rotork
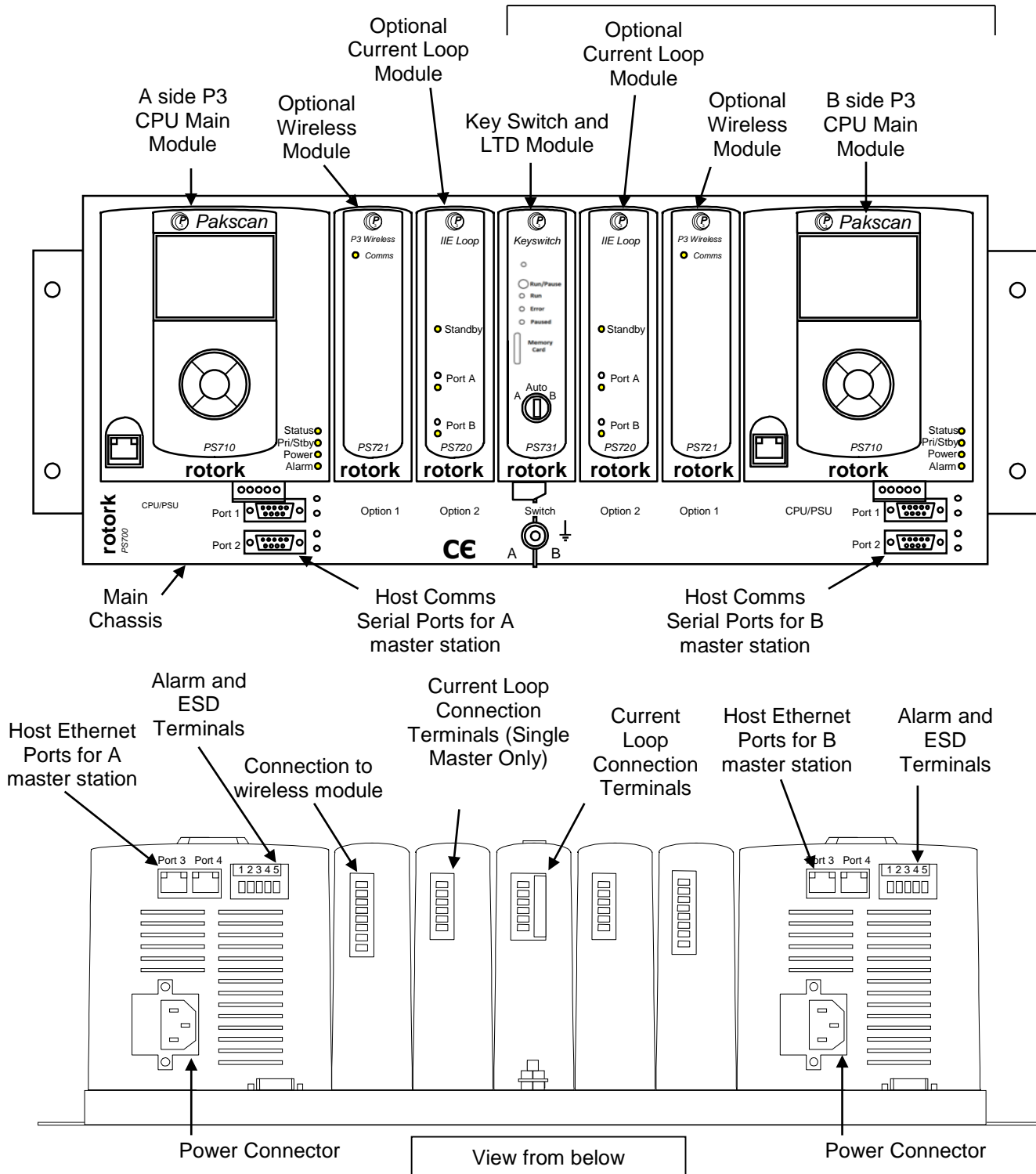

P3 - Pakscan Master Station
Technical Manual

KNOW YOUR MASTER STATION

These modules **not** fitted on single master stations

A side P3 CPU Main Module

Optional Wireless Module

Optional Current Loop Module

Key Switch and LTD Module

Optional Current Loop Module

Optional Wireless Module

B side P3 CPU Main Module

Main Chassis

Host Comms Serial Ports for A master station

Host Comms Serial Ports for B master station

Host Ethernet Ports for A master station

Alarm and ESD Terminals

Connection to wireless module

Current Loop Connection Terminals (Single Master Only)

Current Loop Connection Terminals

Host Ethernet Ports for B master station

Alarm and ESD Terminals

Power Connector

View from below

Power Connector

CONTENTS:

TABLE OF FIGURES:

> **This manual relates to Pakscan 3 Master Stations fitted with PS720 Current Loop modules and/or the PS721 and PS722 Wireless modules**

INTRODUCTION

Pakscan 3 is a complete field network control system from Rotork. With the addition of a wireless (P3W) network the user now has the choice of proven current loop technology of the Pakscan IIE system or the flexibility of a meshed wireless network. The P3W master station is supplied with a P3W Coordinator module; this module is powered by the master station and facilitates the communications between the master station and the wireless network. Most types of Rotork actuators can be connected to a Pakscan current loop provided they are fitted with the necessary field unit. Information on the respective actuator field units can be found in the appropriate manuals. In this guide, the type of actuator is not considered, though reference is made to both the integral and IQ actuator types of field unit. The type of field unit does not affect the setting up of the system. The IQ and IQT range of actuators integrate fully with the wireless network. The network range can be extended using a P3W Repeater module, this module is externally powered and it extends the network range by receiving and retransmitting network messages. Other actuators or devices can be added to the wireless network using a Pakscan 3 Wireless Modbus Adaptor (P3W WMA). This module is very similar to the P3W Repeater, but has a RS-485 serial port for communication. The Pakscan 3 master stations are delivered either as loose items for mounting by the user, or contained in an enclosure provided by Rotork. The master station will generally be either a single unit, or a hot standby pair. This manual provides a guide to setting up the Pakscan master, the various P3W Wireless modules, the loop communications, wireless communications, and the host connections for the most commonly found applications.
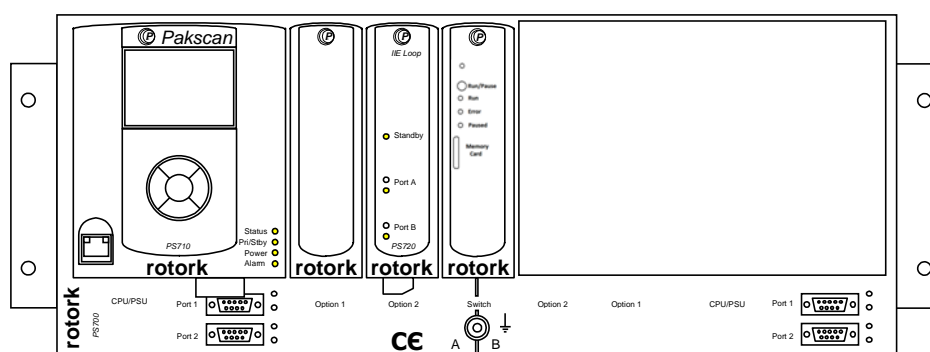
Fig 1: The Pakscan 3 Single Master Station – option: Current loop
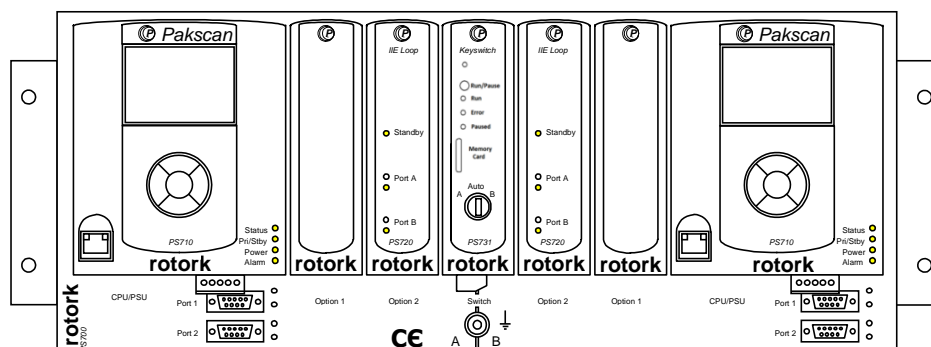
Fig 2: The Pakscan 3 Hot Standby Master Station - option: Current loop

A master station fitted with the wired network only requires the PS720 module that fits in to the back plane. A master station fitted with wireless requires a module to be fitted to the back plane (in option 1) and connected to this module, a P3W coordinator module (PS722).
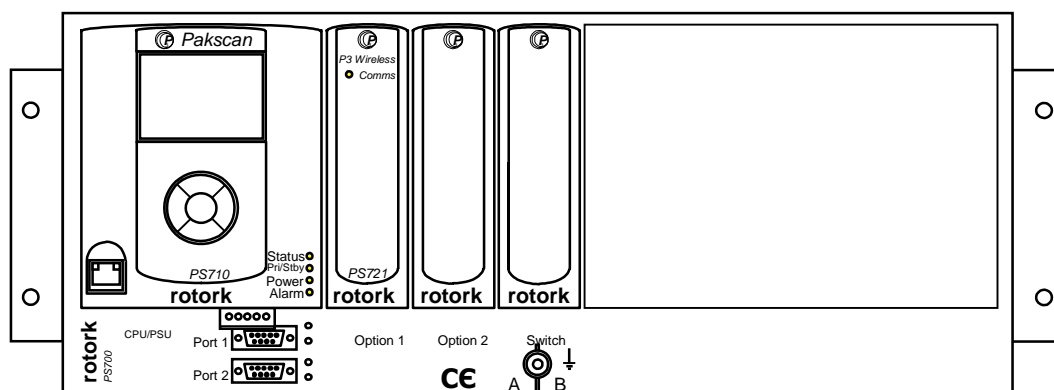
Fig 3: The Pakscan 3 Single Master Station – option: Wireless
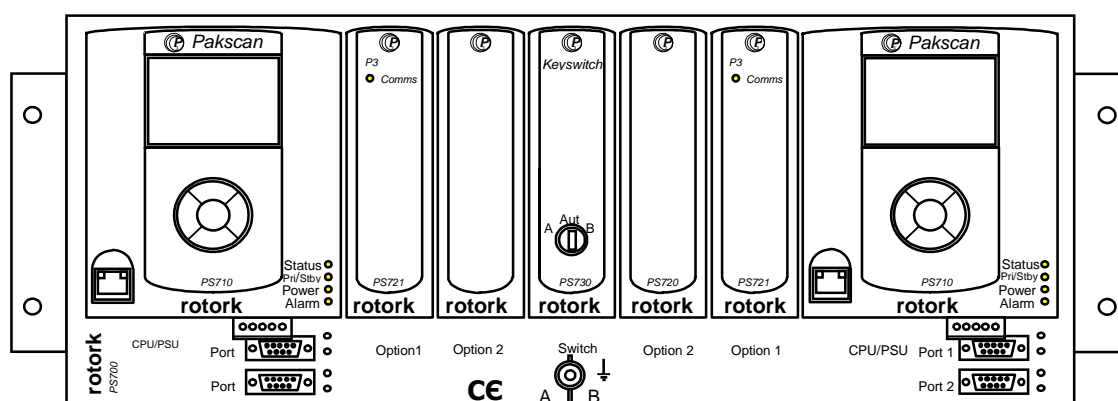
Fig 4: The Pakscan 3 Hot Standby Master Station – option: Wireless
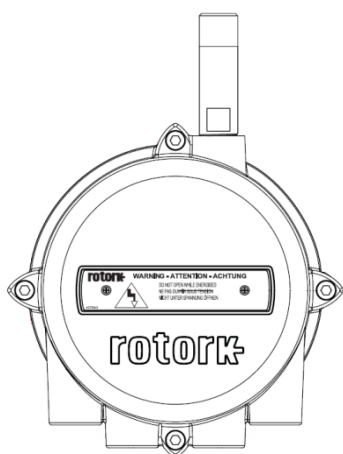
Fig 5:   The P3W (Pakscan 3 Wireless) coordinator – PS722. One required for single channel master stations, two for hot standby master stations. The P3W repeater (a device for extending the range of wireless) and the P3W WMA look identical to this.

1. MOUNTING AND CONNECTING THE MASTER STATION

> ## *Before mounting the master station, set the communications link switches, as discussed in section 3.*

The Pakscan 3 master station (single or hot standby) provides front access for all the user connections, including power feed and the field network connections – either loop wires to the Current Loop module (PS720) or network connection to the P3W coordinator (PS721 and PS722). The host communication links use plug in D-type connectors for the serial communications and RJ45 connections for the Ethernet links.

❑ The field wiring for the current loop, P3W coordinator and the master station alarms are taken to screw terminals on plug in connectors that are fitted from below their appropriate module.

❑ Power wiring is connected using an IEC connector in the bottom of the master station module PS710. Two connections are required for a hot standby system.

❑ Serial communications (RS-232 or RS-485) plug into 9 way female D-type connectors on the front of the mounting chassis.

❑ Ethernet connections use RJ45 connectors on the bottom of the master station module PS710. The connector on the front is intended for connection to a service laptop computer.

1.1 Mechanical Fixing

Room should be left around the module for all the connections and cables, allowing for a suitable bending radius on each lead. Power wiring should be suitably fused or protected with miniature circuit breakers (MCBs) external to the master station.

