
	3 = Main and in alarm
	4 = Main and OK
High Byte – Left side	0 = Unknown
	1 = Backup and in Alarm
	2 = Backup and OK
	3 = Main and in Alarm
	4 = Main and OK

• **Function Code 15 and 16 - Write Multiple Outputs**

Function codes 15 and 16 may be used when data has to be written to more than one register in the *Master Station* either for action by an FCU (such as a command to open a valve) or by the *Master Station* itself (such as accept an alarm).

Although function code 15 is legal for message transactions, its effect is to write data in exactly the same locations as function code 16 (all outputs from the *Master Station* occupy a 16 bit location). The calculation to determine the location for a data write using code 15 produces the same resultant location as a calculation for a register write using code 16. As with single instructions there is no support for writing data to discrete data locations, all locations are registers.

The *Master Station* is able to accept a single transaction multiple write message containing information to be written to a maximum of 123 registers. These instructions are then passed to a queue for onward transmission over the current loop network. The rate at which the data is written into the *Master Station* must not exceed the rate at which it can be sent on to the FCUs. The command filter will remove duplicated commands in the same way as for function code 01 writes.

In the case of actuator control there is never a need to write to turn a register or coil *off* as the output is always treated as a pulse. If commands to turn off registers are sent these will be obeyed by the system with no actual result, the output already having turned off. Sending these unnecessary commands will congest communication on the current loop network.

• **Function Code 17 - Report Slave ID**

The response format is:

Byte count field	- 6
Slave ID field	- 40
Runlight field	- 255
Device dependent data (4 bytes)	- HW version (16 bits) - SW version (16 bits)

• **Function code 43 – Basic Device Identification**

Function code 43 permits reading of the identification of a Modbus device. The Read Device Identification interface is modelled as an address space composed of a set of addressable data elements. The data elements are called objects and an object ID identifies them.

There are three categories of objects (Basic, Regular and Extended) the *Master Station* only supports the Basic Device Identification object, which consists of Vendor Name, Product Code and Revision Number.

A function code 43 Basic Device ID request has the following data:

Function code	1 Byte	0x2B
MEI Type	1 Byte	0x0E (Device ID Request)
Read Device ID Code	1 Byte	01/02/03/04
Object ID	1 Byte	0x00 to 0xFF

Where the Read Device ID Code value is:

ID	Function	Comment
01	Request to get the basic device identification	
02	Request to get the regular device identification	Not Supported
03	Request to get the extended device identification	Not Supported
04	Request to get one specific identification object	

The Object ID defines the data:

Object Id	Object Name / Description	Type	Rotork Data	Category
0x00	VendorName	ASCII String	Rotork	Basic
0x01	ProductCode	ASCII String	Rotork <i>Master Station</i>	
0x02	MajorMinorRevision	ASCII String	V### (#####)	

Example for the *Master Station* using Read device ID code 01:

Function code	1 Byte	0x2B
MEI Type	1 Byte	0x0E (Device ID Request)
Read Device ID Code	1 Byte	01
Object ID	1 Byte	0x00

Response:

Function code	1 Byte	0x2B
MEI Type	1 Byte	0x0E (Device ID Request)
Read Device ID Code	1 Byte	01
Conformity level	1 Byte	01
More Follows	1 Byte	00
Next Object ID	1 Byte	00
Number of Objects	1 Byte	03
Object ID	1 Byte	00
Object Length	1 Byte	0x10
Object Value	Object Length	Rotork
Object ID	1 Byte	01
Object Length	1 Byte	0x12
Object Value	Object Length	Rotork <i>Master Station</i>
Object ID	1 Byte	02
Object Length	1 Byte	0x0D
Object Value	Object Length	V### (#####)

• **Error Codes 01, 02, 04, 06 and 0A**

Error code 01 will be presented back to the host if the function code in the data message is not one of those supported by the *Master Station*, or if the message length is incorrect.

Error code 02 will be presented back to the host if the data address is illegal; or if the write command is a multiple write (code 15 or 16) where the number of coils or registers exceeds the amount acceptable.

Error code 03 will be presented back to the host if the value contained in the data query field is illegal.

Error code 06 will be presented back to the host if the *Master Station* has insufficient buffer space to handle the write request to coils or registers in a single transaction. Buffer space will become free as the writes are issued to the loop and FCUs.

Error code 0A will be presented back to the host if the *Master Station* is unavailable or if the modbus TCP slave address in the message is not the same as the modbus TCP slave address set in the *Master Station*.

10.3 Database Access

Each *Master Station* contains database records relating to itself and the FCUs on the networks connected to it.

10.3.1 Data Organisation

The database comprises a series of records organised into blocks and parameters. Each parameter contains 16 bits of data. A block consists of 8 parameters. There are 32 blocks of data about the *Master Station* itself and 32 blocks of data for each FCU on the current loop.

The data to be found in each record is listed in Section 10.5 for the *Master Station* and in Section 10.6 for the FCUs.

10.3.2 Data Read Requests

If the request is for several registers, the address defines the start point for a group of blocks and parameters. The contiguous records in these registers are either associated with the *Master Station*, or with a group of FCUs. This is particularly useful to collect the Alarm information from all FCUs connected to one *Master Station* in a single Modbus transaction. The alternative is to collect it with multiple transactions, one for each FCU address in use.

10.3.3 Register and Discrete Address Formulae

The following formulae allow discrete and register addressing to be calculated. Refer to Section 10.2 to determine the meaning of particular bits and parameters.

To use these formulae, first decide which bits and registers of information need to be collected, and which need to be written to. This will provide FCU, block, parameter and bit numbers for use in the equations. The Modbus address for the particular *Master Station* also has to be known. The FCU addresses will all be in the range 1-60 even if there are more than 60 FCUs connected. The *Master Station* address increments for each successive group of 60. Next, decide if register or discrete reads and writes are to be used and then determine the function code applicable. Finally, calculate the relevant start point in the database using the information below.

Modbus Slave Address = *Master Station* base address (for physical FCUs 1-60)
= *Master Station* base address + offset (for physical FCUs above 60)

- **Function code 01: Read *Master Station* Status by Bits**
 Start Discrete = $(128 \times B) + (16 \times P) + D$ (see Note 1)
- **Function code 02: Read FCU Data by Bits – Only applies to Blocks 0 to 7**
 Start Discrete = $(7680 \times P) + (960 \times B) + (16 \times [N-1]) + D$ (see Note 1)
- **Function code 03: Read *Master Station* Status by Register**
 Start Register = $(8 \times B) + P$
- **Function code 04: Read FCU Data by Register**
 Start Register = $256 + (480 \times B) + (60 \times P) + (N-1)$
- **Function code 05 or 15: Write *Master Station* Data by Single or Multiple Bits**
 Start Coil = $(8 \times B) + P$ (see Note 2)
- **Function code 05 or 15: Write FCU Data by Single or Multiple Bits**
 Start Coil = $256 + (480 \times B) + (60 \times P) + (N-1)$ (see Note 2)
- **Function code 06 or 16: Write *Master Station* Data by Single or Multiple Register**
 Start Register = $(8 \times B) + P$ (see Note 2)
- **Function code 06 or 16: Write FCU Data by Single or Multiple Register**
 Start Register = $256 + (480 \times B) + (60 \times P) + (N-1)$ (see Note 2)

In the formulae above, the following symbols are used:

- N = FCU address (range 1 to 60)
- B = Block number
- P = Parameter number
- D = Data bit number within parameter (register).

• **Note 1 - Limited address range**

This formula (reading discrete FCU data) has been carefully designed to allow for Modbus hosts that have a limited address range. Parameter 0 has the most useful data and is located near the top end of the address field.


• **Note 2 - Writing data**

The *Master Station* recognises write requests to both coils and registers. When calculating the location of the coil or register to be written to, the start location is the same for both types of *write*. The *Master Station* considers coils and registers to be the same; they are always a whole parameter. There is no support for writing to an individual bit within a parameter.

Where multiple writes are used, the maximum number that may be written in a single transaction is 123 registers. If the host attempts to write more than this or the internal buffer is full, error code 02 is returned by the *Master Station* and no action is taken.

The rate at which data is written should not exceed the rate at which it can be transferred to the current loop network.

• **Note 3 - Address offsets**

 This table and the examples are for a typical Modbus implementation only. Check your system documentation carefully.

The discrete and register addresses calculated in the formulae are those which should appear in the messages as they are transmitted on the Modbus link to the *Master Station*. Some Modbus hosts offset addresses. In such cases, the address programmed by the user into the host would be different from those calculated. Check host system documentation carefully.

Typical offsets are:

Function Code	Offset to be added to formulae result
1	1
2	10001
3	40001
4	30001
5	1
6	40001

Examples:

- 1) Calculate an FCU bit address to read as 1920. Use function code 02, so add 10,001 to get the number to programme into the host system. The result is 11,921.
- 2) Calculate a *Master Station* bit address to write to as 5. Use function code 05, so add 1. The resulting number to be programmed into the host system is 6.

• **Note 4 - FCU number in formulae**

In the formulae the FCU addresses are the offsets within each section of the virtual database. Remember that a *Master Station* appears as four independent slaves (four logical units) from a Modbus point of view..

• **Note 5 - Discrete addressing range**

A discrete address needs to be 16 times the register address to access the same parameter. Because of the limited size of the discrete address field in the Modbus message, discrete addresses can only reach parameters associated with low number registers.

10.4 Notes on the use of the Generic and EPLCG Modbus Protocol

Normally a Modbus host will be set up to cyclically read data representing key variables of the *Master Station* and FCUs. It can do this using read register function codes (03 and 04), and read discrete status function codes (01 and 02).

Parameters may contain either digital (bit) information or analogue (register) information. For digital records the Modbus discrete addressing commands are appropriate. For analogue information the Modbus register address commands should be used.

Register and discrete addresses in this specification are the addresses that should be used within messages on the Modbus data link. Modbus host software **may** need to be configured with addresses that are 1 more than those which must appear on the link. This is due to the host regarding addresses as starting from 1, not 0.

Reading a group of registers in one transaction is more efficient than reading one register at a time.

Support for Modbus diagnostic code (function code 08) is provided, but it is not obligatory to use it.

The *Master Station* includes alarm accept logic with respect to FCU alarms. Alarms from FCUs are automatically accepted by the *Master Station* (so the FCU can clear its alarm latches) and latched within the *Master Station*. These alarms must be read by the host and then accepted (with an alarm accept write, to *Master Station* block 0 parameter 5), before they are cleared..

10.4.1 Suggested Scan Cycle

The host should be configured to scan data from the *Master Station* in the following order:

- Read alarm status
- Read digital status
- Perform alarm accept (strictly necessary if any new alarms have occurred)
- Read analogue status (if any analogue data is to be read)

Commands to FCUs may be fitted in as required.

In some applications it may be desirable to scan some items less frequently than others. This is perfectly acceptable.

10.4.2 Writing to Coils

When writing to a coil, the data field to turn off the coil has to be 0x0000. As the most common device connected is an actuator whose action is controlled by a pulse output, there is often no need to turn off a coil that has previously been turned on. The output command from the DCS should, where possible, use a pulse type output. When writing to a coil the data field to turn ON the coil may be 0xFF00 or any other non zero value.

10.4.3 Readback of Holding Registers

The *Master Station* supports the reading of the data in the Holding Registers. This data may not accurately reflect the state of some older version actuators which could not recognise manual movement, as they may have been moved manually since the data was last updated by the network. The data is a 2's complement 16 bit value (0x0000 – 0x7FFF in the case of the Generic protocol or 0x0000 – 0x0FFF in the case of the Honeywell EPLCG). It is calculated from the actual value used in the data transaction over the current loop network to the FCU. When read back this value may differ by 1 digit due to rounding errors in the calculation. The value sent to the FCU when the register was written will be true. To establish the actual valve position the Input Register relating to the FCU Measured Value should be read.

10.4.4 Alarm Handling

The serial communication ports on the *Master Station* are each served by their own independent database and alarm handling. The handling of alarms on one serial port does not reflect on the alarms of any other serial port unless the *Master Station* is set to link the alarms. The two Ethernet ports on a *Master Station* share another independent database with its own alarm handling which is common to both Ethernet ports.

In the database there is a group of 16 bits of data defined as the *alarm block* for each FCU. These data bits will all be latched by the *Master Station* should they occur. The *Master Station* will therefore capture a transient alarm and keep it in its database ready for the host to read it.

Any latched alarm from these data areas will only be reset on the subsequent conditions. The alarm bit must be read by the host, the alarm bit must be accepted by the host (this is done by issuing an *alarm accept*), and the source of the alarm must return to normal.

An example of the sequence would be:

Consider an actuator thermostat.

1. Actuator motor gets excessively hot and trips the thermostat.
2. Host reads data bit for the thermostat for this actuator.
3. Host issues alarm accept; this is registered by the system as applicable to the thermostat trip alarm.
4. The data bit remains set until the actuator cools down.
5. The data bit returns to normal once the actuator has cooled and the thermostat is automatically reset.

If the host does not read the *thermostat* bit for this FCU then the bit will remain set (in this database), even though the actuator cools down and the actual thermostat resets. Also if the host does not read this bit, any *alarm accept* will not allow the alarm to reset itself. Any alarm bit must be read before it is able to be accepted.

If the alarms are read infrequently then the above procedure guarantees that the host will register any and every alarm from the *alarm block*.

In addition to the alarm data for each FCU there is a *status block*. The status block also contains information about the presence (or absence) of alarms in the *alarm block*.

- **Alarm bit**

For each FCU the *alarm* bit will be present if any of the source signals used to set bits in the *alarm block* are present. Notice that the *alarm* bit is an OR function of any alarm before the latch for that alarm. The *alarm* bit is latched and will not clear until it has been read, accepted and the source of the alarm has returned to normal. In the example of the thermostat, the *alarm* bit will be set when the thermostat is initially tripped.

- **New alarm Bit**

For each FCU *new alarm* will be present every time a new alarm occurs in the FCU. However, every time an *alarm accept* is issued, this data bit will be reset even if the alarm itself is still present.

The purpose of this bit is to indicate to the *host* there is a new alarm to be read from the *alarm block*.

- **System Common Alarms**

In the *Master Station* block 0 parameter 0, bit 2 will be set if any FCU has its own *alarm* bit set. Thus the *common FCU alarm* is set while any one FCU has an input actually in alarm, or if there is an FCU unavailable for communication.

Block 0 parameter 0, bit 3 contains a similar common data bit derived from the actuator *monitor relay* source signals.

10.4.5 Use of Alarm Bits

The host may be configured to read as many, or all, of the alarm block data bits as required. Those that are not being used will possibly fill up as alarms over the course of operating the system; this will not have any detrimental effect on system performance.

Actively used alarms will individually appear in the data locations being read and transferred to the host via the *alarm accept* process. They will also reset themselves as they return to normal providing they are read and accepted.