The master station may be mounted on a flat surface using the mounting brackets provided. Also, the extension brackets allow it to be mounted in a 19-inch rack. In either case it should be located in a way that permits easy access to the pushbuttons and easy viewing of the display panel(s).
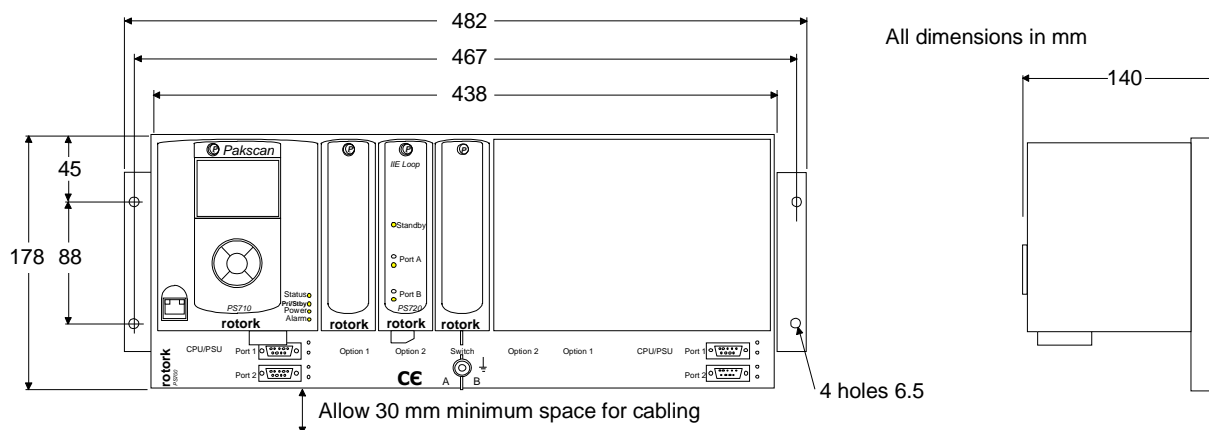
Fig 6: Pakscan 3 surface mounting dimensions.
        (Both single and hot standby master stations may be surface mounted)
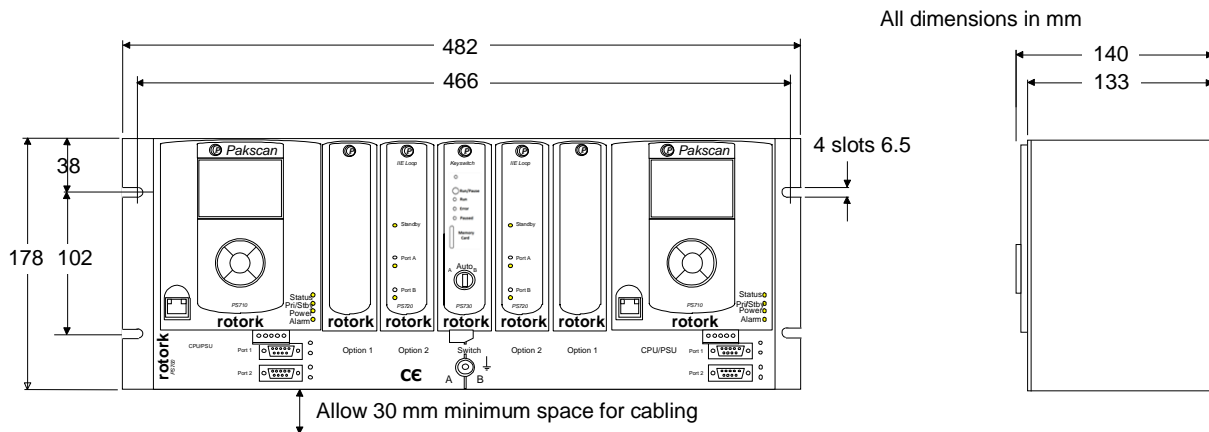
Fig 7: Pakscan 3, 19-inch rack mounting dimensions.
(Both single and hot standby master stations can be panel or rack mounted)
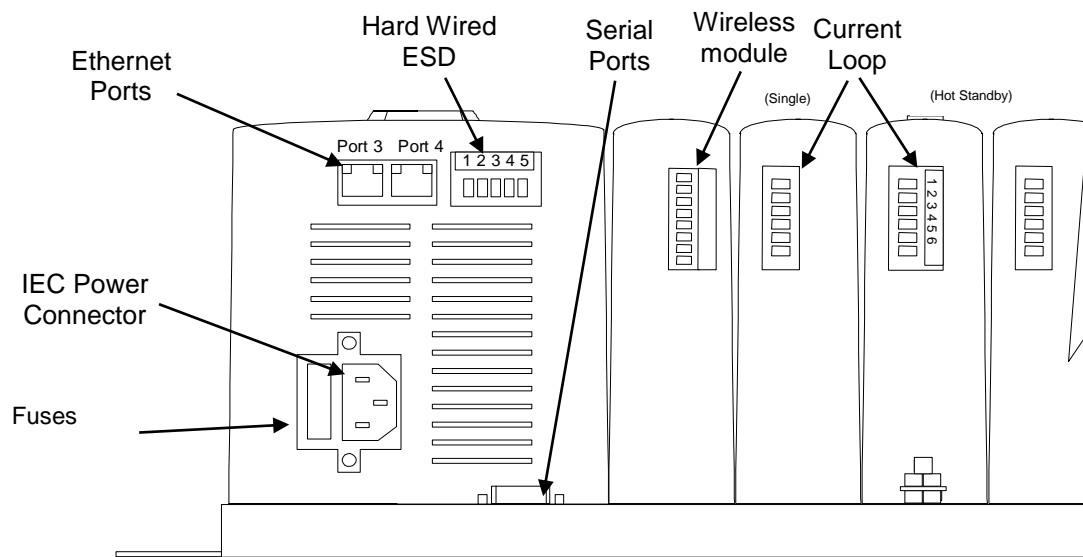
Fig 8: View below the Pakscan P3 master station showing the Connectors
(The B side connections are similar)

Wireless installations will include a P3W Coordinator and may include P3W Repeaters and P3W Wireless Modbus Adaptors (WMA). These units are identical with regards to mechanical fixing.
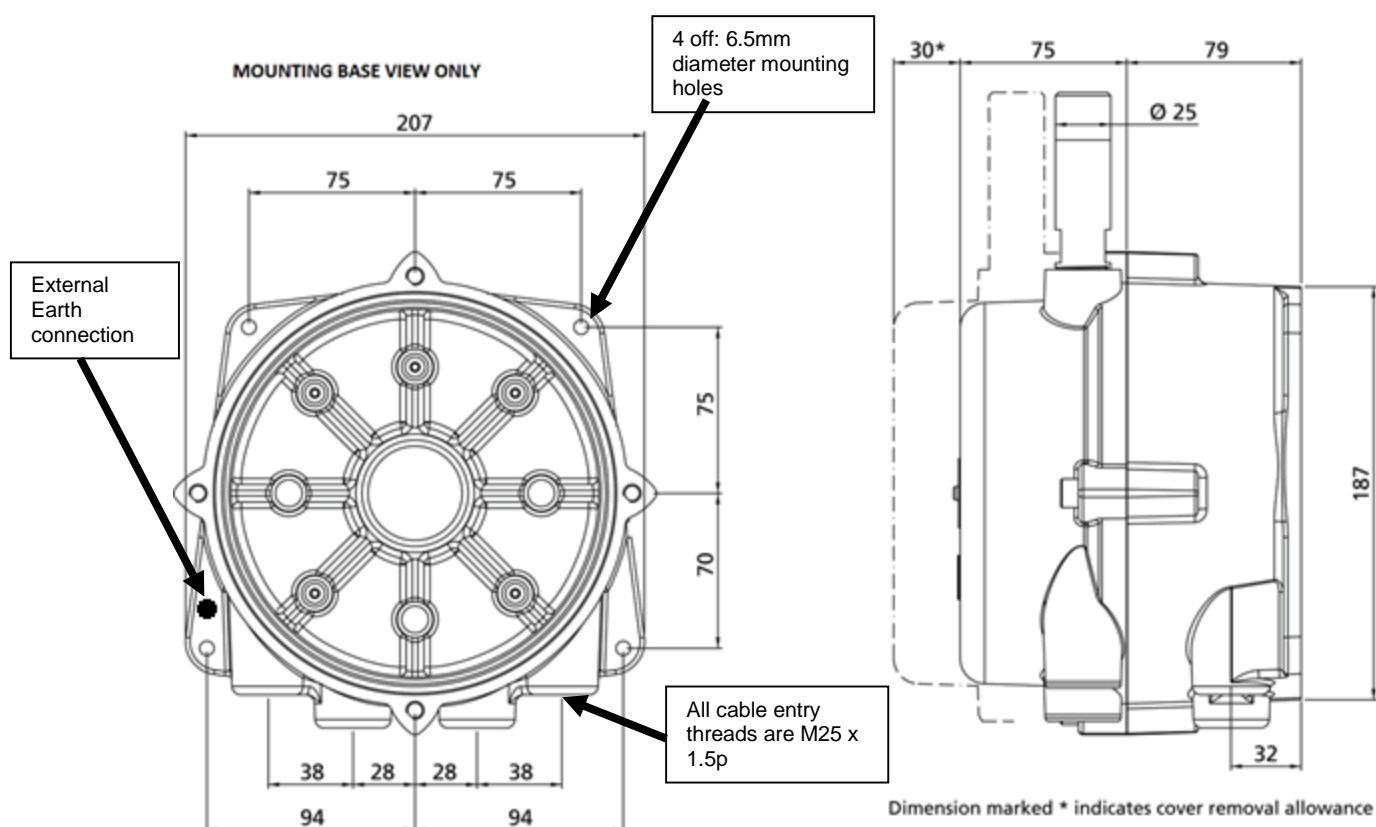
Dimensions in mm, Module weight: 4,400g

Fig 9: P3W coordinator, P3W WMA and P3W Repeater mounting details

---

The P3W Coordinator, P3W Repeater and P3W wireless Modbus Adaptor may be located in Hazardous locations. If this is the case, please refer to the Hazardous Area notes in the General Safety Information section at the back of this manual.

1.2   Host Serial Communications Connections

The serial data connections are via the D-type connectors below each master station PS710 on the main chassis. They are labelled Port 1 and Port 2 on both the A and B (left and right) sides of the assembly. All the connectors are **9 way female** and they may be set for RS-485 (2-wire) or RS-232 use. On hot standby systems they can be cross coupled to provide seamless communication when the systems change over. The pin-out connections are shown below.
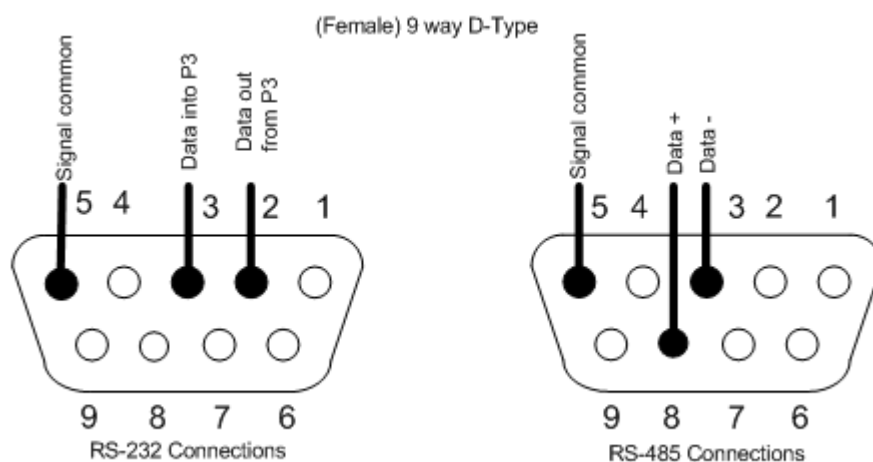
Fig 10:   *Serial Communication connections*

❑   With RS-485 it is possible to arrange a multi-drop data highway for the serial communications, whilst RS-232 must be single point communications.

1.3   Ethernet Communications Connections

Each Pakscan P3 CPU module (master station module) has 2 x RJ45 Ethernet connectors for the two host communication ports (accessed from below) marked Port 3 and Port 4. A third RJ45 connector is located on the front of each module. This is provided to allow a portable computer (laptop) to be connected for diagnostic and set up purposes. Standard Ethernet patch cables can be used with these connectors.

All Ethernet cables must be screened, and of good quality. Many screened Ethernet cables of low quality have questionable screening efficacy.

All Ethernet ports on the master station have LEDs to indicate communication. Green indicates 10M bit/s and orange indicates 100Mbit/s. Communication may be half duplex or full duplex.

1.4   Power Connector and Fuses

Each Pakscan P3 CPU module has its own internal power supply. A standard IEC connector is provided to allow the mains power (85 to 263V AC – 47 to 63 Hz) to be connected from below the module. The mains IEC socket also includes the two fuses for the system, which must only be replaced with the same and rating 250V 1A 5x20mm anti-surge fuses.

For the 24V DC version, a three pin removable screw terminal connector is provided. There is no internal fuse.

1.5 Alarm and Hardwired ESD Connector

There is a removable screw terminal connector in each Pakscan P3 CPU module for the connection of ESD hard-wired inputs and for connection to the internal alarm relay contacts, when required. On most systems these terminals will not be used; in which case a hard-wired link between pins 4 and 5 must be fitted, this is usually fitted by the factory.