The *alarm* bit will inform the host that any alarm is present, even those not normally being identified by the host as relevant. This bit may be used by the host as a flag that an alarm is currently present on an FCU. The host must take care of latching these bits in its own alarm handling system. This bit is comparable to a contact input that is self-resetting. As it is taken from before the internal latch, it is a true statement of the current alarm situation on the FCU.

The *new alarm* bit may be used to indicate to the host that an alarm reading process is required, or that an *alarm accept* write is required. The *new alarm* will by its very nature disappear once the *alarm accept* is issued irrespective of the actual plant status as it has to be available for each new alarm.

10.5 Master Station Database

The discrete and register numbers listed in the tables all start from 0, for example register 40000 would be referenced as 0000 in the serial transaction message and not as 0001.

10.5.1 Master Station Read Only Data

This set of registers exists in each of the 'logical' Master Stations that exist within a single physical Master Station. The Modbus address used in transactions must be the Master Station base address. Reading data from any one of the addresses is the same as any other as all four contain the same data. All the location numbers listed are decimal numbers and zero based.

BLOCK 0 – Read Only Data (accessed with Modbus function code 01, 03 or 04)		Register Location
Parameter 0 – System Status and Alarm		0
		Discrete Location
Bit 0	Loopback in Progress	0
Bit 1	Loopback in Use	1
Bit 2	Common FCU Alarm	2
Bit 3	Common Actuator Alarm	3
* Bit 4	0 = A side, 1 = B Side	4
Bit 5	ESD Mode	5
Bit 6	Reserved	6
* Bit 7	1 = Primary, (In Use), 0 = Standby, (Out of Use)	7
Bit 8	Failure On Start-up	8
Bit 9	Reserved	9
Bit 10	Power On Reset	10
Bit 11	Reserved	11
Bit 12	Auto-Loopback Occurred	12
Bit 13	FCU in Comms Fail	13
* Bit 14	Master Station Side A OK (main unit, left side)	14
* Bit 15	Master Station Side B OK (standby unit, right side)	15
		Register Location
Parameter 1 - FCU on loop to Scan up to Data = XXXX, Highest FCU Address		1
Parameter 2 - Loop Baud Rate Code 1 = 110 Baud 2 = 300 Baud 3 = 600 Baud 4 = 1200 Baud 5 = 2400 Baud 6 = 4800 Baud		2
Parameter 3 - Incremental Count A counter that increments approximately every 0.1 second		3

Note: Data bits marked * are not relevant to single Master Station

Side A and B OK indication is determined by the health of the particular side of the Master Station. For example, if any AIMs are fitted but are faulty this will register as a Master Station side not OK. If Side B cannot be communicated with, it will be reported as not OK through the register reads on Side A.

BLOCK 0 – Read Only Data (accessed with Modbus function code 01, 03 or 04)		Register Location
Parameter 4 - Loop Fault Information Bits 15-12 Loop Address Faults Bit 15 0 = Port A, 1 = Port B Bit 14 Duplicate Address found Bit 13 Address Too High found Bit 12 Zero Address found Bit 11-8 Loop fault type 5 = Loop open circuit 6 = Loop short circuit Bits 7-0 Reason why loop last configured 1 = Reset occurred 2 = FCU found at address zero 3 = FCU found at too high address 4 = Two FCU's at same address found 5 = Loop fault on outward wire (loop complete) 6 = Loop fault found on Side A (loopback in use) 7 = Loop fault found on Side B (loopback in use) 8 = Test of <i>return</i> wire failed 9 = Loop configure command received		4
Parameter 5 - FCU Address Fault data Bits 15-8 Loop position of address fault Bits 7-0 Offending address		5
Parameter 6 - Loop Configuration Progress 1 = Wait for loopbacks 1 2 = Find FCU's on Port A 3 = Test loop 4 = Find FCU's on Port B 5 = Wait for loopbacks 2 6 = Loopbacks off on Port A 7 = Loopbacks off on Port B 8 = Program Baud Rate on Port A 9 = Program Baud Rate on Port B		6
Parameter 7 – Number of FCU's found in Loop Configuration Bits 8-15 Number of FCU's on Port B Bits 0-7 Number of FCU's on Port A		7

BLOCK 1 to 15 – Read Only Data (accessed with function code 03 or 04)		Register Location
Parameter 0-7 FCU Map 240 8-bit fields with the address of each connected FCU, in the order in which they are connected, e.g. Block 1 Parameter 0 Bits 8 to 15 Address of first FCU Bits 0 to 7 Address of second FCU		0008 to 0127

BLOCK 16 to 30 – Read Only Data (accessed with function code 03 or 04)		Register Location
Parameter 0-7 FCU Failure Counts 240 8-bit fields with the failure count for one FCU. Incremented on each comms failure. e.g. Block 16 Parameter 0 Bits 8 to 15 Failure count for FCU 1 Bits 0 to 7 Failure count for FCU 2		0128 to 0247
BLOCK 31 - Read Only Data (accessed with Modbus function code 03 or 04)		Register Location
Parameter 0 – Command Filter timeout (seconds), default value depends on loop speed Loop speed: 110 baud Filter Time: 60 seconds 300 30 600 15 1200 10 2400 5		248
Parameter 1 - Master Station Type 1 = Pakscan IIE 2 = Pakscan IIS 3 = Pakscan 3 4 = Pakscan 4		249
Parameter 2 - Master Station Type Identifies the number of channels and if unit is Hot Standby Bits 8-15 1 = single unit, 2 = hot standby Bits 0-7 0 = 32 channel 1 = 60 channel 2 = 120 channel 3 = 180 channel 4 = 240 channel		250
Parameter 3 - Loop Interface card Software Version Number (see note below)		251
Parameter 4 - FCU's in Loopback at FCU (x) and FCU (y) [zero = none present] Bits 0-7 = FCU (x) Bits 8 - 15 = FCU (y)		252
Parameter 5 - Loop Test Speed Bits 0-7 1 = 110 baud 2 = 300 baud 3 = 600 baud 4 = 1200 baud 5 = 2400 baud		253
Parameter 6 - Loop Test Result in Percent 0000-0x0064)		254
Parameter 7 - FCU Data Upload Progress 0 = FCU data upload not started 255 = FCU data upload complete Other values indicate FCU currently being read		255

Note on software version numbers:
 Software version numbers should be interpreted as 4 digits stored within the register.
 Bits 15 to 8 contain the major release number and bits 7 to 0 contain the minor release number e.g. 0x0156 will be version 01.5.6

10.5.2 *Master Station Write Only Data*

Only a few addresses accept write commands from a Modbus host. All except those listed below return an error code. The written data may be any value (except zero) to achieve the desired action. The *Master Station* considers all writes to be to registers, even when a coil function code command is used.

BLOCK 0 - Write Only Data (accessed with Modbus function code 05, 15, 06 or 16)	Register Location
Parameter 3 - Reconfigure Loop Data = any non-zero value to reconfigure	3
Parameter 4 - Change Main to Standby and vice versa * Data = any non-zero value to change	4
Parameter 5 - Alarm Accept Data = any non-zero value to Accept	5
Parameter 6 - Send ESD Command on Loop Data = any non-zero value to send ESD	6

BLOCK 31 - Write Only Data (accessed with Modbus function code 05, 15, 06 or 16)	Register Location
Parameter 7 – Start FCU Data Upload Data = any non-zero value to start upload	255

Attempting to read back from these locations will only return read only data and will not give a value for these locations.

*Writing a command to parameter 4 is only applicable to a hot standby *Master Station*.

10.6 FCU Database

Data within the system is organised in blocks and parameters relating to specific functions or activities within the FCU on the current loop (e.g. digital inputs, alarms, position control). Each FCU supports up to 32 blocks with each block containing eight 16-bit parameters, though not all these blocks contain relevant data. The *Master Station* maintains the database for all the FCUs on the current loop without the need for any action from the host. This section details the use of these blocks and parameters in the transfer of data between the *Master Station* and host.

Within the FCU database certain areas are restricted to read only (RO), others to write only (WO), and some that are both read and write (R/W).

It is permissible to use function code 02 for single discrete bit (or multiple bits) reads or function code 04 for register (or multiple registers) reads for any data within the database. It is usual to use register reads where the data is an analogue value. A group of 16 bits in 1 parameter may be read as a register.

When writing data all locations are treated as registers. Function codes 05, 15, 06, or 16 may be used and the location to which data is written is always the register location. For relay outputs the data to turn off a relay is always 0000h and any non-zero value will turn the relay on. For example values of 0001h, FF00h, or 00FFh will all energise the relay.

The registers are transmitted Most Significant Data Byte first.

- **Digital Inputs**

Each FCU has direct digital inputs from the connected actuator and the status is reported in the *digital input block* (block 2 parameter 0). The *digital input block* also contains indication of any alarms present in the *alarm block*.

- **Alarm Block**

The *alarm block* holds data about alarms either directly connected to the FCU, or logically derived from the status of all the inputs. These *alarms* data bits are individually latched by the *Master Station* and will not return to normal until both the source alarm condition is corrected and the alarm is both read and accepted by the host.

- **Analogue and Counter Input**

The FCU will report analogue or counter values to the *Master Station* only when the measurement changes by an amount that exceeds the *deviation* setting by 1 digit, or the *update timeout* period has expired. These parameters are adjusted locally within the FCU and included in the system to ensure that analogue reporting only occurs when necessary. The host has access to the last reported analogue value in the *Master Station*.

- **Outputs**

The *Master Station* transfers both digital and analogue outputs from the host computer directly to the connected FCU. There are no registers holding output data present within the *Master Station* itself.

- **FCU Types Available**

IQ Range Actuator	IQ and IQT actuators
CK Range Actuator	CK Atronik and CK Centronik actuators
INTEGRAL	Actuator control integral to the actuator used for older products i.e. A, AQ and Q range
GPFCU (GP)	General Purpose version of GPFCU
GPFCU (Act)	Actuator Control version of GPFCU
IQ Analogue	Analogue input card for IQ range only
EH	EH actuator
SI	SI actuator
CVA	CVL or CVQ actuator
CMA	CMA actuator
ROMpak	ROMpak actuator

- **Key to Symbols Used**

RO	Read Only
R/W	Read / Write
WO	Write Only
Y	Item supported for this type of FCU
R	Reserved for internal or future use
BLANK	A blank entry indicates the item is not supported for the FCU type. Reads of that item generally return zero.
Register Location	The decimal number of the register for FCU address 1, 2 and 60, for the parameter indicated.
Discrete Location	The decimal number of the discrete bit for FCU address 1, 2 and 60, for the parameter and bit indicated.

10.6.1 FCU Database Locations

Read Write	FCU Type									Data Location			
	IQ, CK, SI Ranges	A, AQ, Q, ROMpak	GPFCU (GP)	GPFCU (ACT)	CVA	EH / SI	CMA	IQ Analogue	FCU 1	FCU 2	to	FCU 60	

Block 0 – FCU Type Block

(accessed with Modbus function code 03 or 04)

										Register Location			
Parameter 0 - 7	RO	Y	Y	Y	Y	Y	Y	Y	Y	256	257	-	735

Block 1 – FCU Block

(accessed with Modbus function code 03 or 04)

										Register Location			
Parameter 0 - 7	-	R	R	R	R	R	R	R	R	736	737	-	1215

Block 2 – Digital Input Block

(accessed with Modbus function code 02, 03 or 04)

										Register Location			
Parameter 0	RO	Y	Y	Y	Y	Y	Y	Y	Y	1216	1217	-	1275

Discrete Location

Bit 0	RO	AUX 1	R (AUX1*)	DIN 1	R	R	AUX 1	R	R	1920	1936	-	2864
Bit 1	RO	AUX 2	R (AUX2*)	DIN 2	R	BAKPWR	AUX 2	R	R	1921	1937	-	2865
Bit 2	RO	OAS	OAS	DIN 3	OAS	OAS	OAS	OAS	R	1922	1938	-	2866
Bit 3	RO	CAS	CAS	DIN 4	CAS	CAS	CAS	CAS	R	1923	1939	-	2867
Bit 4	RO	STOP	STOP	DIN 5	STOP	STOP	STOP	R	R	1924	1940	-	2868
Bit 5	RO	MOVE	MRUN	DIN 6	MRUN	MOVE	Travelling	MOVE	R	1925	1941	-	2869
Bit 6	RO	MRO	MRO	DIN 7	MRO	TRO	TRO	R	R	1926	1942	-	2870
Bit 7	RO	MRC	MRC	DIN 8	MRC	TRC	TRC	R	R	1927	1943	-	2871
Bit 8	RO	AUX 3	EXT (AUX3*)	R	EXT	R	AUX 3	R	R	1928	1944	-	2872
Bit 9	RO	AUX 4	R (AUX4*)	R	R	R	AUX 4	R	R	1929	1945	-	2873
Bit 10	RO	LBON	LBON	LBON	LBON	LBON	LBON	LBON	LBON	1930	1946	-	2874
Bit 11	RO	NALRM	NALRM	NALRM	NALRM	NALRM	NALRM	NALRM	NALRM	1931	1947	-	2875
Bit 12	RO	ALRM	ALRM	ALRM	ALRM	ALRM	ALRM	ALRM	ALRM	1932	1948	-	2876
Bit 13	RO	BATT	R	R	R	BAKBATT	R	R	R	1933	1949	-	2877
Bit 14	RO	Remote**	R	R	R	R	R	R	R	1934	1950	-	2878
Bit 15	RO	R	R	R	R	R	R	R	R	1935	1951	-	2879

										Register Location			
Parameter 1 - 7	-	R	R	R	R	R	R	R	R	1276	1277	-	1695

Key to Digital Input Labels:

AUX 1-4	-	Aux Input 1-4	TRO	-	Travelling open direction
OAS	-	Open limit switch	TRC	-	Travelling close direction
CAS	-	Close limit switch	DIN 1 to 8	-	Digital inputs 1 to 8
STOP	-	Actuator stopped in mid travel	EXT	-	External contact input
MOVE	-	IQ/IQT valve moving	LBON	-	Loopback on
MRUN	-	Motor running	NALM	-	New alarm flag
MRO	-	Motor running open direction	ALARM	-	Any alarm present on this FCU
MRC	-	Motor running close direction	BATT	-	Battery Low Indication
Travelling	-	Actuator moving	Remote	-	remote selected
BAKPWR	-	Under battery back-up power	BAKBATT	-	Back-up battery low indication

Note: When using the GPFCU (GP) for pump control the following arrangement is used:
 DIN1 - Represents Monitor2
 DIN2 - Represents Monitor3
 DIN3 - Represents Motor Running
 DIN4 - Not assigned
 DIN5 - Represents Motor Stopped
 DIN6 - Represents Monitor1
 DIN7 & 8 - Not assigned
 all other allocations are unchanged

Notes: (AUXn*) ROMpak only, ** IQ range 3rd generation only (IQ3 and IQ3 Pro ranges)

Read Write	FCU Type									Data Location			
	IQ, CK, SI Ranges	A, AQ, Q, ROMpak	GPFCU (GP)	GPFCU (ACT)	CVA	EH / SI	CMA	IQ Analogue	FCU 1	FCU 2	to	FCU 60	

**Block 3 – Alarm Block
(accessed with Modbus function code 02, 03 or 04)**

										Register Location			
Parameter 0	RO	Y	Y	Y	Y	Y	Y	Y	Y	1696	1697	-	1755
										Discrete Location			
Bit 0	RO	MEMF	MEMF	MEMF	MEMF	MEMF	MEMF	R	MEMF	2880	2896	-	3824
Bit 1	RO	COMMS	COMMS	COMMS	COMMS	COMMS	COMMS	COMMS	COMMS	2881	2897	-	3825
Bit 2	RO	LOCAL	CNA	R	CNA	LOCAL	LOCAL	LOCAL	R	2882	2898	-	3826
Bit 3	RO	POWR	POWR	POWR	POWR	POWR	POWR	POWR	POWR	2883	2899	-	3827
Bit 4	RO	WDOG	WDOG	WDOG	WDOG	WDOG	WDOG	WDOG	WDOG	2884	2900	-	3828
Bit 5	RO	MREL	MREL	R	MREL	MREL	MREL	MREL	R	2885	2901	-	3829
Bit 6	RO	THERM	THERM	R	THERM	THERM	FAULT	R	R	2886	2902	-	3830
Bit 7	RO	LSTOP	LSTOP	R	LSTOP	LSTOP	LSTOP	LSTOP	R	2887	2903	-	3831
Bit 8	RO	SFAIL	SFAIL	R	SFAIL	SFAIL	SFAIL	SFAIL	R	2888	2904	-	3832
Bit 9	RO	VOBS	VOBS	R	VOBS	VOBS	VOBS	VOBS	R	2889	2905	-	3833
Bit 10	RO	VJAM	VJAM	R	VJAM	VJAM	VJAM	R	R	2890	2906	-	3834
Bit 11	RO	AUXOR	MOP	R	MOP	R	AUXOR	R	R	2891	2907	-	3835
Bit 12	RO	VTT	MCL	R	MCL	RL	VTT	R	R	2892	2908	-	3836
Bit 13	RO	R	MOPG	R	MOPG	R	R	R	R	2893	2909	-	3837
Bit 14	RO	MMOVE	MCLG	R	MCLG	MMOVE	MMOVE	R	R	2894	2910	-	3838
Bit 15	RO	EOT	EOT	R	EOT	EOT	EOT	R	R	2895	2911	-	3839
										Register Location			
Parameter 1 - 7	-	R	R	R	R	R	R	R	R	1756	1757	-	2175

- Key to Alarm Labels:**
- | | | |
|--|-------------------------------|--|
| MEMF - RAM/ROM failure | MREL - Monitor relay | MOP - Manual open |
| COMMS - Comms fail | THERM - Thermostat trip | MCL - Manual close |
| LOCAL - Actuator not in remote control | LSTOP - Local stop operated | MOPG - Manual opening |
| CNA - Control not available | SFAIL - Start/stop fail | MCLG - Manual closing |
| POWR - Power on reset | VOBS - Valve obstructed | EOT - Motor running end of travel |
| WDOG - Watchdog fail | VJAM - Valve jammed | FAULT - Fault relay, any fault present |
| | MMOVE - Manual valve movement | |

**Block 4 – Analogue Input Block - Valve Position Feedback
(accessed with Modbus function code 03 or 04)**

										Register Location			
Para' 0 (MV)	RO	Y	Y	R	Y	Y	Y	Y	R	2176	2177	-	2235
MV Range: Using Generic Protocol , 0x0000 = 0%, 0x7FFF = 100% position Using EPLCG Protocol , 0x0000 = 0%, 0x0FFF = 100% position													
Parameter 1 - 7	-	R	R	R	R	R	R	R	R	2236	2237	-	2655

**Block 5 – Position Control Block – Valve Desired Position
(accessed with Modbus function code 03 or 04, writes with 06 or 16)**

										Register Location			
Parameter 0	-	R	R	R	R	R	R	R	R	2656	2657	-	2715
Para' 1 (DV)	R/W	Y	Y	R	Y	Y	Y	Y	R	2716	2717	-	2775
DV Range: Using Generic Protocol , 0x0000 = 0%, 0x7FFF = 100% Desired pos'n Using EPLCG Protocol , 0x0000 = 0%, 0x0FFF = 100% Desired pos'n													
Parameter 2 - 7	-	R	R	R	R	R	R	R	R	2776	2777	-	3135

Read Write	FCU Type									Data Location			
	IQ, CK, SI Ranges	A, AQ, Q, ROMpak	GPFCU (GP)	GPFCU (ACT)	CVA	EH / SI	CMA	IQ Analogue	FCU 1	FCU 2	to	FCU 60	

Block 6 – Digital Output Block

(accessed with Modbus function code 01, 03, 04)

										Register Location			
Parameter 0	RO	R	R	Y	R	R	R	R	R	3136	3137	-	3195
										Discrete Location			
Bit 0	RO	-	-	RLY4	-	-	-	-	-	5760	5776	-	6704
Bit 1	RO	-	-	RLY1	-	-	-	-	-	5761	5777	-	6705
Bit 2	RO	-	-	RLY3	-	-	-	-	-	5762	5778	-	6706
Bit 3	RO	-	-	RLY2	-	-	-	-	-	5763	5779	-	6707
Bit 4	RO	-	-	0	-	-	-	-	-	5764	5780	-	6708
Bit 5	RO	-	-	0	-	-	-	-	-	5765	5781	-	6709
Bit 6	RO	-	-	0	-	-	-	-	-	5766	5782	-	6710
Bit 7	RO	-	-	ACT (1)	-	-	-	-	-	5767	5783	-	6711
Bit 8 to 15	-	-	-	R	-	-	-	-	-	5768-75	5784-91	-	6712-19

(accessed with Modbus function code 01, 03, 04, writes with 05, 15, 06 or 16)

										Register Location			
Parameter 1 - Open	R/W	Y	Y	Y	Y	Y	Y	Y	N	3196	3197	-	3255
Open (Relay 2) : 0x0000 = De-energise 0xFF00 or any non-zero value = Energise relay													
Parameter 2 - Stop	R/W	Y	Y	Y	Y	Y	Y	Y	N	3256	3257	-	3315
Stop (Relay 3) : 0x0000 = De-energise 0xFF00 or any non-zero value = Energise relay													
Parameter 3 - Close	R/W	Y	Y	Y	Y	Y	Y	Y	N	3316	3317	-	3375
Close (Relay 1) : 0x0000 = De-energise 0xFF00 or any non-zero value = Energise relay													
Parameter 4 - ESD	R/W	Y	Y	Y	Y	Y	Y	Y	N	3376	3377	-	3435
ESD (Relay 4) : 0x0000 = De-energise 0xFF00 or any non-zero value = Energise relay													
Parameter 5 - Partial Stroke Test	R/W	Y (Note 1)	N	N	N	N	N	N	N	3436	3437	-	3495
PST : 0x0000 = De-energise 0xFF00 or any non-zero value = Energise relay													
Parameter 6 - 7	-	R	R	R	R	R	R	R	N	3496	3497	-	3615

(1) Key: ACT = Relay action, 0 = Fleeting, 1 = Maintained

Notes: Partial Stroke only IQ3 and CK, software version V209 or later.

Read back of Open and Close registers returns the state of the actuator limit when enabled in the *Master Station*.

Block 7 – Pulse Input Block

(accessed with Modbus function code 03 or 04)

										Register Location			
Parameter 0	RO	-	-	-	Y	-	-	-	-	3616	3617	-	3675
Range: 0x0000 to 0x270F = Counter value													
Parameter 1 – 7	-	R	R	R	R	R	R	R	R	3676	3677	-	4095

Read Write	FCU Type									Data Location			
	IQ, CK, SI Ranges	A, AQ, Q, ROMpak	GPFCU (GP)	GPFCU (ACT)	CVA	EH / SI	CMA	IQ Analogue	FCU 1	FCU 2	to	FCU 60	

**Block 8 – Digital Output operation
(accessed with Modbus function code 01, 03, 04, writes with 05, 15, 06 or 16)**

										Register Location			
Parameter 0	-	R	R	R	R	R	R	R	R	4096	4097	-	4155
Parameter 1 -	R/W	Y	R	R	R	R	R	R	R	4156	4157	-	4215
Digital output 1 : 0x0000 = De-energise 0xFF00 or any non-zero value = Energise relay													
Parameter 2 -	R/W	Y	R	R	R	R	R	R	R	4216	4217	-	4275
Digital output 2 : 0x0000 = De-energise 0xFF00 or any non-zero value = Energise relay													
Parameter 3 -	R/W	Y	R	R	R	R	R	R	R	4276	4277	-	4335
Digital output 3 : 0x0000 = De-energise 0xFF00 or any non-zero value = Energise relay													
Parameter 4 -	R/W	Y	R	R	R	R	R	R	R	4336	4337	-	4395
Digital output 4 : 0x0000 = De-energise 0xFF00 or any non-zero value = Energise relay													
Parameter 5-7	-	R	R	R	R	R	R	R	R	4396	4397	-	4575

Note: This feature is only available with an extra relay or DIO board.

**Block 9 – 12 bit Analogue Input 1 Block
(accessed with Modbus function code 03 or 04)**

										Register Location			
Parameter 0	RO	Y(note1)-	-	Y	-	-	-	-	Y	4576	4577	-	4635
An Input 1 Range: Using Generic Protocol , 0x0000 = 0%, 0x7FFF = 100% Using EPLCG Protocol , 0x0000 = 0%, 0x0FFF = 100%													
Parameter 1 - 7	-	R	R	R	R	R	R	R	R	4636	4637	-	5055

**Block 10 – 12 bit Analogue Input 2 Block
(accessed with Modbus function code 03 or 04)**

										Register Location			
Parameter 0	RO	Y(note1)-	-	Y	-	-	-	-	Y	5056	5057	-	5115
An Input 2 Range: Using Generic Protocol , 0x0000 = 0%, 0x7FFF = 100% Using EPLCG Protocol , 0x0000 = 0%, 0x0FFF = 100%													
Parameter 1 - 7	-	R	R	R	R	R	R	R	R	5116	5117	-	5535

**Block 11 – 12 bit Analogue Output Block
(accessed with Modbus function code 03, 04, 06 or 16)**

										Register Location			
Parameter 0	R/W	-	-	Y	-	-	-	-	-	5536	5537	-	5595
An Output Range: Using Generic Protocol , 0x0000 = 0%, 0x7FFF = 100% Using EPLCG Protocol , 0x0000 = 0%, 0x0FFF = 100%													
Parameter 1 - 7	-	R	R	R	R	R	R	R	R	5596	5597	-	6015

Note 1: Only IQ3, software version V209 or later and additional analogue input cards, one card is required per analogue input.

Read Write	FCU Type									Data Location			
	IQ, CK, SI Ranges	A, AQ, Q, ROMpak	GPFCU (GP)	GPFCU (ACT)	CVA	EH / SI	CMA	IQ Analogue	FCU 1	FCU 2	to	FCU 60	

Block 12 – Historical Torque Profile – Opening Direction
(accessed with Modbus function code 03 or 04)

Register Location

8 torque (For EH / SI pressure.) values related to valve position across the valve stroke. Position 0 and 100% are not used as these may be set to full torque for a torque seating valve. Torque readings are available for 6%, 19%, 31%, 44%, 56%, 69%, 81%, and 94% positions. Parameters 1-7 contain this data for the OPENING direction of travel - note they only update if a complete stroke of the valve is made and contain the last profile.

All are ranged as: Using **Generic Protocol**, 0x0000 = 0% rated torque, 0x7FFF = 120% rated torque
Using **EPLCG Protocol**, 0x0000 = 0% rated torque, 0x0FFF = 120% rated torque

Para' 0 - 6%	RO	Y	-	-	-	Y	Y	-	-	6016	6017	-	6075
Para' 1 - 19%	RO	Y	-	-	-	Y	Y	-	-	6076	6077	-	6135
Para' 2 - 31%	RO	Y	-	-	-	Y	Y	-	-	6136	6137	-	6195
Para' 3 - 44%	RO	Y	-	-	-	Y	Y	-	-	6196	6197	-	6255
Para' 4 - 56%	RO	Y	-	-	-	Y	Y	-	-	6256	6257	-	6315
Para' 5 - 69%	RO	Y	-	-	-	Y	Y	-	-	6316	6317	-	6375
Para' 6 - 81%	RO	Y	-	-	-	Y	Y	-	-	6376	6377	-	6435
Para' 7 - 94%	RO	Y	-	-	-	Y	Y	-	-	6436	6437	-	6495

Note: CK actuators must include DSM to record intermediate torque.

Block 13 – Historical Torque Profile – Closing Direction
(accessed with Modbus function code 03 or 04)

Register Location

8 torque (For EH / SI pressure.) values related to valve position across the valve stroke. Position 0 and 100% are not used as these may be set to full torque for a torque seating valve. Torque readings are available for 6%, 19%, 31%, 44%, 56%, 69%, 81%, and 94% positions. Parameters 1-7 contain this data for the CLOSING direction of travel - note they only update if a complete stroke of the valve is made and contain the last profile.

All are ranged as: Using **Generic Protocol**, 0x0000 = 0% rated torque, 0x7FFF = 120% rated torque
Using **EPLCG Protocol**, 0x0000 = 0% rated torque, 0x0FFF = 120% rated torque

Para' 0 - 6%	RO	Y	-	-	-	Y	Y	-	-	6496	6497	-	6555
Para' 1 - 19%	RO	Y	-	-	-	Y	Y	-	-	6556	6557	-	6615
Para' 2 - 31%	RO	Y	-	-	-	Y	Y	-	-	6616	6617	-	6675
Para' 3 - 44%	RO	Y	-	-	-	Y	Y	-	-	6676	6677	-	6735
Para' 4 - 56%	RO	Y	-	-	-	Y	Y	-	-	6736	6737	-	6795
Para' 5 - 69%	RO	Y	-	-	-	Y	Y	-	-	6796	6797	-	6855
Para' 6 - 81%	RO	Y	-	-	-	Y	Y	-	-	6856	6857	-	6915
Para' 7 - 94%	RO	Y	-	-	-	Y	Y	-	-	6916	6917	-	6975

Note: CK actuators must include DSM to record intermediate torque.

Block 14 – Instantaneous Torque
(accessed with Modbus function code 03 or 04)

Register Location

Parameter 0	RO	Y	-	-	-	Y	Y	Y	-	6976	6977	-	7035
Inst. Torque Range: Using Generic Protocol , 0x0000 = 0%, 0x7FFF = 120% Using EPLCG Protocol , 0x0000 = 0%, 0x0FFF = 120% For EH / SI this value represents pressure.													
Parameter 1 - 3	-	R	R	R	R	R	R	R	R	7036	7034	-	7215
Parameter 4	RO	Y	-	-	-	Y	Y	Y	-	7216	7217	-	7275
Torque Profile Counters Data Bits 8-15 = Opening Torque Profile count Data Bits 0-7 = Closing Torque Profile count													
Parameter 5 - 7	-	R	R	R	R	R	R	R	R	7276	7277	-	7455

Note: CK actuators must include DSM to record intermediate torque.