Terminal	Function
1	Alarm (common)
2	Alarm (normally closed)
3	Alarm (normally open)
4	Emergency Shutdown
5	Emergency Shutdown

Fig 11:   PS710 CPU module connector terminal functions

Note the relay is shown in the 'alarm active' or 'power removed' position. The Alarm relay will activate if there are any alarm conditions in any field unit or the master station. This alarm will not prevent operation of the master station.

1.6 Current Loop Connections

A connector is located in the bottom of the key switch module on hot standby Pakscan 3 systems for the connection of the current loop to the field mounted actuators. On single P3 master stations the connector beneath the current loop module itself should be used.

Terminal	Function
1	Port B In
2	Port B Out
3	Port B Screen
4	Port A In
5	Port A Out
6	Port A Screen

Fig 12:   PS720/PS730/PS731/PS732 Current Loop connections

1.7 P3W Coordinator Connections

A connector is located in the bottom of the (PS721) wireless option module to connect to the P3W coordinator (PS722). The connection between these should be made using a shielded network cable with 3 pairs of wires – each pair to be twisted. Suitable cable conforms to the specification for RS-422 networks. This cable can be up to 200m long so that the P3W coordinator may be mounted, for example, on the roof of the building containing the master station.

The Communications cable and appropriate glands for the P3W coordinator will need to be sourced locally, according to site requirements. Connect the Communications cable as shown below, noting that the connections are **NOT** all one to one.
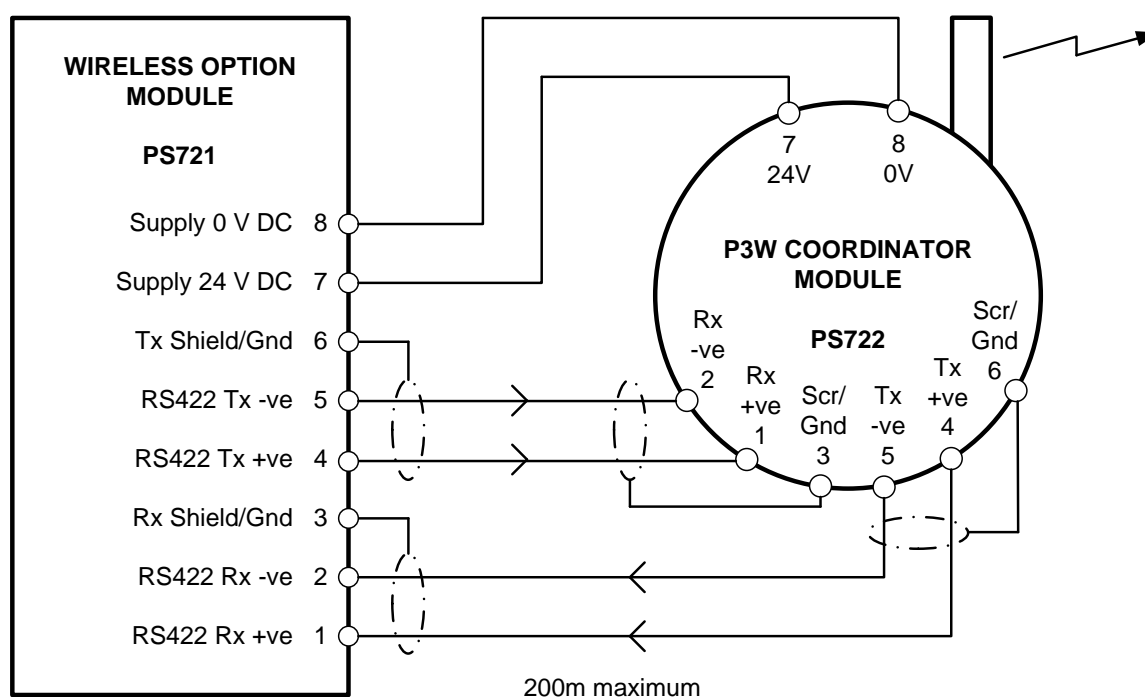
Fig 13:   *PS721 to PS722 connections (Master station to P3W Coordinator)*

1.8 P3W Repeater and P3W WMA AC Power Connections

The P3W Repeater AC and the P3W WMA AC will contain a power module for the appropriate power supply requested by the user. The power module is mounted the base half of the module with the wireless module in the other half, the modules will be connected together by an interconnecting loom, connected to SK1 on the power module and SK3A on the wireless module. The mains AC connections are made to the power module connections L1, L2 and L3, shown in the Figure below. The mains cable will need to be terminated in 4 mm ring crimps.

SK1, a flying lead, will be fitted by the factory to the appropriate tapping for the power supply that the customer has indicated will be used. Fitting to the posts labelled W, X, Y and Z selects the correct voltage. This should be checked for correct fitment before power is applied.

> ***Power should only be applied with the module fully assembled i.e. the base and the cover connected together with the bolts supplied.***
> ***Cable glands used must be appropriate to the classification of the area.***
> ***Conduit seals must be installed at the enclosure.***

A switch or circuit breaker must be included in the wiring installations. The switch or circuit breaker must be mounted as close to the module as possible and shall be marked to indicate that it is the disconnect device for that particular module. The Power cable and appropriate glands for the P3W coordinator will need to be sourced locally, according to site requirements.

Power supply: 3 Phase up to nominal 690V, 50 or 60Hz or
                           Single Phase up to nominal 230V, 50 or 60 Hz.

Check that the supply voltage agrees with that stated on the nameplate.

SK2 is the Modbus connection.
U1 is the cable screen clamp.
SK7 is the loom for the Wireless pcb.
FS1 is a 250 mA S500 fuse.
FS2 is a 100mA TDC11 fuse.
The wire attached to SK11 should be attached by one of the pcb mounting screws to the casing.
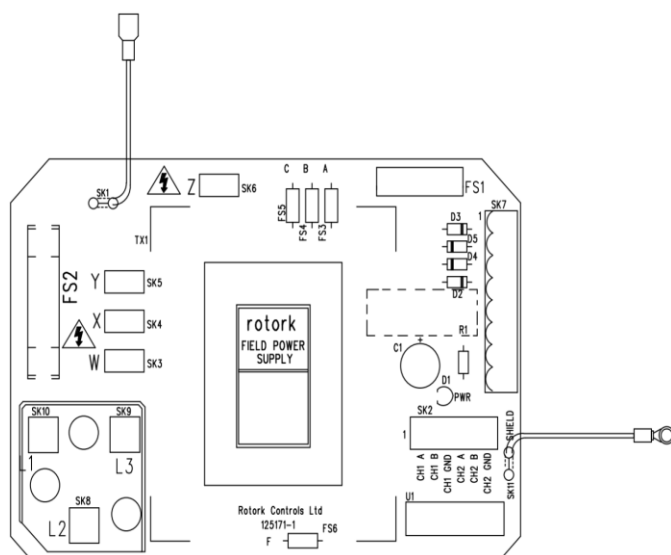
Fig 14:   Power module for P3W Repeater-AC and P3W WMA-AC.

1.9 P3W Repeater and P3W WMA 24VDC Connections

The P3W WMA DC may be powered from the Modbus device to which it is connected, assuming the device has the appropriate DC supply available. Under this circumstance the interconnection cable between the device and the P3W WMA-DC should contain 2 shielded pairs, one for power supply and one for the communication signal. In this case, the distance between the Modbus device and the P3W WMA-DC should not exceed 10 meters.

The P3W repeater DC may also be powered from an external DC supply in the same way.

Connect the power cable as shown below, the connector labelled SK3A is used on the P3W WMA-DC and P3W repeater-DC.

The power supply should be nominally 24volts (range 9-35volts, suggested power supply current capabilities – 200mA)
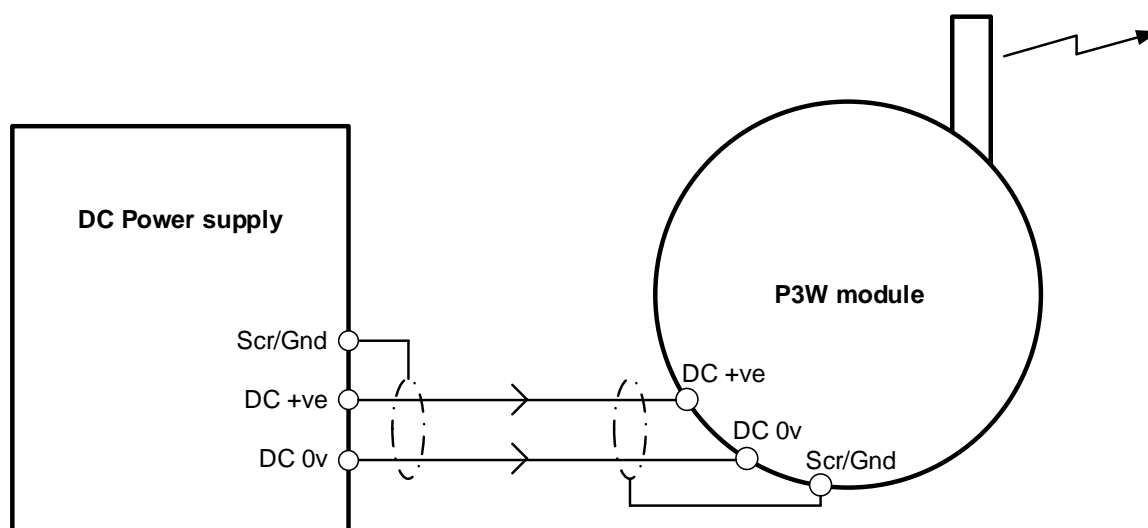
Fig 15:   *Connections from DC power supply to P3W WMA or P3W repeater*

1.10   P3W WMA Modbus Connections

The P3W WMA connects to a Modbus RTU device enabling a Modbus host to connect through the Pakscan wireless system to the Modbus device. The connection between the Modbus device and the P3W WMA should be made using a shielded network cable with 1 twisted pair of wires. Suitable cable conforms to the specification for RS-485 networks. This cable length will depend on the baud rate chosen for communications.

The Communications cable and appropriate glands for the P3W coordinator will need to be sourced locally, according to site requirements. Connect the Communications cable as shown below, the connector labelled SK3A is used on the P3W WMA.
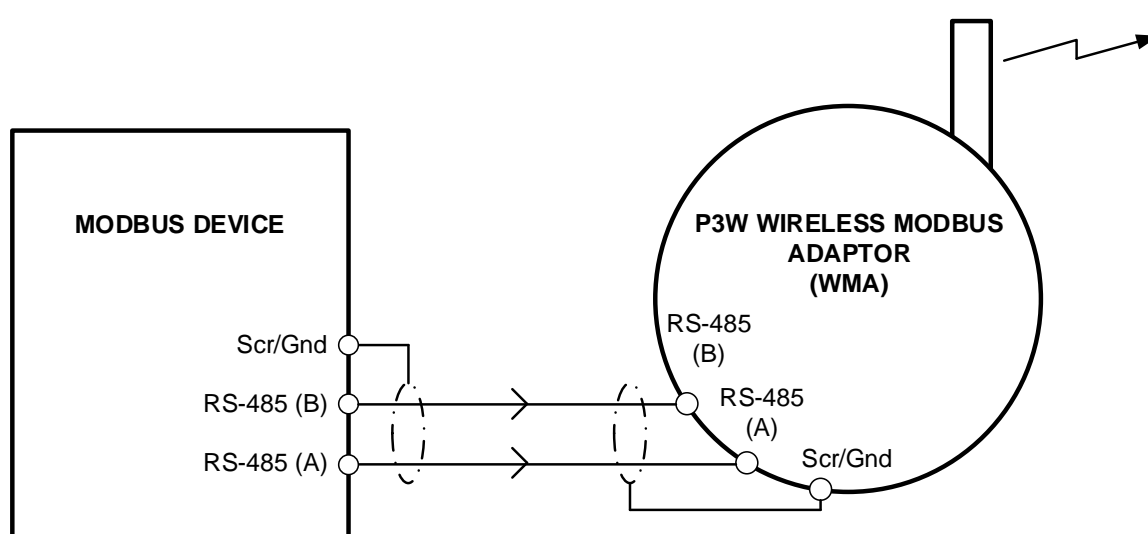
Fig 16:   Connections from Modbus device to P3W WMA

1.11   Setting up the P3W Repeater and P3W WMA

The P3W Repeater requires the PAN ID (Personal Area Network Identification number) and RF Channel to be set up for the network to which it is attached. The P3W WMA also requires these parameters and its Modbus communication parameters to be set up. This is achieved using the Modbus interface that is available on both modules.

The Modbus physical connections are detailed in the previous section 'P3W WMA (Wireless Modbus Adapter) Modbus Connections'. For the purpose of configuration, these connections can be temporary, for example, it may be more convenient to make the configuration changes in a workshop before installation on site. For both devices it is likely that configuration is only required once, therefore after installation there should be no need to access the Modbus connections again on the P3W repeater.

During configuration in a workshop environment, the 2 halves of the module can be separated, such that the Wireless module is disconnected from its power supply module. The wireless module can then be powered, separately, using a 24VDC source as described in the previous section 'P3W WMA (Wireless Modbus Adapter) 24VDC Connections'.

For making configuration changes to the P3W Repeater or P3W WMA, there is a fixed Configuration Modbus address of 248.

The P3W Repeater, requires the PAN ID and RF Channel to be set up, and if there are multiple P3W repeaters the Modbus slave address must be set up such that all P3W repeaters are unique and can appear as separate nodes on the wireless network.

The P3W WMA requires the Modbus communication parameters (baud rate and parity) to be set up, as appropriate for communicating to the Modbus slave device it is to be connected to. The Modbus slave device address is not required to be set up within the P3W WMA, as it will automatically scan for attached devices using the baud rate and parity set. Up to 10 slave Modbus devices can be connected, each device will require a unique Modbus address, within the range 201 to 247. The address must be unique for the host device to be able to access it. Within the master station configuration pages, the Modbus addresses used for the devices fitted to the P3W WMAs are required to be selected. See section 7.5.17 master station configuration.

Changes to RF communication parameters will take place immediately. Changes to Modbus communication parameters will take effect after a power cycle.

The principle of operation of the P3W WMA is shown in the diagram below.
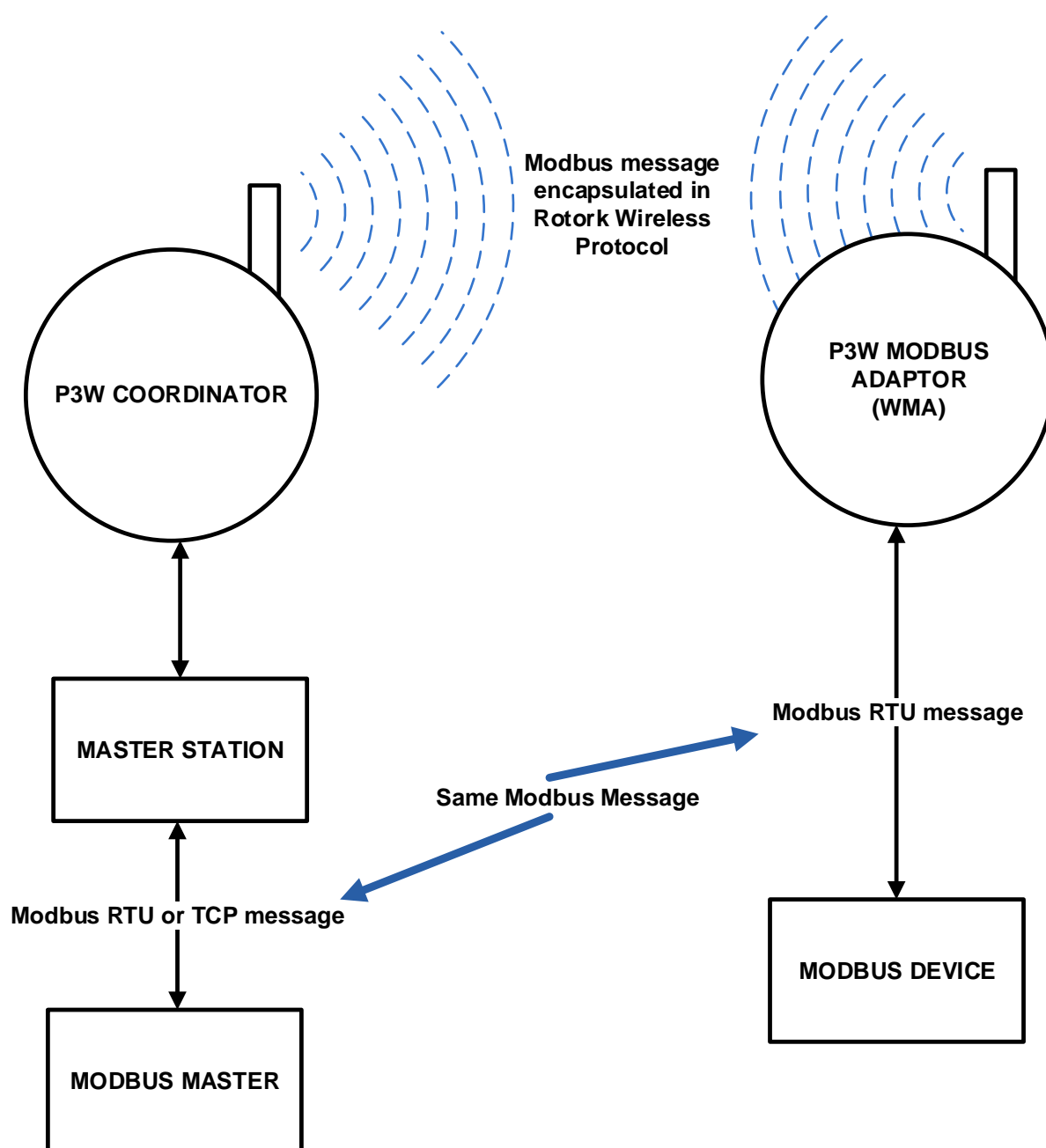
Fig 17: P3W WMA operation

The following parameters can be configured when addressing the P3W repeater or P3W WMA using the configuration Modbus address of 248:

Modbus Register	Modbus Function code	Description	Range	Default Value	Read / Write?
100	03, 04, 06, 16	PAN ID	0000 – FFFFhex (0 – 65535)	DA15 hex	R/W
102	03, 04, 06, 16	RF Channel	16 – 25dec (channel 16 to Channel 25)	22	R/W
104	03, 04	**P3W WMA**: Lowest Modbus Address of device (s) connected to the WMA, if no device is found this will default to 247	201-247dec	247	RO
	03, 04, 06, 16	**P3W Repeater**: Address of the repeater, required to be set up for the device to appear in the master station for status info – must be unique in the network	301-315dec	301	R/W
200	03, 04, 06, 16	Modbus Baud rate	Value 1 to 5: 1–9600 / 2–19200 3–38400 / 4–57600 5-115200	1 (9600)	R/W
201	03, 04, 06, 16	RS-485 Parity	Value 1 to 5: 1–None / 2-Odd 3-Even	1 (None)	R/W

Fig 18:   P3W Repeater and P3W WMA database

The baud rate of communications between the P3W WMA and the Device should be set to a value faster than the host (Modbus Master) will communicate to the master station.

1.12 Front Panel LEDs

There are four Light Emitting Diodes (LEDs) on the front panel of the CPU module, in the bottom right-hand corner. These are fitted to show if a unit is powered-up, which unit is in Primary or Standby mode and whether there are any errors or alarms.
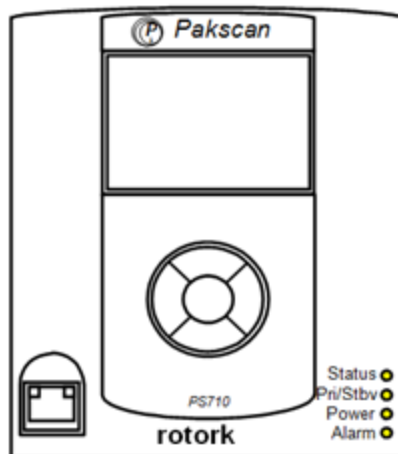
Fig 19:   CPU LEDs (Light Emitting Diodes)

On power-up, there is a sequence of colour changes and flashes from the LEDs, which take almost a minute to complete and confirms that all parts of the system are operating correctly:

The Status LED sequence is: off > amber > flashing green > steady green.
The Pri/Stdby LED sequence is: off > green > off > amber > steady green (amber for standby).
The Power LED sequence is: off > amber > green > green > steady green.
The Alarm LED sequence is: off > red > off > red > off.

The Status LED will show steady red if communications with the host is lost over Ethernet, or there is a communications error between the master station and a field unit. The LED shows flashing green only during the power-up sequence. The LED shows steady green to confirm that all applications are running after power-up is completed.

The Pri/Stdby LED will show steady green if it is a single unit or if it is the Primary unit of a hot standby pair. The LED will show steady amber if it is the Standby unit in a hot standby pair.

The Power LED is off when there is no power and steady green when power is present. It only shows amber during the power-up sequence.

The Alarm LED will show steady red if there are any alarm conditions in any field unit or the master station. This alarm will not prevent operation of the master station.

(The rest of this page is intentionally blank)

2.   THE FIELD CURRENT LOOP NETWORK

The Pakscan current loop field network must be correctly cabled and connected to the master station. The values of the field loop resistance and capacitance must be known to determine the loop speed that can be used. If these are not known then the LOWEST loop speed must be set in each actuator and the master station to ensure good field network connectivity.

Port A
OUT = Term'l 5
IN = Term'l 4

Port B
IN = Term'l 1
OUT = Term'l 2

Up to 240 actuators
per loop

Current loop
- up to 20 km
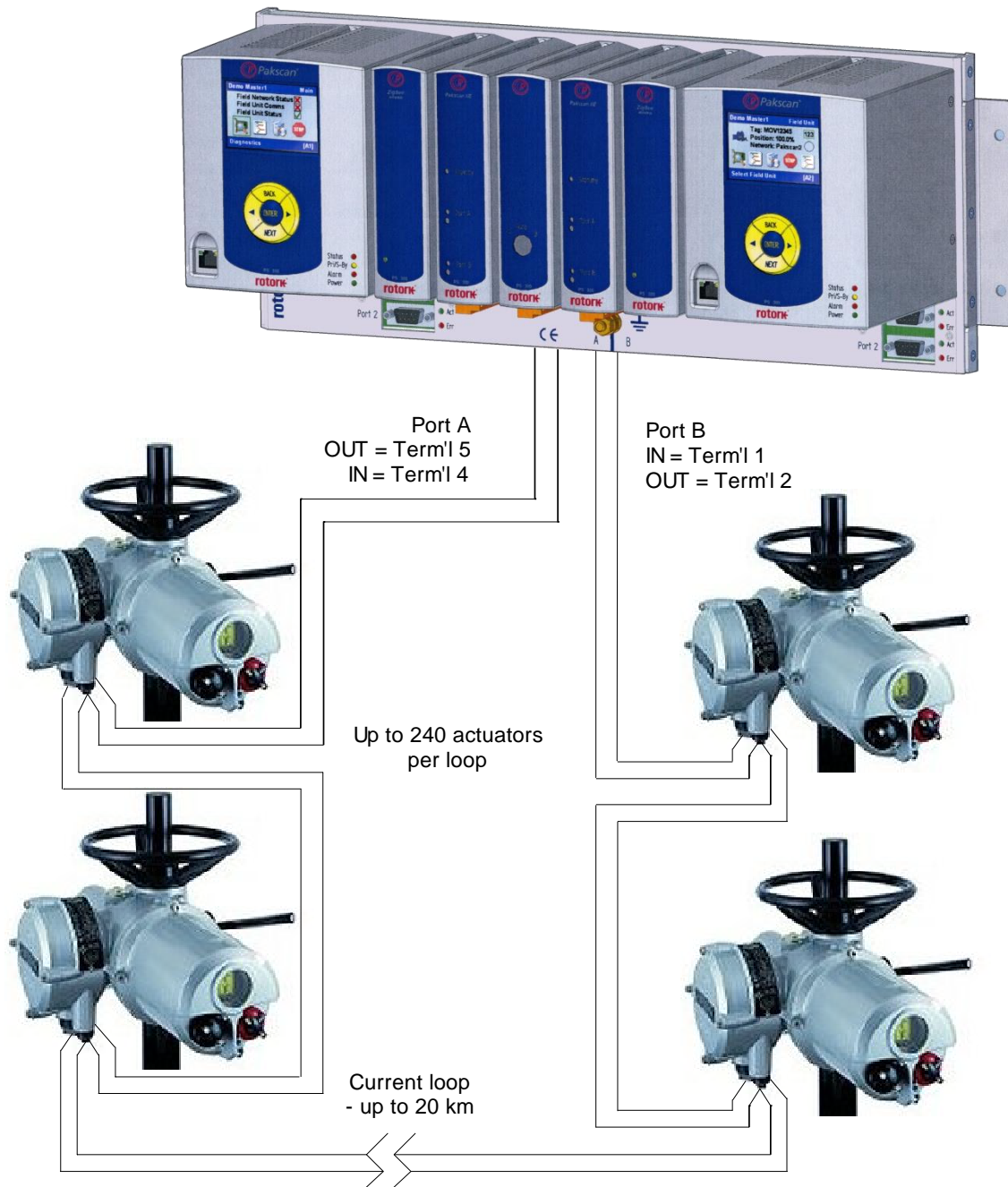
Fig 20:   Pakscan P3 Wired Network

2.1 Loop Checks

The most common errors in installing the system occur on the field wiring.

Loop Continuity

> With all the field units connected, but none of them powered up, check the continuity of the 2 cores of the Pakscan loop cable. Measure and record the resistance of each core. These measurements will be useful as they can be compared with future measurements to determine if cable resistance has changed significantly or not, this may help identify a cable fault. Cable resistance (R) is the sum of the resistance of both cores.

Screen Continuity

> Screen continuity must be continuous between each end of the loop. Ensure the screen is either connected to a signal earth bar at only one point or to terminals on the loop driver plug; pin 6 connects directly 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 loop driver, so as to ensure the product meets the European Directive on EMC.

Cable Capacitance

> The capacitance (C) between the cores of the cable is critical to system performance. Too high a capacitance for the selected loop baud rate will result in poor communications, or even communication failure. If a suitable meter is available, measure and record the capacitance between the cable cores.

Maximum Loop Speed

> The cable resistance must not exceed 500 Ohms (250 Ohms per core) and the total capacitance must not exceed the maximum value for each communication speed. In addition to cable capacitance, each field unit adds a small amount of capacitance to the loop which must also be considered when determining maximum loop speed. Use the measured resistance and capacitance values from the above tests to determine which loop speed should be used.

Baud Rate	R max (ohms)	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 field unit will add a capacitance of 2.2nF
>
> The C max figure given is the maximum value for the network capacitance including the field unit capacitance.