Block 15 to 31 – Reserved

Register Location

Block 15 Para 0 - Block 31 Para 7	-	R	R	R	R	R	R	R	R	7456	7457	-	15615
--------------------------------------	---	---	---	---	---	---	---	---	---	------	------	---	-------

10.7 Modbus Messages Examples

Examples are included here to clarify the use of the Modbus protocol. These examples assume that the *Master Station* base address is 01. **All data in the message tables is in hexadecimal notation.**

The register and discrete locations calculated by the earlier formulae all have a start point of 0 (zero), hence the Modbus message location is the same as that calculated by the formulae.

10.7.1 Read Master Station Status

Master Station block 0 parameter 0, register location is 0000 decimal, and may be read with function code 03, discrete locations are 0000-0015 decimal and may be read with function code 01.

Using function code 01:

Modbus Address	Function Code	Discrete Address	Number of Discretes	CRC Check
01	01	00 00	00 10	CRC

Using function code 03:

Modbus Address	Function Code	Register Address	Number of Registers	CRC Check
01	03	00 00	00 01	CRC

10.7.2 Write Master Station Alarm Accept

Master Station block 0 parameter 5, location 0005 decimal. This is identified as a write instruction by the function code used, which may be 05, 15, 06, or 16. The data written may be any value, excluding zero, to accept the alarm. There is no need to cancel the accept with a zero write.

Using function code 05:

Modbus Address	Function Code	Coil Address	Data	CRC Check
01	05	00 05	FF 00	CRC

Using function code 16: (multiple is 1)

Modbus Address	Function Code	Register Address	Quantity	Byte Count	Data	CRC Check
01	10	00 05	00 01	02	FF 00	CRC

10.7.3 Read FCU 12 Digital Status

FCU digital status is in block 2, parameter 0. For FCU 12, the register location is 1227 decimal (= 0x04CB), or discrete locations 2096 to 2111 decimal (= 0x0830 to 0x083F). The data may be read with function code 02 or 04.

Using function code 02:

Modbus Address	Function Code	Discrete Address	Number of Discretes	CRC Check
01	02	08 30	00 10	CRC

Using function code 04:

Modbus Address	Function Code	Register Address	Number of Registers	CRC Check
01	04	04 CB	00 01	CRC

10.7.4 Read FCU 62 Digital Status

FCU 62 is found in Modbus address base + 1 = 02 as it is above number 60. The data is located in block 2, parameter 0. For FCU 62 the register location is 1217 decimal (= 0x04C1), and discrete locations 1936 to 1951 decimal (= 0x0790 to 0x079F).

Using function code 02:

Modbus Address	Function Code	Discrete Address	Number of Discretes	CRC Check
02	02	07 90	00 10	CRC

Using function code 04:

Modbus Address	Function Code	Register Address	Number of Registers	CRC Check
02	04	04 C1	00 01	CRC

10.7.5 Read Digital Status from 60 FCUs, Addresses 121 to 180

Modbus address = base + 2 = 03. Data is in block 2 parameter 0. FCU 1 data starts in register 1216 decimal (= 0x04C0).

Using function code 04:

Modbus Address	Function Code	Register Address	Number of Registers	CRC Check
03	04	04 C0	00 3C	CRC

10.7.6 Energise Command to OPEN relay of FCU 4

The *open* relay for FCU 4 is located in block 6 parameter 1, register location 3199 decimal (= 0x0C7F). Either function code 05 or 06 can be used, but the location to be written to is always the **register** number.

Using function code 05:

Modbus Address	Function Code	Address	Data	CRC Check
01	05	0C 7F	FF 00	CRC

Using function code 06:

Modbus Address	Function Code	Address	Data	CRC Check
01	06	0C 7F	FF 00	CRC

10.7.7 Write Desired Valve Position for FCU 26 to be 50%

The desired valve position data is written to block 5 parameter 1, register 2741 decimal (= 0x0AB5) for FCU 26.

With **Generic Protocol**, 50% is 0x3FFF and with **EPLCG Protocol**, 50% is 0x07FF.

Using function code 06 and **Generic Protocol**

Modbus Address	Function Code	Address	Data	CRC Check
01	06	0A B5	3F FF	CRC

Using function code 06 and **EPLCG Protocol**

Modbus Address	Function Code	Address	Data	CRC Check
01	06	0A B5	07 FF	CRC

This section describes the two protocols that pack the FCU data in the tightest way. This allows the host system to minimise the data traffic to and from the *Master Station*. The tables give register and discrete locations in the *Master Station* from which the data may be read.

The Yokogawa protocol is recommended when interfacing between a *Master Station* and a Yokogawa Centum CS and ACM11 interface card, Centum XL, EFCD gateway and RS4 cards, or similar system where the data packing is suitable. The protocol has been tested by Yokogawa in Japan, Holland, and Singapore and found to successfully connect the *Pakscan* and Yokogawa systems together. The protocol allows a standard Yokogawa SI22 faceplate to be used for the screen displays associated with motor operated valves.

The Honeywell SI protocol is recommended for connection between the *Master Station* and the Honeywell SI gateway. Honeywell has tested and approved the SI version for connecting the *Pakscan* system to a Honeywell TDC 3000 with an Advanced Process Manager and Serial Interface Gateway, or similar system where the data packing is suitable.

Select *Yokogawa* for the Yokogawa configuration of the database or *Honeywell SI* for the SI version of the database: the difference between these two choices is in the analogue data scaling only. Yokogawa uses 16-bit 2's complement and Honeywell SI uses an integer value in the register, all locations for the data are identical. Care must be taken to ensure that the correct protocol is selected for the application concerned.

The *Master Station* responds as a Modbus Slave to messages from the host. Each *Master Station* responds to a single Modbus address. The serial ports can each use different databases, whilst the two Ethernet ports must both use the same database and protocol.

The *Master Station* maintains a database covering all its connected FCUs, and the host reads this data without the need to access FCUs directly. The *Master Station* performs the functions of Data Concentrator, Protocol Converter, and Field AIMS are the field network masters. Within the FCUs, data is organised in blocks. The database locations listed in this section are the spaces from which and to which this data is moved.

11.1 Modbus Unit Address

The first byte of all Modbus message frames is the Modbus address byte. Modbus supports 248 addresses, of which value 0 is always allocated for broadcast messages. This leaves 247 addresses for use by connected devices on the Modbus data link.

Modbus Address	Function Code	Register or Discrete Address	Number of Registers or Bits	Data Field	CRC Check
8 bits	8 bits	16 bits	16 bits	N bits	16 bits

Fig 11.1.1: Modbus transaction format

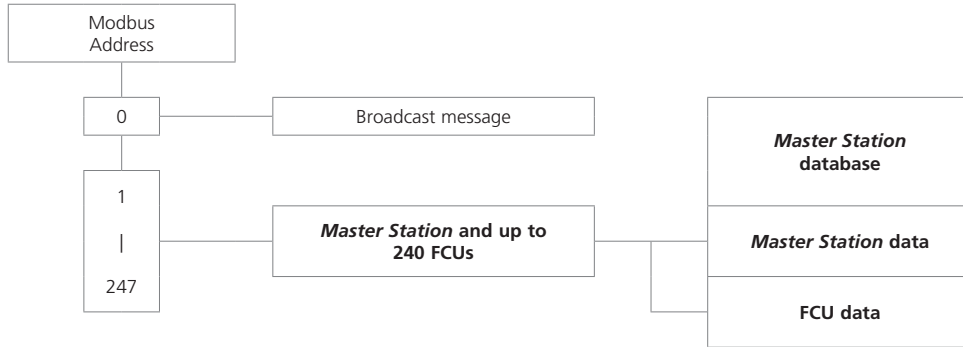


Fig 11.1.2: Modbus unit address structure – Yokogawa and Honeywell SI protocol

Each *Pakscan* Classic module occupies a single Modbus address in which all the data relating to itself and the connected FCUs is located. Modbus read requests return FCU data from the database in the appropriate *Master Station*; Modbus write requests are translated into *Pakscan* write commands which are sent to the FCU concerned.

Modbus Address	Responding Master Station	Interpretation
0	All	Modbus Broadcast
1	1	Database access
2	2	Database access
247	247	Database access

Fig 11.1.3: Modbus addressing for Master Stations

11.2 Modbus Function Code Support

Details of request and reply formats are contained in the *Modbus Reference Guide*. The following section deals with how the *Master Station* interprets commands. Fig 11.2.1 lists the supported Modbus commands.

Function Code	Modbus Name	Addressing
01	Read coil status	Discrete
02	Read input status	Discrete
03	Read holding registers	Register
04	Read input registers	Register
05	Force single coil	Discrete
06	Preset single register	Register
08	Loopback diagnostic test	
15	Force multiple coils	Discrete
16	Preset multiple registers	Register

Error code	Meaning
01	Illegal function code or incorrect message length
02	Illegal data address (Register address invalid)
03	Illegal data value
06	Slave Device Busy

Fig 11.2.1: Modbus function codes and error codes

Within the *Master Station* there is one database associated with each serial comms port and one shared between the two Ethernet ports. All data read commands access these databases.

- **Function Code 01 - Read Coil Status Requests**

Where the gateway is set up to read the data from the open or close coils, for example prior to writing data, this is permitted by the *Master Station*. However the coils do not physically exist and the data read back by the host is the current status of the Open and Close limit switch in the actuator (OAS for an Open command and CAS for a Close command). These signals may not reflect the state of the command coil. For example the actuator may have been opened by a system command to the open coil and then closed manually. The coil for open would be expected to be *on*, but the actuator will report the close coil as being *on* since CAS will be present, and the open coil as being *off*. In addition for actuator control all the write signals become pulsed outputs at the FCU and the actuator responds to these pulse commands itself.

- **Function Code 02 - Read Input Status Requests**

Any Input Status data within the *Master Station* may be read with a Code 02 Read request. The returned data will be valid for the discrete locations chosen.

- **Function Code 03 - Read Holding Register Requests**

Holding registers are used for the location of Output registers. In the case of *Pakscan* systems these output registers are used either to position a valve or for setting an analogue output. Where the gateway is set up to read the data in a Holding register, for example prior to writing data, the *Master Station* permits this. However, the data read back by the host may not be true.

In the case of reading the state of an output (holding) register the *Master Station* may not directly reflect the current position of the attached FCU or actuator since the actuator may have been moved manually or by a digital command since the analogue position was last sent. The data read may not be valid, though it will be the last state written.

- **Function Code 04 - Read Input Register Requests**

Any register data within the *Master Station* may be read with a Code 04 Read request. The returned data will be valid for the discrete locations chosen.

- **Function Code 05 and 06 - Force Single Coil, Preset Single Register**

If a Write request is to a discrete coil or register associated with the *Master Station*, then data is written directly to that coil or register.

If the Write request is to a discrete coil or register associated with an FCU, then the information contained in the message is translated into a command that an FCU understands. The command is then sent to the FCU over the current loop network. The rate at which instructions are sent must not exceed the rate at which they can be sent on to the FCUs.

The sequence of events is:

- (1) - Write command received by the *Master Station*.
- (2) - Response sent back to Host
- (3) - Write message sent to FCU

A good response to the Host indicates that the request was received correctly, the message length is acceptable, and that the addressed FCU is on-line. It does not indicate that the Write to the FCU was successful. A successful write is confirmed some time later when new data is reported as a change in the main database.

In the case of the Current Loop AIM, if commands are written at too high a rate then the current loop network is prevented from collecting data from the FCUs and the system will appear to slow down. The Command Filter provides some protection against too high a frequency of writing commands. It causes the system to ignore duplicated commands to the same FCU if the duplicate is within the time setting for the filter.

- **Function Code 08 – Diagnostics**

The purpose of the loopback test is to check the communication system between the host and the *Master Station*. Only diagnostic sub codes 00 and 02 are supported.

- **Function Code 08 Sub Code 00 – Return Query Data**

The purpose of this function is to echo the request data, indicating good communications. The data in the request message is copied into the reply message.

- **Function Code 08 Sub Code 02 – Return Diagnostic Register**

The purpose of this function is to return information about the status of the *Master Station* sides; which side is in control and which unit is the back up. The returned data register is decoded as follows:

Register	Value
Low Byte – Right side	0 = Unknown
	1 = Backup and in Alarm
	2 = Backup and OK
	3 = Main and in alarm
	4 = Main and OK
High Byte – Left side	0 = Unknown
	1 = Backup and in Alarm
	2 = Backup and OK
	3 = Main and in Alarm
	4 = Main and OK

- **Code 15 and 16 - Force Multiple Coils, Preset Multiple Registers**

If a Write request is to discrete coils or registers associated with the *Master Station*, then data is written directly to those coils or registers.

If the Write request is to discrete coils or registers associated with FCUs, then the information contained in the message is translated into commands that FCUs understand. The command is then sent to the FCU over the current loop network. The *Master Station* is able to accept a single transaction multiple write message containing information to be written to a maximum of 123 registers. These instructions are then passed to a queue for onward transmission over the current loop network. The rate at which instructions are sent must not exceed the rate at which they can be sent on to the FCUs.

If commands are written at too high a rate then the current loop network is prevented from collecting data from the FCUs and the system will appear to slow down. The Command Filter provides some protection against too high a frequency of writing commands. It causes the system to ignore duplicated commands to the same FCU if the duplicate is within the time setting for the filter.

In the case of actuator control there is never a need to write to a coil to turn it off as the output is always treated as a pulse. The DCS control should be arranged for the outputs to be pulse type. If this is not done the communication on the current loop network will carry unnecessary control commands to turn off coils that are already off.

- **Error Codes 01, 02, 03, 06 and 0A**

Error code 01 will be presented back to the host if the function code in the data message is not one of those supported by the *Master Station* or the message length is not as expected.

Error code 02 will be presented back to the host if the Data Address is illegal; or if the write command is a multiple write (code 15 or 16) where the number of coils or registers exceeds the amount acceptable.

Error code 03 will be presented back to the host if the value contained in the data query field is illegal.

Error code 06 will also be sent back to the host if the *Master Station* has insufficient buffer space to handle the write request to coils or registers in a single transaction. Buffer space will become free as the writes are issued to the loop and FCUs.

Error code 0A will be presented back to the host if the *Master Station* is unavailable or, in the case of the Modbus TCP, if the modbus slave address in the message is not the same as the modbus slave address set in the *Master Station*.

11.3 Database Access

The database is accessed by use of the Modbus address structure using Register Numbers or Discrete Numbers in accordance with the Modbus standard. The database contains information collected from FCUs and is the data actually in the *Master Station*. Data transfers to and from the FCUs are under the control of the *Master Station* Field network AIM.