Test Equipment

> A good quality multimeter with capacitance test facility is adequate for testing loop resistance and capacitance. Under no circumstances should any high voltage test equipment be used such as insulation Megger testers when any part of the cable loop is connected to either the master station or actuators. The high test voltages generated by such equipment may damage the Pakscan components.

2.2 Connecting Up

Once the checks are complete, connect the Loop Cables to the PS730 Key switch module on a hot standby system or the PS720 Current Loop module on a single system. The Pakscan loop should look like the figure below. Check the loop wiring complies with this drawing and then proceed to Section 8.1 for commissioning instructions.
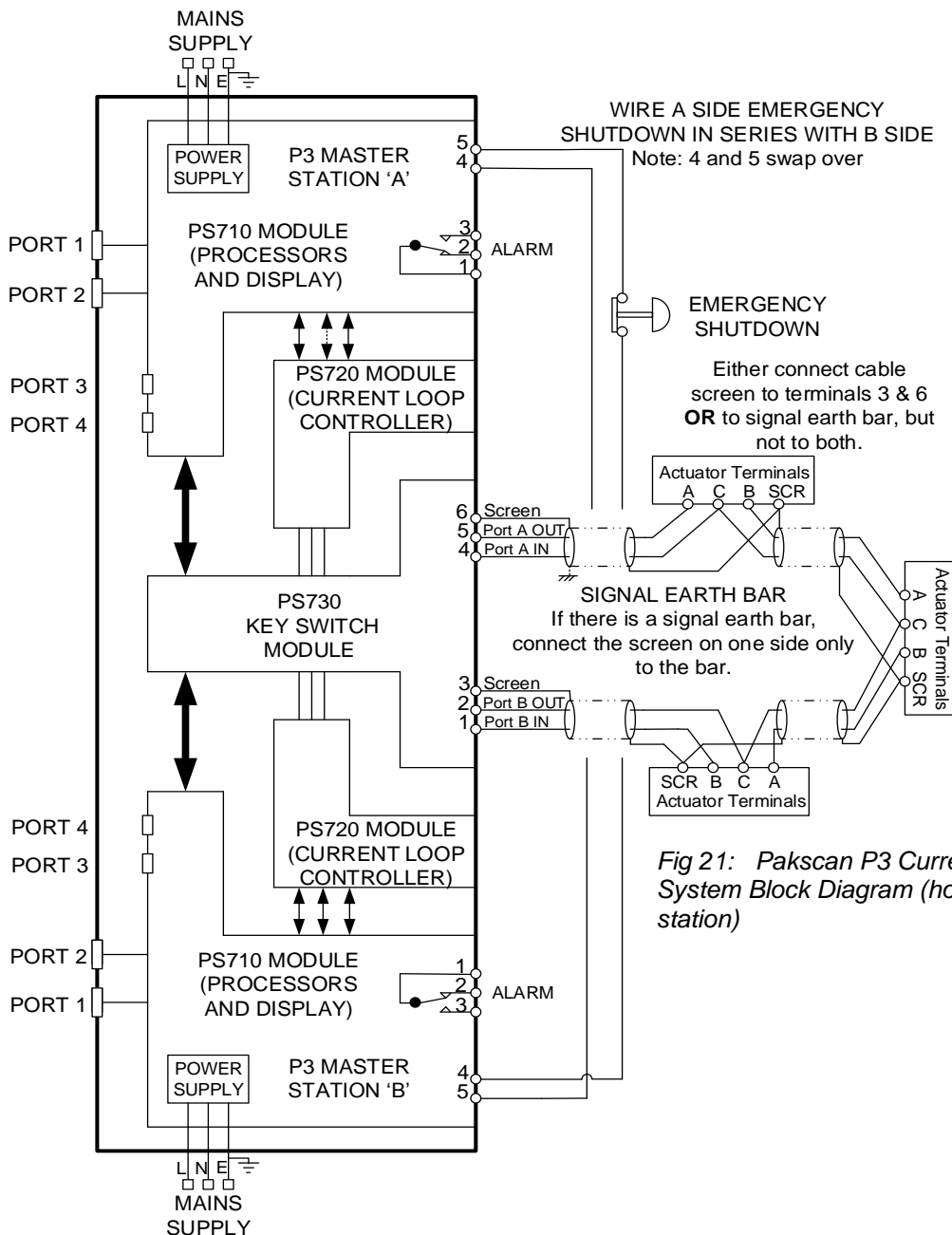
Fig 21: *Pakscan P3 Current Wired Loop System Block Diagram (hot standby master station)*

Note: If there is no hard-wired ESD requirement a shorting link must be fitted across pins 4 and 5 on both side A and side B of the PS710 modules.
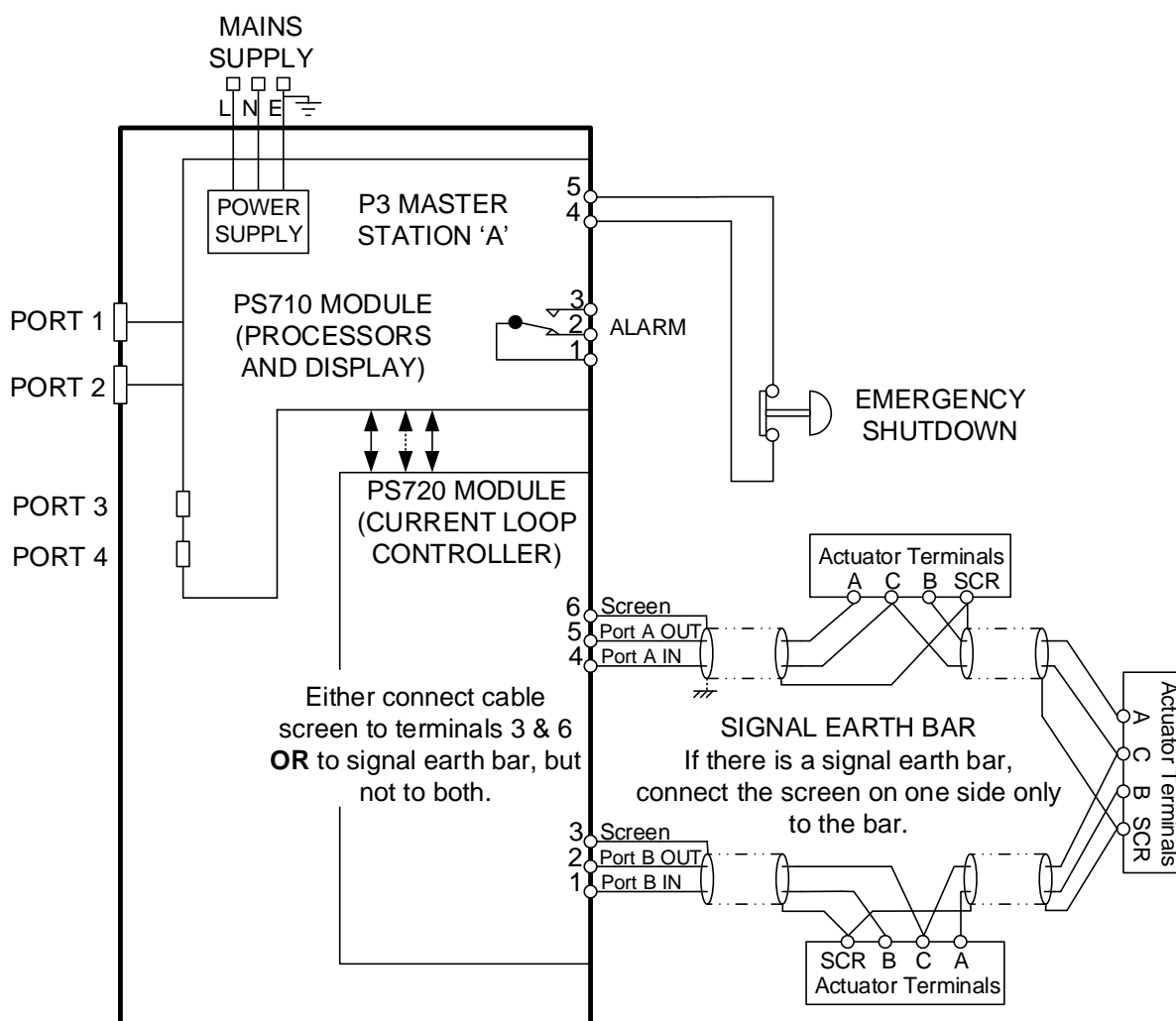
Fig 22: Pakscan P3 Current Wired Loop System Block Diagram (single master station)

Note: If there is no hard-wired ESD requirement a shorting link must be fitted across pins 4 and 5 of the PS710 module

3.   THE FIELD WIRELESS NETWORK

A Pakscan wireless network will contain a master station with a PS721 module fitted to its back plane (2 for hot standby). Each of these will connect to a PS722 P3W coordinator module. The P3W coordinator module is the device that controls and organises the wireless network. For an actuator to be connected on the network it must have a wireless actuator module. The IQ and IQT range of actuators fully integrate into the wireless system. Other devices can be integrated into the system using a Wireless to Modbus adaptor (P3W WMA). The P3W WMA can be attached to any device that has a Modbus interface on it. The host then uses the master station and the wireless network as a transport layer only to send Modbus messages that are directed to a Modbus device.

A network may also require a number of P3W repeaters to overcome wireless dead spots or to ensure a redundant path to all devices.
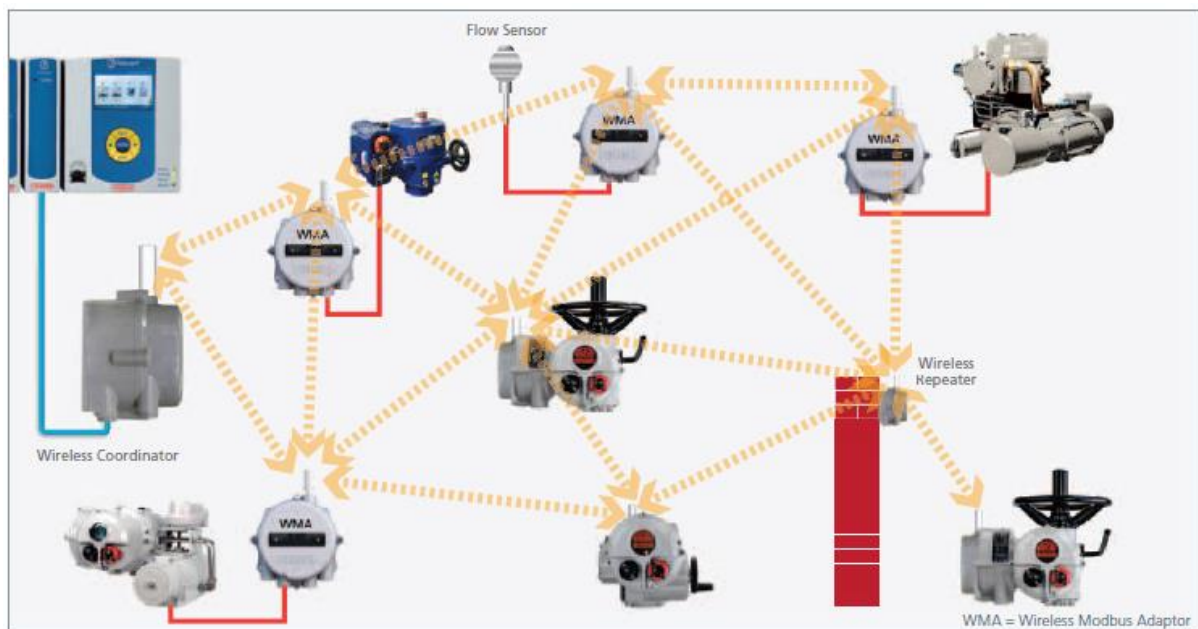
Fig 23:   *A typical P3 wireless network*

Up to 60 devices can be connected in a wireless network. The distances between each node in the network is recommended to be no more than:
>   Indoors: 30 metres
>   Outside: 100 metres

In practice, it has been found that these distances can be extended, but a site survey is required to confirm this. Each device is able to route messages onto the next device. By this method, the range of the network is increased. It is recommended to have no more than 7 'hops' from the master station to the final device. A 'hop' is where a message routes through a wireless device to get to the destination device.

3.1 Wireless Site Survey

The first step in setting up a wireless network will be a Wireless Site Survey, which would be performed by Rotork Personnel. This will establish the suitability of the site for a wireless network. The survey will establish the levels of background wireless signals within the spectrum of the 2.4 GHz band used for the P3 wireless network and also the potential strength of the wireless signals between the actuator and P3W coordinator locations. This will aid in positioning the P3W coordinator and in deciding upon the need for P3W repeaters.

As a result of the survey, one or more channels within the band will be found to be suitable for the network. All devices on the network will be shipped with a default channel set.

3.2 Wireless Specification

Network Based on:	IEEE 802.15.4, DSSS (Direct Sequence Spread Spectrum).
Maximum Wireless devices:	60.
Frequency:	2.4GHz band.
Operating Range:	30m indoors, 100m outside.
Network Structure:	Mesh.
Channels available:	16. (Currently 13 are useable).
Security:	AES and anti-spoofing.
Power:	10mW default, potential for 100mW if the location allows.

3.3 Connecting Up

The IQ and IQT actuators fitted with a wireless module will only require mains power connections and the appropriate glands for the environment to be connected to them. Where a P3W WMA is supplied, power is required to be provided by the user and the user must also provide the necessary cable and glands between the WMA and the device to which it is attached. A P3W repeater also only requires a power cable and glands supplied by the user. The power required for the P3W Repeater and P3W WMA will be indicated on the serial label.