11.3.1 Data Organisation

The database comprises a series of records organised in accordance with the Modbus documentation. Messages with function codes 01 to 06, 15 and 16 indicate specifically which locations in the database are to be accessed.

Function Codes 01, 05, and 15	refer to coils 0XXXX
Function Code 02	refers to discrete inputs 1XXXX
Function Code 04	refers to read only registers 3XXXX
Function Codes 03, 06, and 16	refer to registers 4XXXX

Coils are used for digital outputs. The status of maintained digital outputs should be read from discrete status inputs and not from the coil itself. Data read back from a coil may not be valid.

Registers are used for all multiple bit signals (analogues and counters). Some are protected and may only be read. Data read back from a Holding register with code 03 will contain the last data written to that coil. It may not reflect the actual status of the register in the FCU.

The data in each record is listed in the following sections for both the *Master Station* and FCUs.

11.3.2 Data Interchange Requests

Data may be interchanged between the host and the *Master Station* database using Modbus Register or Discrete Numbers.

11.4 Notes on the use of the Yokogawa and Honeywell SI Modbus Protocol

Normally the Modbus host will be set up to cyclically read data representing key variables of the *Master Station* and FCUs. It can do this using Read Input Register function code 04, and Read Discrete Status function code 02. In addition the gateway may be set to use function code 01 to read Output Coils prior to a write (05) or code 03 to read Holding Registers prior to a write (06).

Register and Discrete address numbers referred to in the standard Modbus documentation all start from number 1, though the actual data request on the data link takes its start as 0. The Modbus host software **may** need to be configured with addresses that are 1 less than those listed in the tables following. This is due to the Host regarding addresses as starting from 0, not 1. The actual method used by the gateway is specified in its documentation.

The discrete and register numbers listed in the tables all start from 1, register 40001 would be referenced as 0000 in the serial transaction.

The database is arranged to provide maximum efficiency in the use of the gateway space available and reading a group of registers in one transaction is more efficient than reading one register at a time. The Honeywell SI, because of the link to the APM Arrays may be easily set to collect multiple data in a transaction. The Yokogawa gateway should be organised to use efficient data transfer at all times. Note that the discrete bits may be moved in a minimum of 16 bits to the card working space.

The *Master Station* includes Alarm Accept logic with respect to FCU alarms. Alarms from FCUs are automatically accepted by the *Master Station* (so the FCU can clear its alarm latches) and latched within the *Master Station*. These alarms must be read by the Host and then accepted (with an Alarm Accept write to coil 32) before they can clear.

11.4.1 Suggested Scan Cycle

The Host should be configured to scan data from the *Master Station* in the following order:

- Read Alarm Status
- Read Digital Status
- Perform Alarm Accept (only strictly necessary if any New Alarms have occurred)
- Read Analogue Status (if any analogue data is to be read)

Commands to FCUs may be fitted in as required.

In some applications it may be desirable to scan some items e.g. analogues, less frequently than others. This is perfectly acceptable.

Within the *Master Station* area of the database there are common alarm bits for loop fault, FCU fault and actuator fault. These may be used as a quick way of checking for new alarms.

11.4.2 Writing to Coils

When writing to a coil the data field to turn off the coil has to be 0x0000. As the most common device connected is an actuator whose action is controlled by a pulse output there is often no need to turn off a coil that has previously been turned on. The output command from the DCS should, where possible, use a pulse type output. When writing to a coil the data field to turn on the coil may be 0xFF00 or any other non zero value.

11.4.3 Readback of Holding Registers

The *Master Station* supports the reading of the data in the Holding Registers. This data may not accurately reflect the state of the actuator as it could have been moved manually since the data was written. The data is a 2's complement 16 bit value (0x0000 – 0x7FFF) in the case of the Yokogawa protocol or a signed integer value (0-0x0064) in the case of the Honeywell SI. It is calculated from the actual value used in the data transaction over the current loop network to the FCU. When read back this value may differ by 1 digit due to rounding errors in the calculation. The value sent to the FCU when the register was written will be true. To establish the actual valve position the Input Register relating to the FCU Measured Value should be read.

11.4.4 Alarm Handling

The serial communication ports on the *Master Station* are each served by their own independent database and alarm handling. The handling of alarms on one serial port does not reflect on the alarms of any other serial port unless the *Master Station* is set to link the alarms. The two Ethernet ports on a *Master Station* share another independent database with its own alarm handling which is common to both Ethernet ports.

In the database there is a group of 16 bits of data defined as the *alarm block* for each FCU. Similarly, there are *system alarms* as listed in Section 12.1.2. These data bits will all be latched by the *Master Station* should they occur. The *Master Station* will therefore capture a transient alarm and keep it in its database ready for the host to read it.

Any latched alarm from these data areas will only be reset on the subsequent conditions. The alarm bit must read by the host, the alarm bit must be accepted by the host (this is done by issuing an *alarm accept*), and the source of the alarm must return to normal.

An example of the sequence would be:

Consider an actuator thermostat.

1. Actuator motor gets excessively hot and trips the thermostat.
2. Host reads data bit (bit 19) for the thermostat for this actuator.
3. Host issues *alarm accept*; this is registered by the system as applicable to the thermostat trip alarm.
4. The data bit remains set until the actuator cools down.
5. The data bit returns to normal once the actuator has cooled and thermostat is automatically reset.

If the host does not read the *thermostat* bit for this FCU then the bit will remain set, even after the actuator cools down and the thermostat resets. Also if the host does not read this bit, any *alarm accept* will not allow the alarm to reset itself. Any alarm bit must be read before it is able to be accepted.

If the alarms are read infrequently then the above procedure guarantees that the host will register any and every alarm from the *alarm block*.

In addition to the alarm data for each FCU there is a *status block*. The status block also contains information about the presence (or absence) of alarms in the *alarm block*.

- **Alarm bit (bit 12)**

For each FCU the *alarm* bit will be present if any of the source signals used to set bits in the *alarm block* are present. Notice that the *alarm* bit is an OR function of any alarm before the latch for that alarm. The *alarm* bit is latched and will not clear until it has been read, accepted and the source of the alarm has returned to normal. In the example of the thermostat, the *alarm* bit will be set when the thermostat is initially tripped.

- **New alarm bit (bit 11)**

For each FCU, *new alarm* will be present every time a new alarm occurs in the FCU. However, every time an *alarm accept* is issued, this data bit will be reset even if the alarm itself is still present.

The purpose of this bit is to indicate to the host there is a new alarm to be read from the *alarm block*.

- **System Common Alarms**

In the *Master Station* bit 10250 will be set if any FCU has its own *alarm* bit set. Thus the *common FCU alarm* is set while any one FCU has an input actually in alarm, or there is an FCU unavailable for communication.

Bit 10251 contains a similar common data bit derived from the actuator *monitor relay* source signals.

11.4.5 Use of Alarm Bits

The host may be configured to read as many, or all, of the *alarm block* data bits as required. Those that are not being used will possibly fill up as alarms over the course of operating the system; this will not have any detrimental effect on system performance.

Actively used alarms will individually appear in the data locations being read and transferred to the host via the *alarm accept* process. They will also reset themselves as they return to normal provided they are read and accepted.

The *alarm* bit will inform the host that any alarm is present, even those not normally being identified by the host as relevant. This bit may be used by the host as a flag that an alarm is currently present on an FCU. The host must take care of latching these bits in its own alarm handling system. This bit is comparable to a contact input that is self-resetting. As it is taken from before the internal latch, it is a true statement for the current alarm situation on the FCU.

The *new alarm* bit may be used to indicate to the host that an alarm reading process is required, or that an *alarm accept* write is required. The *new alarm* will by its very nature disappear once the *alarm accept* is issued irrespective of the actual plant status as it has to be available for each new alarm.

11.5 Master Station Database

11.5.1 Master Station Records

The discrete and register numbers listed in the tables all start from 1, for example discrete input 10001 would be referenced as 0000 in the serial transaction and not 0001.

- Digital Inputs – Read Only Data (accessed with Modbus function code 02)**

Individual bits – discrete locations (1 bit per)

Location	Description
System Alarms	
10001 to 10240	Reserved
10241	Reserved
10242	Reserved
10243	Power on reset
10244	Reserved
10245	Auto loopback
10246	Reserved
10247	Reserved

Location	Description
System status and flags	
10248	Loopback in progress
10249	Loopback in use
10250	Common FCU alarm
10251	Common actuator alarm
10252	Side A (primary) ok
10253	Side B (standby) ok
10254	Communicating to: 0 = Side A (Left), 1 = Side B (Right)
10255	1 = Primary (in use), 0 = Standby (out of use)

- Digital Outputs – Write function (accessed with Modbus function code 05 and 15)**

Individual bits – discrete locations (1 bit per)

When writing to a location the data field should comply with the Modbus instructions, although writing any non-zero value to these locations will cause the action to occur.

Function	Action	Location	Description
Global ESD Trigger	Write to trigger ESD	0001	ESD
Change master	Write to change over	0015	Change primary control between Side A or B
System reconfiguration	Write to trigger	0016	Reset loop
System/Comms alarm accept	Write to accept	0032	Alarm accept

11.6 FCU Database

The FCU database is organised to present the same information from each sequential FCU address in adjacent record entries. This general rule is broken only by the signals indicating valve open (OAS) and valve closed (CAS), and the commands to *open* and *close* the valves. These records are located adjacent to one another in pairs for each FCU.

As the FCUs may be of differing types, a bit number, relay number or register description identifier is attached, together with its meaning for each record group. The different bit number, relay number and register meanings are also listed for the different FCU types at the end of this section.

11.6.1 Digital Inputs (FCUs)

The discrete and register numbers listed in the tables all start from 1, discrete input 10001 would be referenced as 0000 in the serial transaction and not 0001.

- **Read Only Data (accessed with Modbus function code 02)**

Status – adjacent bits per FCU – discrete locations (1 bit per)

Location	Description	Location	Description
10257	Bit 3 FCU 1 (CAS)	10258	Bit 2 FCU 1 (OAS)
10259	Bit 3 FCU 2 (CAS)	10260	Bit 2 FCU 2 (OAS)
10261	Bit 3 FCU 3 (CAS)	10262	Bit 2 FCU 3 (OAS)
10263	Bit 3 FCU 4 (CAS)	10264	Bit 2 FCU 4 (OAS)
10265	Bit 3 FCU 5 (CAS)	10266	Bit 2 FCU 5 (OAS)
10267	Bit 3 FCU 6 (CAS)	10268	Bit 2 FCU 6 (OAS)
10269	Bit 3 FCU 7 (CAS)	10270	Bit 2 FCU 7 (OAS)
10271	Bit 3 FCU 8 (CAS)	10272	Bit 2 FCU 8 (OAS)
	FCU N bit 3 = 10256 + 2N - 1		FCU N bit 2 = 10256 + 2N
10723	Bit 3 FCU 234 (CAS)	10724	Bit 2 FCU 234 (OAS)
10725	Bit 3 FCU 235 (CAS)	10726	Bit 2 FCU 235 (OAS)
10727	Bit 3 FCU 236 (CAS)	10728	Bit 2 FCU 236 (OAS)
10729	Bit 3 FCU 237 (CAS)	10730	Bit 2 FCU 237 (OAS)
10731	Bit 3 FCU 238 (CAS)	10732	Bit 2 FCU 238 (OAS)
10733	Bit 3 FCU 239 (CAS)	10734	Bit 2 FCU 239 (OAS)
10735	Bit 3 FCU 240 (CAS)	10736	Bit 2 FCU 240 (OAS)

Note that the information in these locations is also mapped to alternate locations starting 11217 (OAS) and 11457 (CAS)
 N = FCU address number in the range 1 to 240

• **Read Only Data (accessed with Modbus function code 02)**

Status bits – individual bits per FCU – discrete locations (1 bit per)

Location	Description	Location	Description	Location	Description
Bit 0 - AUX 1		Bit 1 - AUX 2		Bit 2 - OAS	
10737	Bit 0 FCU 1	10977	Bit 1 FCU 1	11217	Bit 2 FCU 1
10738	Bit 0 FCU 2	10978	Bit 1 FCU 2	11218	Bit 2 FCU 2
10739	Bit 0 FCU 3	10979	Bit 1 FCU 3	11219	Bit 2 FCU 3
10740	Bit 0 FCU 4	10980	Bit 1 FCU 4	11220	Bit 2 FCU 4
	FCU N bit 0 = 10736 + N		FCU N bit 1 = 10976 + N		FCU N bit 2 = 11216 + N
10974	Bit 0 FCU 238	11214	Bit 1 FCU 238	11454	Bit 2 FCU 238
10975	Bit 0 FCU 239	11215	Bit 1 FCU 239	11455	Bit 2 FCU 239
10976	Bit 0 FCU 240	11216	Bit 1 FCU 240	11456	Bit 2 FCU 240
Bit 3 - CAS		Bit 4 - STOP		Bit 5 - MOVE	
11457	Bit 3 FCU 1	11697	Bit 4 FCU 1	11937	Bit 5 FCU 1
11458	Bit 3 FCU 2	11698	Bit 4 FCU 2	11938	Bit 5 FCU 2
11459	Bit 3 FCU 3	11699	Bit 4 FCU 3	11939	Bit 5 FCU 3
11460	Bit 3 FCU 4	11700	Bit 4 FCU 4	11940	Bit 5 FCU 4
	FCU N bit 3 = 11456 + N		FCU N bit 4 = 11696 + N		FCU N bit 5 = 11936 + N
11694	Bit 3 FCU 238	11934	Bit 4 FCU 238	12174	Bit 5 FCU 238
11695	Bit 3 FCU 239	11935	Bit 4 FCU 239	12175	Bit 5 FCU 239
11696	Bit 3 FCU 240	11936	Bit 4 FCU 240	12176	Bit 5 FCU 240
Bit 6 - MRO		Bit 7 - MRC		Bit 8 - AUX3	
12177	Bit 6 FCU 1	12417	Bit 7 FCU 1	12657	Bit 8 FCU 1
12178	Bit 6 FCU 2	12418	Bit 7 FCU 2	12658	Bit 8 FCU 2
12179	Bit 6 FCU 3	12419	Bit 7 FCU 3	12659	Bit 8 FCU 3
12180	Bit 6 FCU 4	12420	Bit 7 FCU 4	12660	Bit 8 FCU 4
	FCU N bit 6 = 12176 + N		FCU N bit 7 = 12416 + N		FCU N bit 8 = 12656 + N
12414	Bit 6 FCU 238	12654	Bit 7 FCU 238	12894	Bit 8 FCU 238
12415	Bit 6 FCU 239	12655	Bit 7 FCU 239	12895	Bit 8 FCU 239
12416	Bit 6 FCU 240	12656	Bit 7 FCU 240	12896	Bit 8 FCU 240

• **Read Only Data (accessed with Modbus function code 02)**

Status bits – individual bits per FCU – discrete locations (1 bit per)