Figure on the next page shows the master station block diagram.

The site survey will have indicated the appropriate position to locate the P3W coordinator(s) and any P3W repeaters. Once all the equipment is in place, the user can then proceed to Section 8.2 for commissioning instructions.
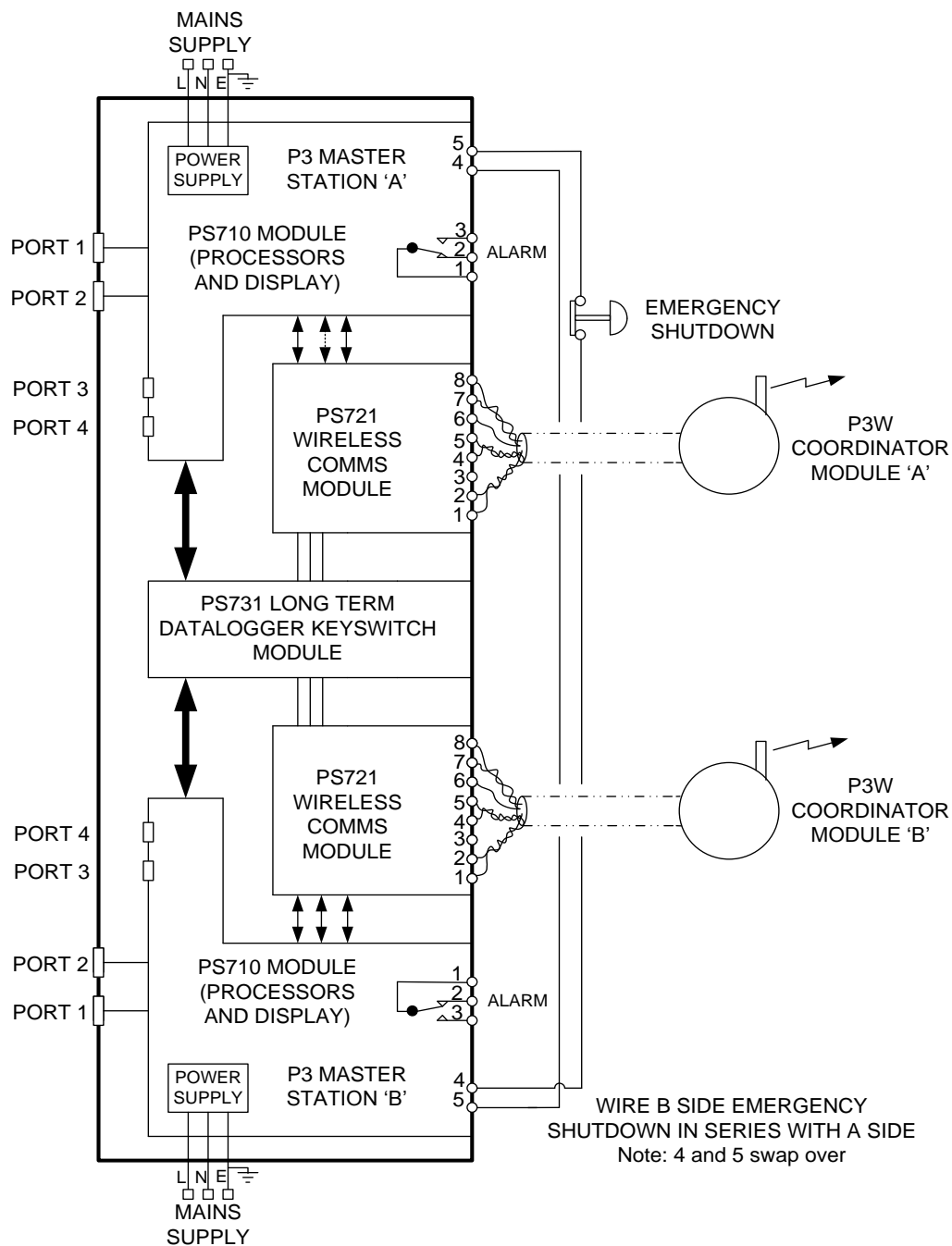
Fig 24:   *Pakscan P3 Wireless network Block Diagram (hot standby master station)*

Note: If there is no hard-wired ESD requirement a shorting link must be fitted across pin 4 and 5 on both side A and side B of the PS710 modules.

(The rest of this page is intentionally blank)

4. CONFIGURING SERIAL COMMUNICATIONS

The Pakscan 3 CPU module has two serial ports. Each of these is configurable for RS-232 or RS-485. Most hot standby systems will probably require two RS-485 connections in a seamless redundant configuration. Single systems may use RS-232 or RS-485.

4.1 Setting Port 1 and 2 for RS-232 or RS-485

The chassis has DIP switches behind the PS710 CPU module for setting the type of serial port that is presented at the port connectors.
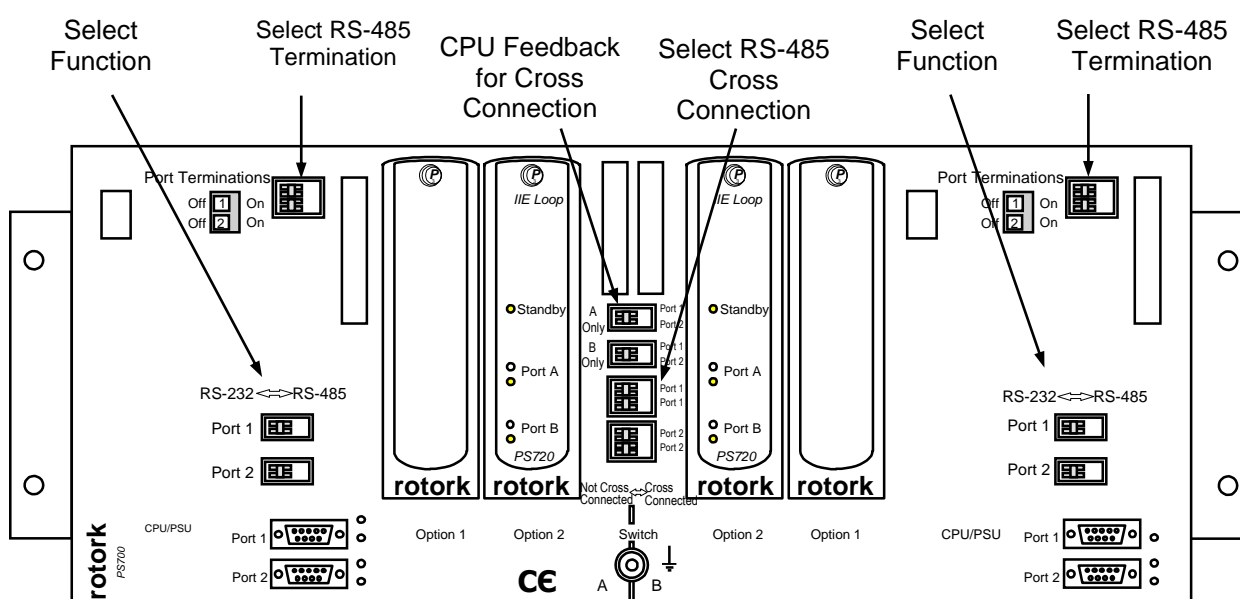
Fig 25:   Pakscan P3 Chassis, CPU and Key Switch modules removed

The switches on the backplane behind the PS710 CPU Module are used to set Port 1 and Port 2 parameters.

To access the switches, you will need to remove the modules shown above from the backplane.

To do this, power-off the master station completely from any power sources, either mains or DC. Then unscrew the hex head bolt from the top of the module using the 2mm ball driver tool supplied with the master station. Once the screw is removed, or loosened sufficiently, the module may be carefully pulled forward at the top until the lower claws of the module can be unhooked from the slots in the backplane.

If any plugs are left in the power sockets or serial sockets, these may prevent you from tipping the module forward sufficiently to unhook it from the backplane.

Replacement of the module is the opposite of removal, being careful to align the module and backplane connectors.

Port Function

RS-232 ⟸⟹ RS-485

Port 1

Port 2

Two DIP switches allow each port to be selected between RS-232 and RS-485. For RS-485 slide the appropriate Port switches to the right, for RS-232 they should be on the left.

Each of the two ports may be set independently.
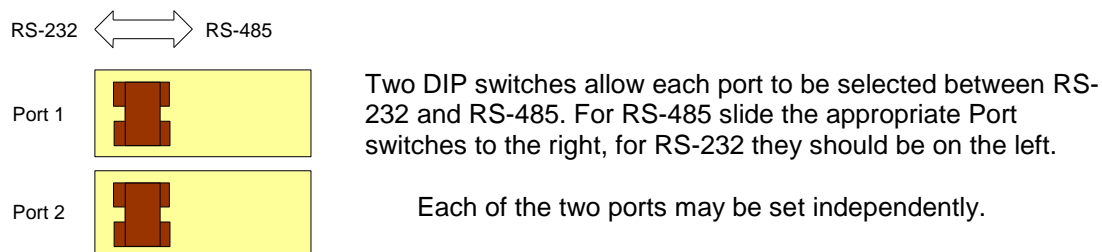
Fig 26:   Port Function Switches shown in RS-232 position

RS-485 Termination Resistors

Two DIP switches are used to connect end-of-line termination and biasing resistors to the RS-485 highway. All RS-485 network highways must be terminated at **both ends of the highway,** in this case, at the host controller and at the master station. Only RS-485 highways need termination and biasing resistors. If a CPU port is configured for RS-232, it must never be terminated. Each port can be terminated independently.

Each CPU module serial port sits on an independent highway and should be terminated independently. So, if ports 1 & 2 on a CPU module are both being used for redundant RS-485 communications to a Host controller, then each port may need to be terminated and biased.

However, where more than one CPU Module sits on the same RS-485 highway, then only the one furthest from the host controller needs the biasing and termination resistors to be enabled.

Port Terminations

Off | 1 | On
Off | 2 | On

+5V
1k
Off   On
Data +
120
Data -
Off   On
1k
Gnd
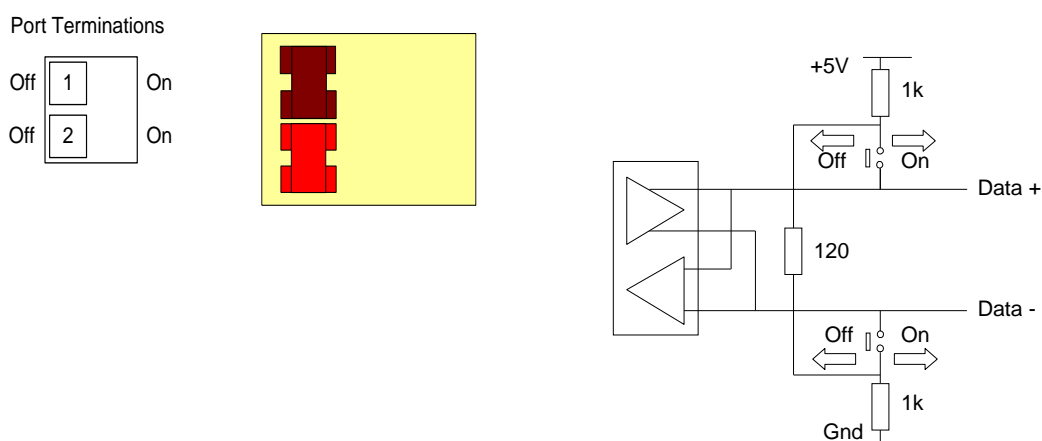
Fig 27:   Port Termination Switches shown in Off position

Cross Connection switches

The cross connection switches, found on the backplane behind the PS710 CPU Module, are used to cross connect the serial RS-485 connections. They are only applicable for a hot standby system and should ONLY be set as cross connected for a port that has been selected as RS-485.
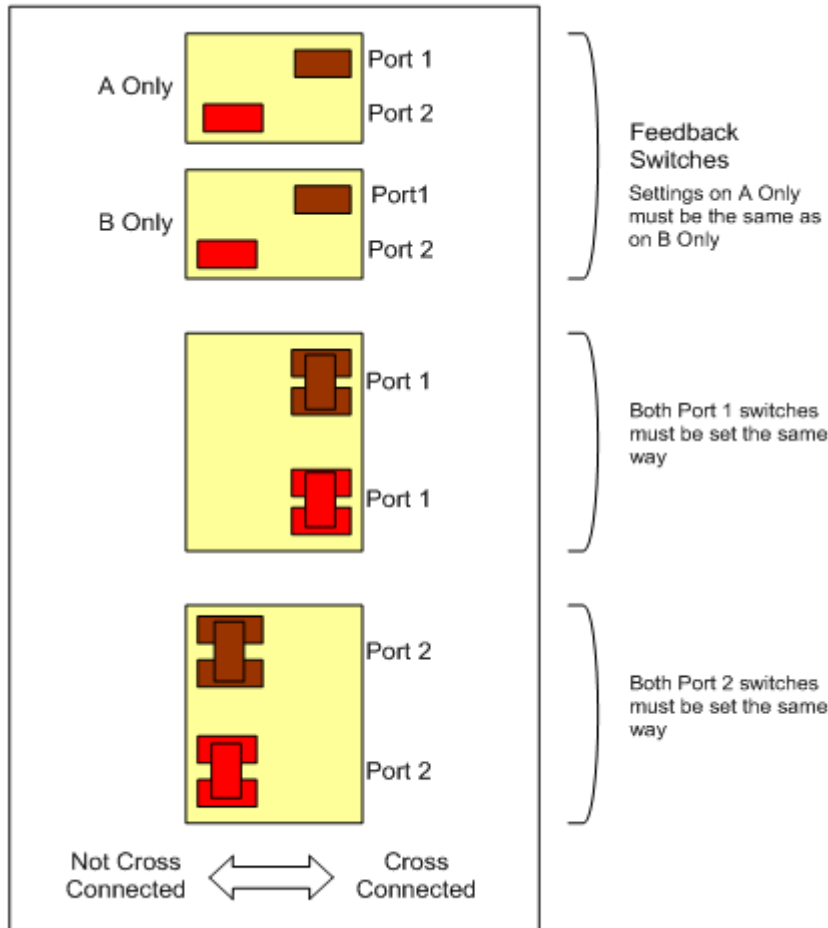
Fig 28:   C*ross connection switch settings on the backplane behind the Switch Module*

The switches are shown in the Factory Default positions (Hot Standby).

Port 1 is set to Cross-Connected for RS-485 Serial communications. Port 2 is set to Not Cross-Connected for RS-232 Serial Communications.

The feedback switch positions must reflect the Cross-Connection settings for Port 1 and Port 2. These switches are used, by the master station CPU, to indicate to the user (via the HMI or web pages) the position of the cross-connect switches.

Typical Serial Host connections to the P3 master station and appropriate switch settings:

Hot Standby RS-485 communications
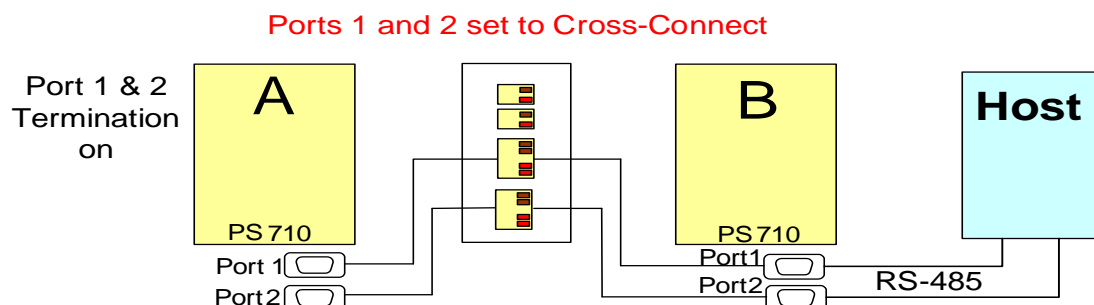
Communications between the Host and the master stations uses the Modbus protocol. Because the Master A is cross-connected to Master B, they both share the same Modbus address. The standby action must then be set to passive. Thus, the host can have two-way communications with the Primary (Main) module and the Standby module will only listen to the messages.

Hot Standby RS-232 Communications
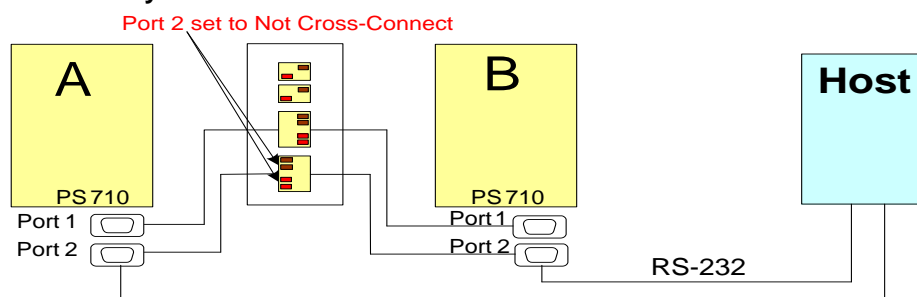
With RS-232, communications between the Host and Hot Standby master station must be point-to-point. Multi-drop connection is not allowed, so separate cables must be run from the Host to each side of the master station. Also, the Cross-Connect switch must be set to Not Cross-Connect. The standby action must be set to active, so that the Host has full communications with Master A and Master B. Note: only actuator commands sent to the Primary CPU Module will be actioned.

Hot Standby dual Host RS-232 or RS-485 communications
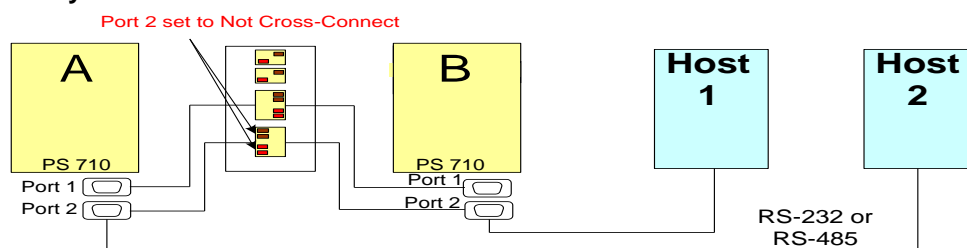
Fully dual-redundant system. Port 2 set to RS-232 or RS-485 to match Host communication

Fig 29:   Hot Standby Serial Communications

5. CONFIGURING ETHERNET COMMUNICATIONS

Pakscan 3 master stations come complete with two Ethernet ports for connection to host systems. A third Ethernet port is also available for connection to a computer for configuration purposes. The master station is ready to use with Ethernet and Modbus TCP protocol for the host to access data and control the actuators on the field network. The IP address is factory set to the default value and can be changed during set up of the master station.

The Pakscan master station defaults to the same IP address on both ports, and can use the same address on the A and B master stations. It is possible to change the IP address on either master station, but ports 3 and 4 of each CPU Module always have the same address.

Hot Standby Ethernet communications
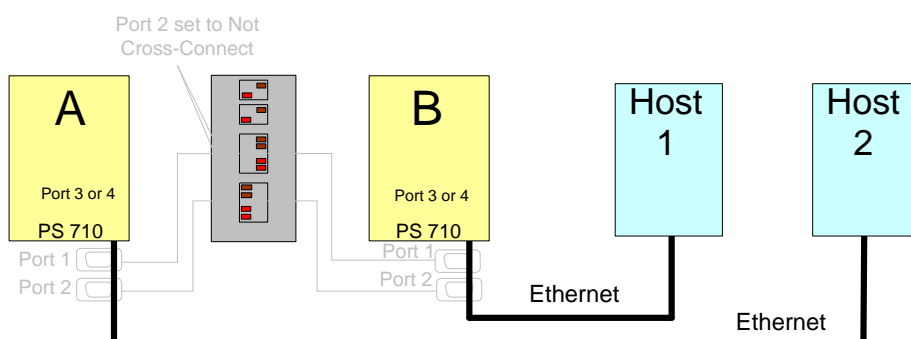
Ethernet comms between Hosts and master station are made using Port 3 or Port 4. The Cross-Connect switches can be in either position, or set appropriately for any additional serial comms. In this case, with two Hosts, Standby must be set to Active. The IP address of Master A and Master B can be set to be the same or different, with Standby Active.
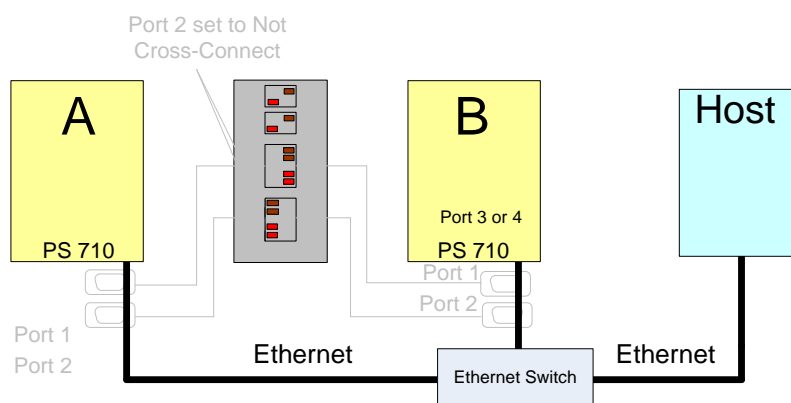
Where an Ethernet switch is used to connect a Host to the hot standby master station and the IP address is set the same for Master A and B, then Standby must be set to Passive.

Fig 30:   Hot Standby Ethernet Communications

Hot Standby Redundant Host, Redundant Ethernet communications
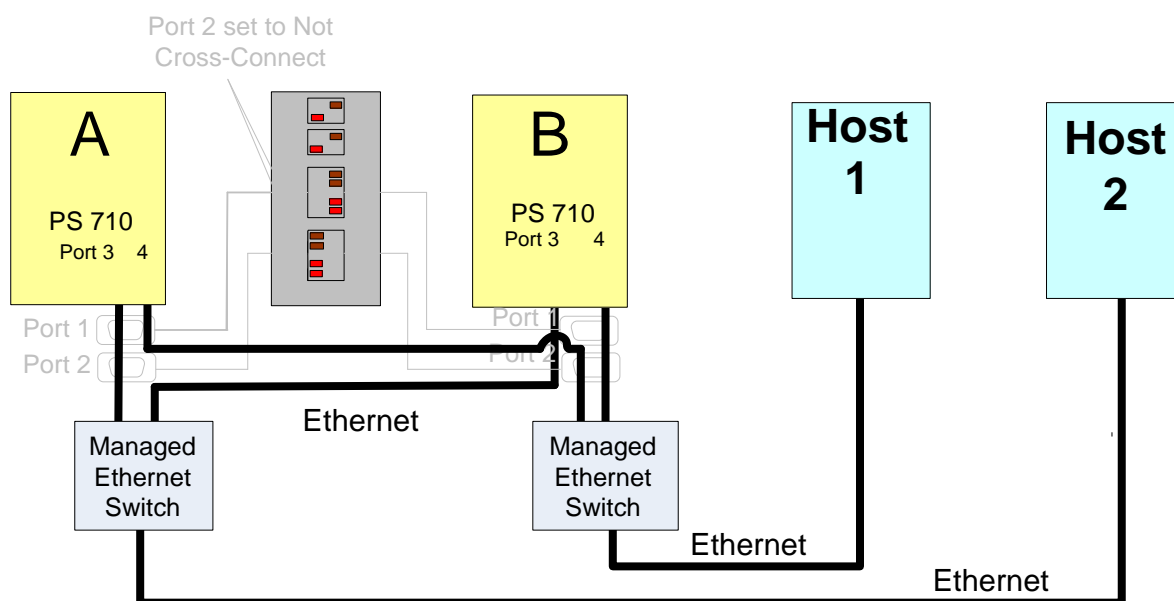
Fig 31:   *Hot Standby, Dual Redundant Ethernet Communications*

For full Ethernet communications redundancy, use two Hosts and two managed Ethernet switches. Managed Ethernet switches with rapid spanning tree protocol are required. This type of switch is able to prevent Ethernet Storms, where messages are re-circulated continuously.

Ethernet communications between Hosts and master station are made using Port 3 and Port 4. In this case, with two Hosts, Standby must be set to Passive. The IP addresses of Master A and Master B can be set to be the same with Standby Passive, or different, with Standby Active.

The Pakscan P3 master station defaults to the same IP address on all ports. It is possible to change the IP address for Master A and Master B independently, but all ports for each master will have the same address. In a hot standby system, if the Copy IP Settings option is selected, both sides of the master station will have the same IP address.

5.1 Default Ethernet Settings

The default Ethernet parameters set in each Pakscan 3 CPU Module are given below:

DHCP	Static			
Default IP address	10	200	1	1
Default Subnet mask	255	255	255	0
Standby Action	Passive			

Changes to the IP address, Subnet Mask or clock settings will cause a re-boot of the CPU module.

The master station uses the 192.168.1 subnet internally, therefore if it is required to set the external IP address of the master station to a value within this range the internal address will need to be modified. Contact your local technical support team for details.

5.2 Ethernet Security

When connecting the master station to an Ethernet network, care should be taken to consider security of the master station.

There are a number of Ethernet services available in the master station and, where appropriate, the user should ensure that the Ethernet infrastructure is able to protect the master station from unwanted access to a service.

Transmission Control Protocol (TCP) and Internet Protocol (IP) are the core protocols utilised in Local Area Networks (LANs) and computer networking. Within these networks a 'port' is an endpoint to a logical connection – not to be confused with the physical port!

The port number in this case refers to the type of port. For example, port 80 is used for HTTP web page traffic.

The ports that are available at the master station are:

Port description	Port number
HTTP	80
HTTPS	443
Modbus/TCP	502, 50003, 50004, 50005, 50006, 50007, 50008 and 50009

Ethernet products, like routers, can prevent other Ethernet equipment on the same LAN from accessing certain services in the master station. If web page access were not required, the most secure set up would be to prevent all but Modbus traffic entering the master station.

(The rest of this page is intentionally blank)

6. SETTING UP THE MASTER STATION BY THE KEYPAD

The Pakscan 3 master station CPU module has a full colour display and 5 button input pad. All the settings for the performance of the master station, the Option module fitted and the Field Network can be made using these facilities. The keypad and screen also allows every connected actuator to be interrogated and its status monitored. Finally, the actuators and valves can be moved using these facilities.