Location	Description	Location	Description	Location	Description
Bit 9 - AUX4		Bit 10 - LBON		Bit 11 - NALM	
12897	Bit 9 FCU 1	13137	Bit 10 FCU 1	13377	Bit 11 FCU 1
12898	Bit 9 FCU 2	13138	Bit 10 FCU 2	13378	Bit 11 FCU 2
12899	Bit 9 FCU 3	13139	Bit 10 FCU 3	13379	Bit 11 FCU 3
12900	Bit 9 FCU 4	13140	Bit 10 FCU 4	13380	Bit 11 FCU 4
	FCU <i>N</i> bit 9 = 12896 + <i>N</i>		FCU <i>N</i> bit 10 = 13136 + <i>N</i>		FCU <i>N</i> bit 11 = 13376 + <i>N</i>
13134	Bit 9 FCU 238	13374	Bit 10 FCU 238	13614	Bit 11 FCU 238
13135	Bit 9 FCU 239	13375	Bit 10 FCU 239	13615	Bit 11 FCU 239
13136	Bit 9 FCU 240	13376	Bit 10 FCU 240	13616	Bit 11 FCU 240
Bit 12 - ALARM					
13617	Bit 12 FCU 1				
13618	Bit 12 FCU 2				
13619	Bit 12 FCU 3				
13620	Bit 12 FCU 4				
	FCU <i>N</i> bit 12 = 13616 + <i>N</i>				
13854	Bit 12 FCU 238				
13855	Bit 12 FCU 239				
13856	Bit 12 FCU 240				

N = FCU address number in the range 1 to 240

• **Read Only Data (accessed with Modbus function code 02)**

Alarm bits – individual bits per FCU – discrete locations (1 bit per)

Location	Description	Location	Description	Location	Description
Bit 13 - MEMF		Bit 14 - COMMS		Bit 15 - LOCAL	
13857	Bit 13 FCU 1	14097	Bit 14 FCU 1	14337	Bit 15 FCU 1
13858	Bit 13 FCU 2	14098	Bit 14 FCU 2	14338	Bit 15 FCU 2
13859	Bit 13 FCU 3	14099	Bit 14 FCU 3	14339	Bit 15 FCU 3
13860	Bit 13 FCU 4	14100	Bit 14 FCU 4	14340	Bit 15 FCU 4
	FCU N bit 13 = 13856 + N		FCU N bit 14 = 14096 + N		FCU N bit 15 = 14336 + N
14094	Bit 13 FCU 238	14334	Bit 14 FCU 238	14574	Bit 15 FCU 238
14095	Bit 13 FCU 239	14335	Bit 14 FCU 239	14575	Bit 15 FCU 239
14096	Bit 13 FCU 240	14336	Bit 14 FCU 240	14576	Bit 15 FCU 240
Bit 16 - POWR		Bit 17 - WDOG		Bit 18 - MREL	
14577	Bit 16 FCU 1	14817	Bit 17 FCU 1	15057	Bit 18 FCU 1
14578	Bit 16 FCU 2	14818	Bit 17 FCU 2	15058	Bit 18 FCU 2
14579	Bit 16 FCU 3	14819	Bit 17 FCU 3	15059	Bit 18 FCU 3
14580	Bit 16 FCU 4	14820	Bit 17 FCU 4	15060	Bit 18 FCU 4
	FCU N bit 16 = 14576 + N		FCU N bit 17 = 14816 + N		FCU N bit 18 = 15056 + N
14814	Bit 16 FCU 238	15054	Bit 17 FCU 238	15294	Bit 18 FCU 238
14815	Bit 16 FCU 239	15055	Bit 17 FCU 239	15295	Bit 18 FCU 239
14816	Bit 16 FCU 240	15056	Bit 17 FCU 240	15296	Bit 18 FCU 240
Bit 19 - THERM		Bit 20 - LSTOP		Bit 21 - SFAIL	
15297	Bit 19 FCU 1	15537	Bit 20 FCU 1	15777	Bit 21 FCU 1
15298	Bit 19 FCU 2	15538	Bit 20 FCU 2	15778	Bit 21 FCU 2
15299	Bit 19 FCU 3	15539	Bit 20 FCU 3	15779	Bit 21 FCU 3
15300	Bit 19 FCU 4	15540	Bit 20 FCU 4	15780	Bit 21 FCU 4
	FCU N bit 19 = 15296 + N		FCU N bit 20 = 15536 + N		FCU N bit 21 = 15776 + N
15534	Bit 19 FCU 238	15774	Bit 20 FCU 238	16014	Bit 21 FCU 238
15535	Bit 19 FCU 239	15775	Bit 20 FCU 239	16015	Bit 21 FCU 239
15536	Bit 19 FCU 240	15776	Bit 20 FCU 240	16016	Bit 21 FCU 240

• **Read Only Data (accessed with Modbus function code 02)**

Alarm bits – Individual Bits per FCU – Discrete Locations (1 bit per)

Location	Description	Location	Description	Location	Description
Bit 22 - VOBS		Bit 23 - VJAM		Bit 24 - AUXOR	
16017	Bit 22 FCU 1	16257	Bit 23 FCU 1	16497	Bit 24 FCU 1
16018	Bit 22 FCU 2	16258	Bit 23 FCU 2	16498	Bit 24 FCU 2
16019	Bit 22 FCU 3	16259	Bit 23 FCU 3	16499	Bit 24 FCU 3
16020	Bit 22 FCU 4	16260	Bit 23 FCU 4	16500	Bit 24 FCU 4
	FCU <i>N</i> bit 22 = 16016 + <i>N</i>		FCU <i>N</i> bit 23 = 16256 + <i>N</i>		FCU <i>N</i> bit 24 = 16496 + <i>N</i>
16254	Bit 22 FCU 238	16494	Bit 23 FCU 238	16734	Bit 24 FCU 238
16255	Bit 22 FCU 239	16495	Bit 23 FCU 239	16735	Bit 24 FCU 239
16256	Bit 22 FCU 240	16496	Bit 23 FCU 240	16736	Bit 24 FCU 240
Bit 25 - VTT		Bit 26 - R		Bit 27 - MMOVE	
16737	Bit 25 FCU 1	16977	Bit 26 FCU 1	17217	Bit 27 FCU 1
16738	Bit 25 FCU 2	16978	Bit 26 FCU 2	17218	Bit 27 FCU 2
16739	Bit 25 FCU 3	16979	Bit 26 FCU 3	17219	Bit 27 FCU 3
16740	Bit 25 FCU 4	16980	Bit 26 FCU 4	17220	Bit 27 FCU 4
	FCU <i>N</i> bit 25 = 16736 + <i>N</i>		FCU <i>N</i> bit 26 = 16976 + <i>N</i>		FCU <i>N</i> bit 27 = 17216 + <i>N</i>
16974	Bit 25 FCU 238	17214	Bit 26 FCU 238	17454	Bit 27 FCU 238
16975	Bit 25 FCU 239	17215	Bit 26 FCU 239	17455	Bit 27 FCU 239
16976	Bit 25 FCU 240	17216	Bit 26 FCU 240	17456	Bit 27 FCU 240
Bit 28 - EOT					
17457	Bit 28 FCU 1				
17458	Bit 28 FCU 2				
17459	Bit 28 FCU 3				
17460	Bit 28 FCU 4				
	FCU <i>N</i> bit 28 = 17456 + <i>N</i>				
17694	Bit 28 FCU 238				
17695	Bit 28 FCU 239				
17696	Bit 28 FCU 240				

N = FCU address number in the range 1 to 240

• **Read Only Data (accessed with Modbus function code 02)**

Digital inputs (FCUs) – relay coil status (applies to GPFCU only)

The following data locations contain the status of the output relays in the General Purpose Field Control Units (GPFCU). These may be considered as *status signals*. The state of the coil may be examined by using function code 02 on a discrete by discrete basis. For writing data to relay coils see the Write Data section.

Location	Description	Location	Description	Location	Description
Relay 4 Coil		Relay 1 Coil		Relay 3 Coil	
17697	Rly 4 FCU 1	17937	Rly 1 FCU 1	18177	Rly 3 FCU 1
17698	Rly 4 FCU 2	17938	Rly 1 FCU 2	18178	Rly 3 FCU 2
17699	Rly 4 FCU 3	17939	Rly 1 FCU 3	18179	Rly 3 FCU 3
17670	Rly 4 FCU 4	17940	Rly 1 FCU 4	18180	Rly 3 FCU 4
FCU N relay 4 = 17696 + N		FCU N relay 1 = 17936 + N		FCU N relay 3 = 18176 + N	
17934	Rly 4 FCU 238	18174	Rly 1 FCU 238	18414	Rly 3 FCU 238
17935	Rly 4 FCU 239	18175	Rly 1 FCU 239	18415	Rly 3 FCU 239
17936	Rly 4 FCU 240	18176	Rly 1 FCU 240	18416	Rly 3 FCU 240
Relay 2 Coil					
18417	Rly 2 FCU 1				
18418	Rly 2 FCU 2				
18419	Rly 2 FCU 3				
18420	Rly 2 FCU 4				
FCU N relay 2 = 18416 + N					
18654	Rly 2 FCU 238				
18655	Rly 2 FCU 239				
18656	Rly 2 FCU 240				

N = FCU address number in the range 1 to 240

11.6.2 Digital Outputs (FCUs)

- **Write Data (accessed with Modbus function code 01, writes with function codes 05 and 15)**

When writing outputs to the FCUs, to assert the command (energise the coil) write 0xFF00 (or any data other than 0x0000). To remove the command (de-energise the coil) write 0x0000. Actuator control commands never require to be turned off, so there is no need to write a de-energise command.

Commands – adjacent coils per FCU – coil locations (1 bit per)

Location	Description	Location	Description
00033	Rly 1 FCU 1 (Close Cmd)	00034	Rly 2 FCU 1 (Open Cmd)
00035	Rly 1 FCU 2 (Close Cmd)	00036	Rly 2 FCU 2 (Open Cmd)
00037	Rly 1 FCU 3 (Close Cmd)	00038	Rly 2 FCU 3 (Open Cmd)
00039	Rly 1 FCU 4 (Close Cmd)	00040	Rly 2 FCU 4 (Open Cmd)
00041	Rly 1 FCU 5 (Close Cmd)	00042	Rly 2 FCU 5 (Open Cmd)
00043	Rly 1 FCU 6 (Close Cmd)	00044	Rly 2 FCU 6 (Open Cmd)
00045	Rly 1 FCU 7 (Close Cmd)	00046	Rly 2 FCU 7 (Open Cmd)
00047	Rly 1 FCU 8 (Close Cmd)	00048	Rly 2 FCU 8 (Open Cmd)
00049	Rly 1 FCU 9 (Close Cmd)	00050	Rly 2 FCU 9 (Open Cmd)
00051	Rly 1 FCU 10 (Close Cmd)	00052	Rly 2 FCU 10 (Open Cmd)
00053	Rly 1 FCU 11 (Close Cmd)	00054	Rly 2 FCU 11 (Open Cmd)
00055	Rly 1 FCU 12 (Close Cmd)	00056	Rly 2 FCU 12 (Open Cmd)
00057	Rly 1 FCU 13 (Close Cmd)	00058	Rly 2 FCU 13 (Open Cmd)
00059	Rly 1 FCU 14 (Close Cmd)	00060	Rly 2 FCU 14 (Open Cmd)
00061	Rly 1 FCU 15 (Close Cmd)	00062	Rly 2 FCU 15 (Open Cmd)
00063	Rly 1 FCU 16 (Close Cmd)	00064	Rly 2 FCU 16 (Open Cmd)
	FCU N relay 1 00032 + 2N - 1		FCU N relay 2 = 00032 + 2N
00501	Rly 1 FCU 235 (Close Cmd)	00502	Rly 2 FCU 235 (Open Cmd)
00503	Rly 1 FCU 236 (Close Cmd)	00504	Rly 2 FCU 236 (Open Cmd)
00505	Rly 1 FCU 237 (Close Cmd)	00506	Rly 2 FCU 237 (Open Cmd)
00507	Rly 1 FCU 238 (Close Cmd)	00508	Rly 2 FCU 238 (Open Cmd)
00509	Rly 1 FCU 239 (Close Cmd)	00510	Rly 2 FCU 239 (Open Cmd)
00511	Rly 1 FCU 240 (Close Cmd)	00512	Rly 2 FCU 240 (Open Cmd)

Note that the access to these coils is also mapped to alternate locations starting 00513 (open command) through to 01472 (ESD command, FCU 240)
 N = FCU address number in the range 1 to 240

- **Write Data (accessed with Modbus function code 01, writes with function codes 05 and 15)**

Commands – individual coils per FCU – coil locations (1 bit per)

Location	Description	Location	Description	Location	Description
Relay 2 - OPEN COMMAND		Relay 3 - STOP COMMAND		Relay 1 - CLOSE COMMAND	
00513	Rly 2 FCU 1	00753	Rly 3 FCU 1	00993	Rly 1 FCU 1
00514	Rly 2 FCU 2	00754	Rly 3 FCU 2	00994	Rly 1 FCU 2
00515	Rly 2 FCU 3	00755	Rly 3 FCU 3	00995	Rly 1 FCU 3
00516	Rly 2 FCU 4	00756	Rly 3 FCU 4	00996	Rly 1 FCU 4
	FCU <i>N</i> relay 2 = 00512 + <i>N</i>		FCU <i>N</i> relay 3 = 00752 + <i>N</i>		FCU <i>N</i> relay 1 = 00992 + <i>N</i>
00750	Rly 2 FCU 238	00990	Rly 3 FCU 238	01230	Rly 1 FCU 238
00751	Rly 2 FCU 239	00991	Rly 3 FCU 239	01231	Rly 1 FCU 239
00752	Rly 2 FCU 240	00992	Rly 3 FCU 240	01232	Rly 1 FCU 240
Relay 4 - ESD COMMAND					
01233	Rly 4 FCU 1				
01234	Rly 4 FCU 2				
01235	Rly 4 FCU 3				
01236	Rly 4 FCU 4				
	FCU <i>N</i> relay 4 = 01232 + <i>N</i>				
01470	Rly 4 FCU 238				
01471	Rly 4 FCU 239				
01472	Rly 4 FCU 240				

N = FCU address number in the range 1 to 240

11.6.3 Analogue Inputs (FCUs)

• **Read Only Data (accessed with Modbus function code 04)**

Each suitably equipped FCU is able to collect analogue data from various inputs. In the Yokogawa protocol the registers each contain a 2's complement value for the measurement. In the Honeywell SI protocol the registers each contain an integer value for the measurement.

Location	Description	Location	Description
Applicable to Actuator FCUs only		Applicable to GPFCU and IQ with Analogue input option only	
Valve Position		Analogue Input 1	
Range: Yokogawa , 0x0000 = 0% 0x7FFF = 100% Honeywell SI , 0x0000 = 0% 0x0064 = 100%		Range: Yokogawa , 0x0000 = 0% 0x7FFF = 100% Honeywell SI , 0x0000 = 0% 0x0064 = 100%	
30001	FCU 1 Position	30241	FCU 1 An 1 I/P
30002	FCU 2 Position	30242	FCU 2 An 1 I/P
30003	FCU 3 Position	30243	FCU 3 An 1 I/P
30004	FCU 4 Position	30244	FCU 4 An 1 I/P
	FCU N position = 30000 + N		FCU N analogue input 1 = 30240 + N
30238	FCU 238 Position	30478	FCU 238 An 1 I/P
30239	FCU 239 Position	30479	FCU 239 An 1 I/P
30240	FCU 240 Position	30480	FCU 240 An 1 I/P
Applicable to GPFCU and IQ with Analogue input option only		Applicable to GPFCU only	
Analogue Input 2		Pulse Input	
Range: Yokogawa , 0x0000 = 0% 0x7FFF = 100% Honeywell SI , 0x0000 = 0% 0x0064 = 100%		Range: Yokogawa and Honeywell SI , 0x0000 to 0x270F counter value	
30481	FCU 1 An 2 I/P	30721	FCU 1 Pulse I/P
30482	FCU 2 An 2 I/P	30722	FCU 2 Pulse I/P
30483	FCU 3 An 2 I/P	30723	FCU 3 Pulse I/P
30484		30724	FCU 4 Pulse I/P
	FCU N analogue input 2 = 30480 + N		FCU N pulse input = 30720 + N
30718	FCU 238 An 2 I/P	30958	FCU 238 Pulse I/P
30719	FCU 239 An 2 I/P	30959	FCU 239 Pulse I/P
30720	FCU 240 An 2 I/P	30960	FCU 240 Pulse I/P

N = FCU address number in the range 1 to 240

- **Read Only Data (accessed with Modbus function code 04)**

IQ Range, SI Range, CK Range, CVA and EH / SI actuator FCUs are able to collect both current and historical force (torque, thrust or pressure) data from the actuator. The following 16 bit register locations each contain a value relating to the actuator torque.

Location	Description
Current Force (Torque, Thrust or Pressure)	
Range: Yokogawa , 0x0000 = 0% 0x7FFF = 120%	
Honeywell SI , 0x0000 = 0% 0x0078 = 120%	
30961	FCU 1 Current Force
30962	FCU 2 Current Force
30963	FCU 3 Current Force
30964	FCU 4 Current Force
	FCU <i>N</i> position = 30960 + <i>N</i>
31198	FCU 238 Current Force
31199	FCU 239 Current Force
31200	FCU 240 Current Force

11. Modbus Database – Yokogawa and Honeywell SI *continued*

Location	Description	Location	Description
Historical Force (Torque, Thrust or Pressure)			
Range: Yokogawa , 0x0000 = 0% 0x7FFF = 120% Honeywell SI , 0x0000 = 0% 0x0078 = 120%			
The force value is related to the readings taken across the valve stroke, position 0 and 100% are not used as these may be set to full force for valve seating. Force readings are available for 6%, 19%, 31%, 44%, 56%, 69%, 81%, and 94% positions. The data is stacked in pairs where an open force is followed by a close force for each position, for each FCU. The data is historical and only updated on completion of a full stroke of the valve from open to close, or from close to open. The data is not reported from the actuator to the <i>Master Station</i> unless the <i>torque data filter factor</i> is set to 0 (refer to the applicable FCU manual for more information).			
31201	6% open torque FCU 1	31202	6% close torque FCU 1
31203	6% open torque FCU 2	31204	6% close torque FCU 2
31205	6% open torque FCU 3	31206	6% close torque FCU 3
	FCU N 6% open torque = 31200 + 2N -1		FCU N 6% close torque = 31200 + 2N
31679	6% open torque FCU 240	31680	6% close torque FCU 240
31681	19% open torque FCU 1	31682	19% close torque FCU 1
	FCU N 19% open torque = 31680 + 2N -1		FCU N 19% close torque = 31680 + 2N)
32159	19% open torque FCU 240	32160	19% close torque FCU 240
32161	31% open torque FCU 1	32162	31% close torque FCU 1
	FCU N 31% open torque = 32160 + 2N -1		FCU N 31% close torque = 32160 + 2N
32639	31% open torque FCU 240	32640	31% close torque FCU 240
32641	44% open torque FCU 1	32642	44% close torque FCU 1
	FCU N 44% open torque = 32640 + 2N -1		FCU N 44% close torque = 32640 + 2N
33119	44% open torque FCU 240	33120	44% close torque FCU 240
33121	56% open torque FCU 1	33122	56% close torque FCU 1
	FCU N 56% open torque = 33120 + 2N -1		FCU N 56% close torque = 33120 + 2N
33599	56% open torque FCU 240	33600	56% close torque FCU 240
33601	69% open torque FCU 1	33602	69% close torque FCU 1
	FCU N 69% open torque = 33600 + 2N -1		FCU N 69% close torque = 33600 + 2N
34079	69% open torque FCU 240	34080	69% close torque FCU 240
34081	81% open torque FCU 1	34082	81% close torque FCU 1
	FCU N 81% open torque = 34080 + 2N -1		FCU N 81% close torque = 34080 + 2N
34559	81% open torque FCU 240	34560	81% close torque FCU 240
34561	94% open torque FCU 1	34562	94% close torque FCU 1
	FCU N 94% open torque = 34560 + 2N -1		FCU N 94% close torque = 34560 + 2N
35039	94% open torque FCU 240	35040	94% close torque FCU 240

N = FCU address number in the range 1 to 240

11.6.4 Analogue Outputs (FCUs)

- **Write Data (accessed with Modbus function codes 03, 06, 16)**

Particular actuator FCUs are able to accept a desired position signal. The following 16 bit register locations may be written to with a 2's complement value (Yokogawa protocol), or signed integer value (Honeywell SI protocol) relating to the desired valve position.

Location	Description
Applicable to Actuator FCUs only	
Valve Position Control	
Range: Yokogawa , 0x0000 = 0% 0x7FFF = 100% Honeywell SI , 0x0000 = 0% 0x0064 = 100%	
40001	FCU 1 position control
40002	FCU 2 position control
40003	FCU 3 position control
40004	FCU 4 position control
	FCU <i>N</i> position = 40000 + <i>N</i>
40238	FCU 238 position control
40239	FCU 239 position control
40240	FCU 240 position control

General Purpose Field Control Units (GPFCU) are able to accept an *analogue output* signal for connection to a controller or positioner. The following 16 bit register locations may be written to with a 2's complement value (Yokogawa protocol), or signed integer value (Honeywell SI protocol) relating to the setting of this output.

Location	Description
Applicable to GPFCU only	
Analogue Output	
Range: Yokogawa , 0x0000 = 0% 0x7FFF = 100% Honeywell SI , 0x0000 = 0% 0x0064 = 100%	
40241	FCU 1 analogue output
40242	FCU 2 analogue output
40243	FCU 3 analogue output
40244	FCU 4 analogue output
	FCU <i>N</i> analogue output = 40240 + <i>N</i>
40478	FCU 238 analogue output
40479	FCU 239 analogue output
40480	FCU 240 analogue output

11.7 FCU Inputs and Outputs Available

11.7.1 Digital Inputs

Data Bit or Register	FCU Type							
	IQ Range, SI Range Actuator	A, AQ, Q, ROMpak	GPFCU (GP)	GPFCU (ACT)	CVA	EH / SI	CMA	IQ Analogue
Bit 0	AUX 1	R	DIN 1	R	R	AUX 1	R	R
Bit 1	AUX 2	R	DIN 2	R	BAKPWR	AUX 2	R	R
Bit 2	OAS	OAS	DIN 3	OAS	OAS	OAS	OAS	R
Bit 3	CAS	CAS	DIN 4	CAS	CAS	CAS	CAS	R
Bit 4	STOP	STOP	DIN 5	STOP	STOP	STOP	R	R
Bit 5	MOVE	MRUN	DIN 6	MRUN	MOVE	Travelling	MOVE	R
Bit 6	MRO	MRO	DIN 7	MRO	TRO	MRO	R	R
Bit 7	MRC	MRC	DIN 8	MRC	TRC	MRC	R	R
Bit 8	AUX 3	EXT	R	EXT	R	AUX 3	R	R
Bit 9	AUX 4	R	R	R	R	AUX 4	R	R
Bit 10	LBON	LBON	LBON	LBON	LBON	LBON	LBON	LBON
Bit 11	NALRM	NALRM	NALRM	NALRM	NALRM	NALRM	NALRM	NALRM
Bit 12	ALRM	ALRM	ALRM	ALRM	ALRM	ALRM	ALRM	ALRM
Bit 13	MEMF	MEMF	MEMF	MEMF	MEMF	MEMF	R	MEMF
Bit 14	COMMS	COMMS	COMMS	COMMS	COMMS	COMMS	COMMS	COMMS
Bit 15	LOCAL	CNA	R	CNA	LOCAL	LOCAL	LOCAL	R
Bit 16	POWR	POWR	POWR	POWR	POWR	POWR	POWR	POWR
Bit 17	WDOG	WDOG	WDOG	WDOG	WDOG	WDOG	WDOG	WDOG
Bit 18	MREL	MREL	R	MREL	MREL	MREL	MREL	R
Bit 19	THERM	THERM	R	THERM	THERM	FAULT	R	R
Bit 20	LSTOP	LSTOP	R	LSTOP	LSTOP	LSTOP	LSTOP	R
Bit 21	SFAIL	SFAIL	R	SFAIL	SFAIL	SFAIL	SFAIL	R
Bit 22	VOBS	VOBS	R	VOBS	VOBS	VOBS	VOBS	R
Bit 23	VJAM	VJAM	R	VJAM	VJAM	VJAM	R	R
Bit 24	AUXOR	MOP	R	MOP	R	AUXOR	R	R
Bit 25	VTT	MCL	R	MCL	R	VTT	R	R
Bit 26	R	MOPG	R	MOPG	R	R	R	R
Bit 27	MMOVE	MCLG	R	MCLG	MMOVE	MMOVE	R	R
Bit 28	EOT	EOT	R	EOT	EOT	EOT	R	R
Relay 4	R	0	RL4	0	0	R	R	R
Relay 1	R	0	RL1	0	0	R	R	R
Relay 3	R	0	RL3	0	0	R	R	R
Relay 2	R	0	RL2	0	0	R	R	R

- AUX1 - Aux. Input 1
- AUX2 - Aux Input 2
- OAS - Open limit switch
- CAS - Close limit switch
- STOP - Actuator stopped in mid travel
- MOVE - IQ/IQT valve moving
- MRUN - Motor running
- MRO - Motor running open direction
- MRC - Motor running close direction
- AUX3 - Aux Input 3
- AUX4 - Aux Input 4
- DIN 1 to 8 - Digital inputs 1 to 8
- EXT IP - External digital input
- LBON - Loopback on

- NALM - New alarm present on this FCU
- ALARM - Any alarm present on this FCU
- R - Reserved
- Travelling - Actuator in motion
- TRO - Travelling open direction
- TRC - Travelling closed direction
- MEMF - RAM/ROM failure
- COMMS - Comms fail
- LOCAL - Actuator not in remote control
- CNA - Control not available
- POWR - Power on reset
- WDOG - Watchdog fail
- MREL - Monitor relay
- THERM - Thermostat trip

- FAULT - Actuator fault
- LSTOP - Local stop operated
- SFAIL - Start/stop fail
- VOBS - Valve obstructed
- VJAM - Valve jammed
- AUXOR - Aux I/P Override
- VTT - Valve Travel Time
- MOP - Manual open
- MCL - Manual close
- MMOVE - Manual valve movement
- MOPG - Manual opening
- MCLG - Manual closing
- EOT - Motor running end of travel
- BAKPWR - Under battery back-up power

11.7.2 Digital Outputs

Data Bit or Register	FCU Type							
	IQ Range, SI Range Actuator	A, AQ, Q, ROMpak	GPFCU (GP)	GPFCU (ACT)	CVA	EH / SI	CMA	IQ Analogue
Open (Relay 2)	Y	Y	Y	Y	Y	Y	Y	N
Stop (Relay 3)	Y	Y	Y	Y	Y	Y	Y	N
Close (Relay 1)	Y	Y	Y	Y	Y	Y	Y	N
ESD (Relay 4)	Y	Y	Y	Y	Y	Y	Y	N

11.7.3 Analogue Inputs

Data Bit or Register	FCU Type							
	IQ Range, SI Range Actuator	A, AQ, Q, ROMpak	GPFCU (GP)	GPFCU (ACT)	CVA	EH / SI	CMA	IQ Analogue
Valve Position	Y	Y	N	Y	Y	Y	Y	N
Current Torque	Y	N	N	N	Y	Y (pressure)	N	N
Historical Torque	Y	N	N	N	Y	Y	N	N
Analogue Input 1	N	N	Y	N	N	N	N	Y
Analogue Input 2	N	N	Y	N	N	N	N	Y
Pulse Input	N	N	Y	N	N	N	N	N

11.7.4 Analogue Outputs

Data Bit or Register	FCU Type							
	IQ Range, SI Range Actuator	A, AQ, Q, ROMpak	GPFCU (GP)	GPFCU (ACT)	CVA	EH / SI	CMA	IQ Analogue
Position Control	Y	Y	N	Y	Y	Y	Y	N
Analogue Output	N	N	Y	N	N	N	N	N

11.8 Modbus Message Examples

A few examples are included here to clarify the use of the Modbus protocol. These examples assume that the *Master Station* address is set to 01. **All data is in hexadecimal notation.**

Remember that the address used in the Modbus message assumes start points of zero for coils, registers etc. However the locations indicated in the tables above put the first register or coil etc. as number 1. Therefore 1 must be deducted from the locations indicated when determining the Modbus message location.

11.8.1 Read FCU Bit 5 from FCU 1 to 100

To determine which actuator motors are running. Bit 5 is located in discrete areas 11937 to 12036 for actuators 1 to 100.

Modbus Address	Function Code	Discrete Address	Number of Discretes	CRC Check
01	02	07 90	00 64	CRC

11.8.2 Read FCU Bit 2 and 3 from FCU 1 to 120

To use a single transaction by collecting the data from the *two bit* area. Bits 2 and 3 are located in discrete areas 10257 to 10496 for actuators 1 to 120.

Modbus Address	Function Code	Discrete Address	Number of Discretes	CRC Check
01	02	01 00	00 F0	CRC

11.8.3 Read Valve Position from FCU 26

Register is located at 30026.

Modbus Address	Function Code	Register Address	Number of Registers	CRC Check
01	04	00 19	00 01	CRC

11.8.4 Energise Command to Open Relay of FCU 104

The coil is located at 00616. To write a single coil the data field must be FF00.

Modbus Address	Function Code	Coil Address	Data	CRC Check
01	05	02 68	FF 00	CRC

OR:

Using the *two command area* the coil is located at 00240. To write a single coil the data field must be FF00.

Modbus Address	Function Code	Coil Address	Data	CRC Check
01	05	00 F0	FF 00	CRC

11.8.5 Write Desired Valve Position for FCU 26 to be 50%

Register is located at 40026.

With **Yokogawa protocol**, 50% is 3FFF and with **Honeywell SI protocol**, 50% is 0032.

Using **Yokogawa protocol**:

Modbus Address	Function Code	Register Address	Data	CRC Check
01	06	00 19	3F FF	CRC

Using **Honeywell SI protocol**:

Modbus Address	Function Code	Register Address	Data	CRC Check
01	06	00 19	00 32	CRC

12. Data Interpretation (All Modbus Databases)



This section describes the data organisation and meaning of the various data bits found in the protocol data for the *Pakscan* Modbus databases: Generic, Honeywell EPLCG, Yokogawa and Honeywell SI.

12.1 Master Station Data

The *Master Station* field network AIMS perform various self-checking routines and control the field networks. The status of the *Master Station* itself is available for interrogation by a host DCS over the host interface. The relevant registers and the location of the data within them, together with the methods for reading and writing to these registers is detailed in Sections 10 and 11. The data is always related either to an FCU on the field network, to the *Master Station* module or the field network AIM.

This section provides the interpretation of the information reported by each data bit or register in the *Master Station* area of the database and the available registers to which system instructions may be written.

Details of the information reported in the FCU area of the database is contained in the individual FCU instruction manuals. A brief overview of these data bit interpretations follows later in this manual.

12.1.1 Database Segregation

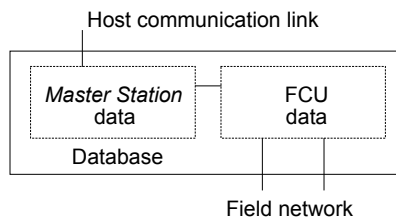


Fig 12.1.1: Database segregation

Whichever database Interface is chosen it will contain at least two sections. One of these is termed the *Master Station* Database, while the other is the FCU Database. The FCU Database contains the information from the attached devices on the field network, while the *Master Station* Database contains the system data.

- **Logical and physical *Master Stations***

The physical *Master Station* may contain up to four logical *Master Stations* as described in Section 10. The logical *Master Station* has a different Modbus slave address and contains data about different groups of FCUs on the network. All of these logical *Master Station* contain the same *Master Station* data. A command or write instruction to one is equivalent to writing to them all and all transactions should take place using the slave address of the base unit only. There is no need to read or write to more than one of them to achieve a read or write for all of them.

In the case of Yokogawa and Honeywell SI Modbus database, there is both one logical and one physical *Master Station* covering all the connected FCUs on the current loop.



12. Data Interpretation (All Modbus Databases) *continued*

12.1.2 Master Station Data Description

The available data depends on the interface chosen; this section describes all the data bits. When a bit is present or asserted it will be a logical 1.

Auto loopback occurred	This bit is an alarm bit that is present if a fault is detected on the current loop network and an automatic reconfiguration of the loop occurred.
Common actuator alarm	This data is an alarm bit that is present if any FCU on the loop has its MREL data bit present. MREL is only available from Rotork actuator FCUs and is the state of the <i>monitor relay</i> . It indicates that the actuator is not available for control. The actuator FCU MREL bit is described in the actuator FCU manual.
Common FCU alarm	This data is an alarm bit that is present if any FCU on the current loop network has any of its alarm bits present, including those FCUs connected to other logical <i>Master Stations</i> within this physical station. Thus, this alarm is present while any one FCU is actually in alarm or if there is an FCU unavailable for communication. The FCU alarm bits are described in the FCU manual.
ESD mode	This bit is present if a contact input wired to the ESD terminals of the <i>Master Station</i> is open circuit and the remote contact input ESD facility is enabled in the <i>Master Station</i> setup.
Loopback in progress	This alarm is present while the <i>Master Station</i> is in the process of reconfiguring the current loop network. It provides an indication that the <i>Master Station</i> is busy and the FCU data may not be true during the reconfiguration time.
Loopback in use	This signal is present whenever the <i>Master Station</i> has found a loop fault and is operating with <i>loopback</i> asserted on the field cable. Note that under this condition, loop doubling is not available.
Power on reset	This bit is an alarm bit that is present if the system power has been lost and restored.

12.1.3 Alarm Handling

Some of the data bits are described as *alarm bits*. These represent information that is considered an alarm. In each case the alarm bit is latched and it will not clear until the data has been read by the host, a serial data *alarm accept* has been issued to the *Master Station* and the source of the alarm has returned to normal.

12.1.4 Data Relevant to Hot Standby Systems

This data only has a true meaning for a hot standby *Master Station*. Side A (left side) is always the designated primary unit.

0 = Side A 1 = Side B	This bit indicates Side A / Side B communicating. It is used to determine if the communication is to Side A or Side B of a standby pair. Side A is the designated primary unit. The data bit will be a 0 if communication is to Side A. It is a 1 if communication is to Side B.
Side A OK (primary unit)	Present if Side A is functioning correctly.
Side B OK (standby unit)	Present if Side B is functioning correctly.
1 = primary (in use) 0 = standby (out of use)	Indicates whether the current <i>Master Station</i> side communicating on serial link is also in control of the current loop network. 1 indicates communication to the primary side. 0 indicates communication to the standby side.



12.1.5 Additional Data Available using Generic and Honeywell EPLCG

FCU failure count	This is a series of registers containing data showing the absolute number of communication failures (including retries) for every connected FCU on the current loop. The maximum count for an FCU is 256 failures after which its counter rolls over to zero and starts again.
FCU map	This is a series of registers containing the FCU addresses in the order in which they are connected on the 2-wire current loop.
FCU on loop to scan up to	This register contains a number equal to the <i>Master Station</i> setting for the highest FCU address to look for.
FCU's connected	This register contains data to show the number of FCU's communicating on each of the current loop network ports. In normal circumstances all the FCU's will be connected to Port A. However, if there is a cable fault, then some will be connected to Port A and some to Port B. The numbers indicate the position of the cable fault.
FCU address fault	This register holds data about the position and address number that is found to be at fault during configuration.
Loop baud rate	This register contains a number that may be decoded to give the loop baud rate setting.
Loop configuration process	This register changes its value as the <i>Master Station</i> proceeds through the stages used in configuring the loop.
Loop fault information	This register holds data indicating loop faults that may be present and preventing complete loop configuration. Additionally it includes the last system reconfiguration code and the loop fault type.
P4720 <i>Pakscan</i> Classic module software version	This register contains a number collected from the loop card EPROM to indicate the software version that is in use.
Loop test result (%)	This register holds a hex number for the result of the last loop test in percent.
Loop test speed	The number in this register relates to the last loop test performed and the speed at which it was done.
Command filter timeout	This register contains the timeout setting for the command filter.
<i>Master Station</i> type number	This register contains a number that identifies the type and capacity of the <i>Master Station</i> .

12.1.6 Command Description

It is possible to issue instructions to the system over the serial interface. These commands are directed either at a particular FCU or at the system as a whole. The commands relating to the system are as follows.

Alarm accept	Energise this coil to accept any alarm in the database (FCU or <i>Master Station</i>) which has been read in a previous transaction. There is only one accept coil for alarms, though each serial port, the Ethernet ports and the LCD on each <i>Master Station</i> side, have their own accept system and virtual databases. Any alarms will only clear from the database if they are read over the serial link or Ethernet link prior to being accepted and the alarm condition returns to normal. Note that if the alarms are 'linked' then the <i>alarm accept</i> accepts all the alarms on the linked the database.
Change primary / standby	Energise this coil to transfer control between the primary and standby units. The primary unit can be switched to standby or the standby unit switched to primary. This command is operative even when sent to a standby unit that is set to <i>standby passive</i> , regardless of which port the command arrives on (Serial or Ethernet). It is the only message obeyed by a unit in this condition. <i>Standby passive</i> regardless of which port the command arrives on (Serial or Ethernet). It is the only message obeyed by a unit in this condition. 'Standby Passive' is the normal setting for a <i>Master Station</i> on a multi-drop system.
ESD command to network	Energise this coil to issue a global emergency shut down instruction over the network to all the FCUs. The command will only be issued to the loop if the ESD facility is enabled in the <i>Master Station</i> setup.
Reconfigure loop	Energise this coil to reconfigure the current loop. This command can be used to reset the system after the repair of a cable fault.



12. Data Interpretation (All Modbus Databases) *continued*

12.2 FCU Data

FCU data is made available from the *Master Station*. The *Master Station* collects the data asynchronously from the connected FCUs in the actuators on the network. The FCUs vary depending on the data available to report. See actuator manuals for details of the network card type fitted.

In the database sections of this manual, a series of abbreviations are used for the data bits. The information on the exact reason for each data bit to be present is explained in the individual instruction manuals for each FCU type. The list below provides a brief explanation of each of the major data bits listed. Not all the bits are available from all FCUs and the list is a definition table only.

All data is present (1) when the state is true.

12.2.1 Digital Status Bits

ALARM	There is an alarm present on this FCU.
AUX 1 to AUX 4	Refers to the auxiliary digital inputs available from certain FCUs.
BATT	The FCU battery is low (IQ range and SI only).
DIN1 to DIN8	Digital inputs 1 to 8 on a GPFCU.
EXT	The external FCU contact is closed (AQ or Q actuators only). This is not available if the FCU has to report actual percentage position data.
LBON	Loopback is active on this FCU.
MOVE	FCU output drive moving.
MRO and MRC	Motor running in the open (MRO) / close (MRC) direction
MRUN	FCU motor is running.
NALARM	There is a new, unread, alarm on this FCU.
OAS and CAS	The FCU open limit switch (OAS) or close limit switch (CAS) is made.
Remote	FCU mode local/remote selector in the remote position.
STOP (reported data)	FCU stationary in mid position.
TRO and TRC	FCU travelling towards the open (TRO) position or closed (TRC) position.
Travelling	FCU in motion.
BAKPWR	FCU operating on reserve battery power (CVA and CMA actuators only).
BAKBATT	FCU reserve battery power low (CVA and CMA actuators only).



12.2.2 Alarm Data Bits

AUXOR	Indicates that one of the auxiliary digital inputs is active.
CNA	FCU remote control not available because the mode selector is not in the remote position.
COMMS	Communication failure between <i>Master Station</i> and FCU.
EOT	FCU continues to run the motor beyond the end of travel limit switch.
LOCAL	Mode selector in the local position.
LSTOP	Mode selector in the stop position.
MEMF	Memory chip fault.
MMOVE	Manual movement of the valve detected.
MOP and MCL	FCU has reached the open (MOP) or close (MCL) position due to manual movement of the handwheel. MOP is manually opened, MCL is manually closed.
MOPG and MCLG	FCU has left the close position (MOPG) or the open position (MCLG) due to manual movement of the handwheel. MOPG is manual opening of the valve and MCLG is manual closing of the valve.
MREL	FCU monitor relay tripped. The monitor relay is a combination signal usually indicating that remote control is not available, check FCU manual for details of alarms included in the monitor relay indication.
POWR	FCU power on reset alarm.
SFAIL	FCU fails to start or stop when expected to do so.
THERM	FCU thermostat tripped.
FAULT	General fault indication (EH and SI only).
VJAM	Valve jammed at end of travel causing an unexpected torque, thrust or pressure trip.
VOBS	Obstructed valve at intermediate position causing an unexpected torque, thrust or pressure trip.
VTT	Indicates valve travel time exceeded.

12.2.3 FCU Commands

The actuators on the field network can be commanded to open, close, or stop by writing to the appropriate location in the database. In all cases, there is no requirement to cancel a command to remove it. A new command will always remove any existing commands.

Most FCUs are capable of adopting an analogue position (0-100%), check the technical manual for the FCU to confirm whether the actuator supports this feature. Writing an analogue position to the appropriate register cancels any existing command. Writing an open/stop/close command will cancel any analogue setting previously made.

General Purpose Field Control Units (GPFCUs) can have their relay outputs operated (energised or de-energised) and, additionally, they have an analogue output signal. Similar to actuator commands, with the GPFCU relays there is no requirement to cancel a command to remove it unless the relay outputs have been set to *maintained* action within the FCU.

OPEN	The FCU will move open.
STOP	The FCU will stop.
CLOSE	The FCU will close.
ESD	The FCU will perform internally set Emergency Shut Down operation.
Position control	The FCU will move to the written desired position value. This method of intermediate positioning must be used for modulating duty. The use of pulsed control will not be successful as the current loop network timing is not deterministic.
RLY1 to RLY4	Energise or de-energise the applicable relay depending on the data written. Only a GPFCU will consider the commands as operating relays. All other FCUs have logic outputs to their respective internal controls.



12. Data Interpretation (All Modbus Databases) *continued*

- **Command Filtering (only applicable for the *Pakscan Classic* field network)**

The *Master Station* includes a command filter to reduce the replication of commands to an FCU over the current loop interface. If a command sent over the serial or Ethernet links is repeated within the set filter time, the second command will be discarded and only the first command will be actioned. The effect is to remove unwanted field network commands from the system and free up the maximum available time space for other valid commands or data retrieval from the field.

12.2.4 FCU Analogue Inputs

There are several analogue inputs available from FCUs. Not all signals will be reported by all actuators and the tables for each protocol indicate what is available from each type of FCU. In particular A, AQ, Q and ROMpak range actuators cannot report valve position unless they are fitted with a potentiometer.

Valve position feedback	Reports the actual valve position as a percentage of full travel.
Pulse input	This register from a GPFCU contains a counter value that increments on receipt of inputs to DIN1.
12-bit analogue input 1 and 2	There are two registers that report the value of the analogue input connected (GPFCU and IQ range with Analogue option only). These are 12 bit because the input signal is resolved to 12 bits (1 in 4096). The actual register value will vary in accordance with the input signal over a range that depends on the protocol selected.
Historic torque profile	Registers detailing historic torque, thrust or pressure at various positions across the valve stroke.
Instantaneous torque	Indicates the last recorded torque, thrust or pressure value.

Glossary of Terms

Term	Description
AIM	Add In Module
API	Application Programming Interface
CPU	Central Processing Unit
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarised Zone
DoS	Denial of Service
DDoS	Distributed Denial of Service
DPI	Deep Packet Inspection
ESD	Emergency Shutdown
FCU	Field Control Unit
GPFCU	General Purpose Field Control Unit
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP address	Internet Protocol address
IPS	Intrusion Prevention System
LAN	Local Area Network
MAC address	Media Access Control address
NTP	Network Time Protocol
PLC	Programmable Logic Controller
PSU	Power Supply Unit
RAM	Random Access Memory
ROM	Read Only Memory
RSTP	Rapid Spanning Tree Protocol
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTM	Unified Threat Management
VPN	Virtual Private Network

rotork®



www.rotork.com

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

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

PUB059-052-00
Issue 05/24

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

The name Rotork is a registered trademark. Rotork recognises all registered trademarks. Published and produced in the UK by Rotork. POLCH0524