Alternatively, a computer with an Internet browser facility can be used with the internal web server pages. These pages allow the whole system to be set up and modified. In addition, they allow the connected actuators to be viewed and controlled.
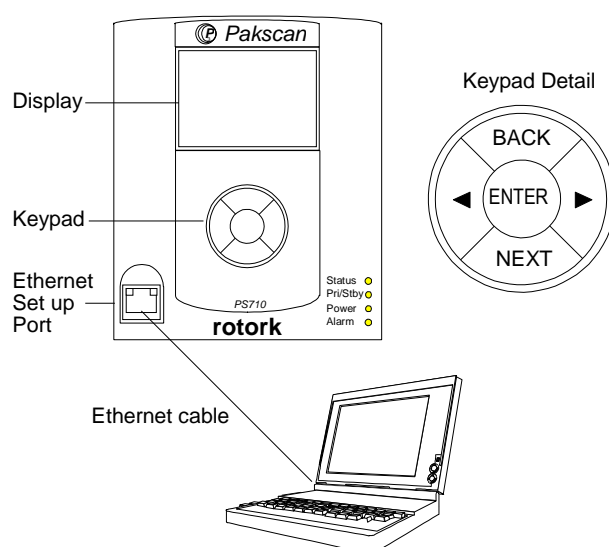
Fig 32:   Pakscan P3 Main module connection to laptop and keypad detail

6.1 Using the Keypad

The keypad controls the movement through the display screens and the movement within each screen, as well as the ability to input data or requests.
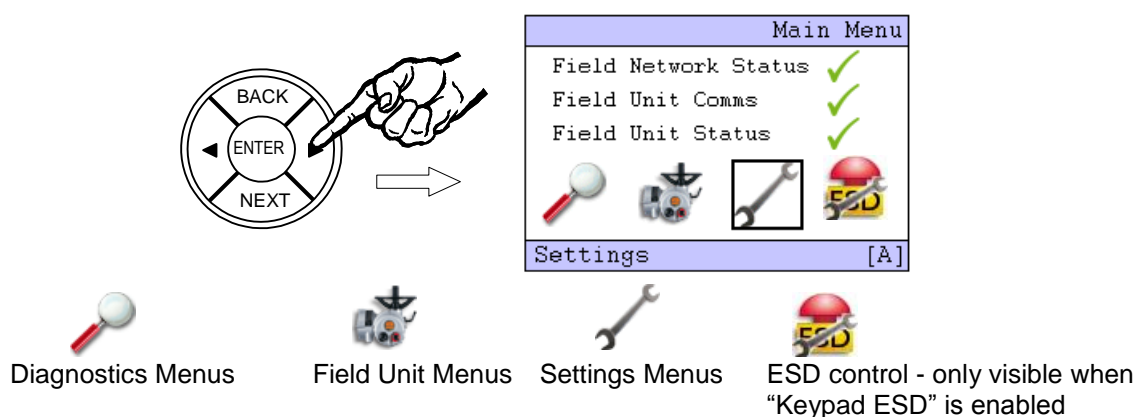
❑ ◄ **(Left) and ► (Right) arrow keys** Allow active items within a page display to be highlighted. If the item is selected and a numeric input is needed, then these keys increase or decrease the number.

❑ **ENTER** Selects a highlighted element on the screen or completes the entry of information.

❑ **BACK** and **NEXT** **BACK** moves up one level in the menu of the displays, returning to the previous screen viewed. **NEXT** only functions if there is more data to show than fits on the screen. When there is additional data, a small arrow is shown on the right side of the screen. It points down (↓) for **NEXT** and up (↑) for **BACK** to operate.

6.2 The Screen Display

The opening, or top screen display shows the network status and three icons (four icons, if keypad ESD is enabled – see below).

Menu Section

Network Information

Current Status

Selected Icon Highlighted

Selected Icon Function

Menu Location

The Diagnostics icon (Magnifying Glass) will have a black square around it. The position of the square indicates the part of the menu that will be accessed if the **ENTER** key is pressed. The highlighted icon can be changed by pressing the arrow buttons (◀ or ▶) to scroll round them. The bottom bar shows the selected function as a text message.
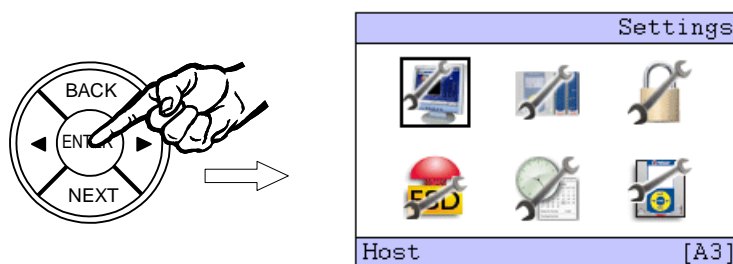
Diagnostics Menus   Field Unit Menus   Settings Menus   ESD control - only visible when "Keypad ESD" is enabled

Highlight the Spanner icon for 'Settings'; then press **ENTER**. The menu location changes to A3 and the 'Settings' menu screen appears with the 'Host' icon selected.

This screen also contains the icons used for access to all the other setting menus.

 Host   Option Module   Security

 ESD   Date/Time   M/S

6.3 Setting the Current Loop Option Module Parameters

On the 'Settings' menu, select the Option Module Icon by pressing the right arrow key (►) followed by the **ENTER** key.
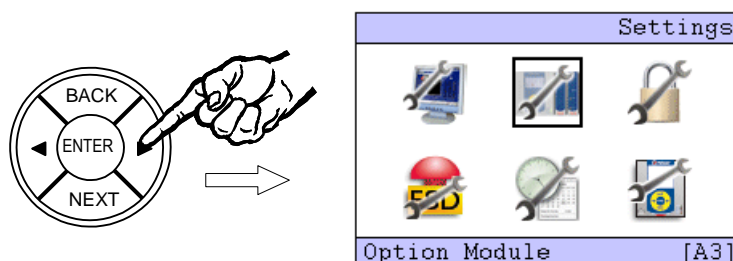
The Option choice screen appears where the module to be set can be selected. Firstly we need to ensure that the field units are correctly assigned to the field network chosen. The selection box by the 'Option 1' text should be highlighted by pressing the right arrow key twice (►).
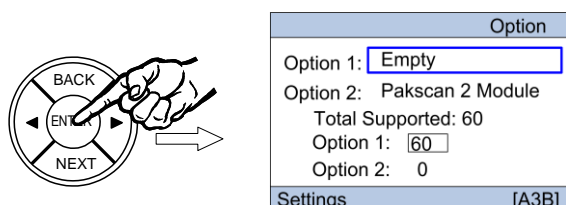
Pressing **ENTER** enables changes to be made using the left (◄) or right (►) arrow key, press the **ENTER** key to make a change to the value. This box will increment in steps of 60. In a wired only network all available field units should be allocated to the Pakscan 2 module. Once the number is correct, press **ENTER** once more
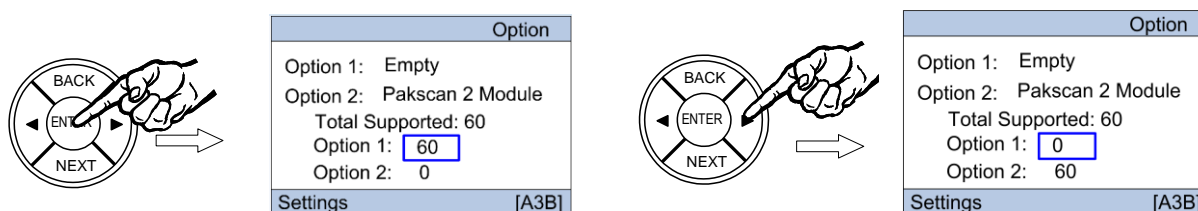
To make changes to the Pakscan 2 Current Loop module settings, highlight Option 2 by using the left (◄) or right (►) arrow key.
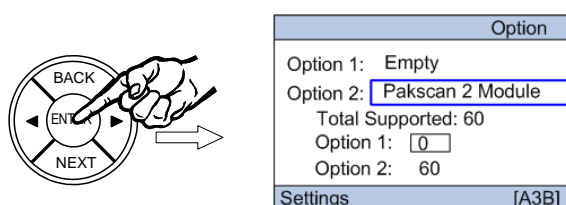
Pressing **ENTER** brings the next choice for the setting. This time select 'Loop Settings' by once more using the right arrow key (▶).
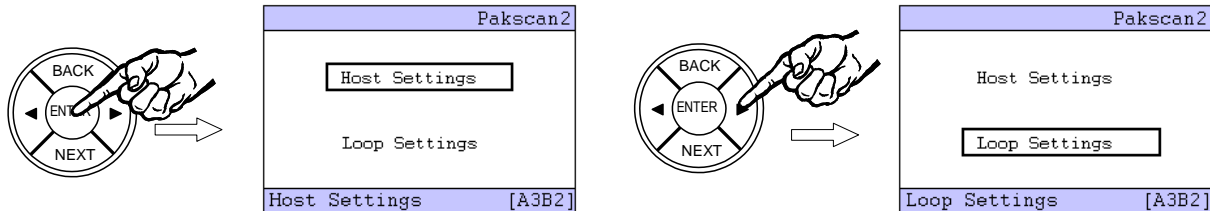
The Loop Settings screen is split over two pages, as indicated by the small arrow (↓) on the right side of the screen, so the **NEXT** and **BACK** buttons are used to jump between the two.

Once a setting box is highlighted, by using the left (◀) or right (▶) arrow key, press the **ENTER** key to make a change to the value. This will make the security screen appear for the PIN number entry. The default value for the system security requires a PIN to be entered before any settings can be changed. This setting can be altered from the Security Setting menu.

The default PIN number is 0000. To enter a PIN, or accept the number, press **ENTER** and the first digit will flash. The value can be changed by using the left or right arrow keys (◀ or ▶). Once the number is correct, press **ENTER** once more. When all 4 digits of the PIN are entered correctly, select the OK button with the arrow keys (◀ or ▶).

Press **ENTER** and the screen will return to the settings screen and the Current Speed will be highlighted. Press **ENTER** once more to select this parameter and the current value begins to flash.
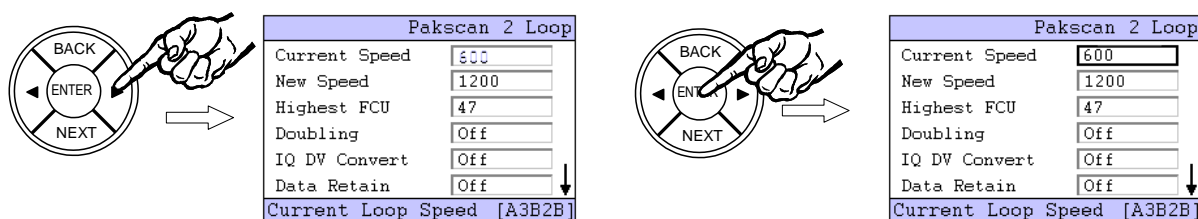
Use the arrow keys (◄ or ►) to change the value shown until the desired figure appears, then press **ENTER** and the new value will be set. The arrow keys can be used to navigate to other settings, and the **NEXT** button goes to the Loop Test screen and Loop Reset function.

❑ Set the loop performance parameters in accordance with the data recorded earlier. Make sure the loop speed is compatible with the setting for the loop capacitance.

❑ Set the highest field unit address parameter equal to the actual highest address.

❑ Doubling can be set to 'On' if the loop performance is not fast enough. It has the effect of halving the time to collect data from the field units. This feature will only operate if the loop is functioning correctly with "loopbacks off".

❑ IQ DV Convert should be set to 'On' if analogue position control is being used on the IQ / IQT actuators on the network.

❑ Data Retain set to 'Off' clears all the field unit data if communication is lost. Some host systems want the data to be retained, in which case set the parameter to 'On'.

Once the parameters are all set, leave this part of the setting menu to ensure the new values are loaded. Use the **BACK** button to return to the Host Settings page, and then **ENTER** to select the Host Settings menu.
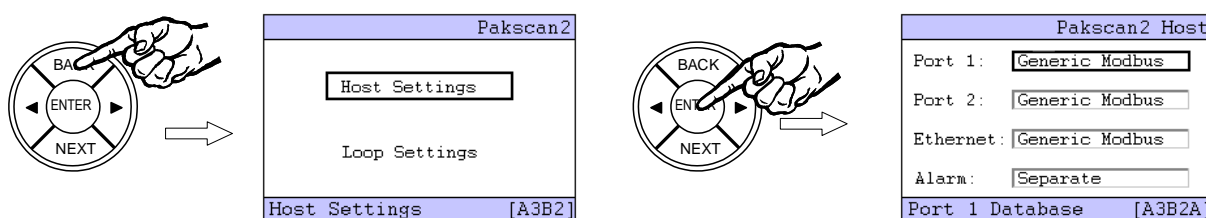
Make alterations to the host protocol settings and Alarm linkage, if required, in a similar manner to altering the loop performance parameters described earlier. The PIN will need to be entered if no keys are operated for approximately 5 minutes from the last PIN entry. Where the two serial ports are being used by the same host system it is advisable to 'Link' the alarms so that both ports always report exactly the same alarm data.

When the settings are as required, use the **BACK** key to return to the top Settings menu.
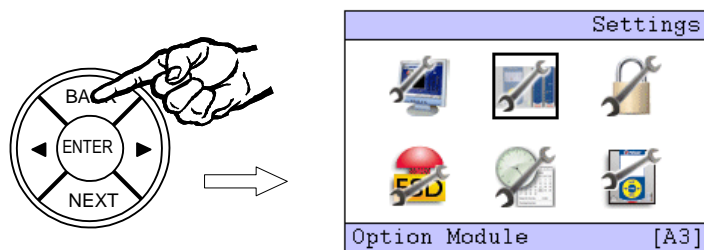
6.4 Setting the Wireless Option Module Parameters

On the 'Settings' menu, select the Option Module Icon by pressing the right arrow key (▶) followed by the **ENTER** key.
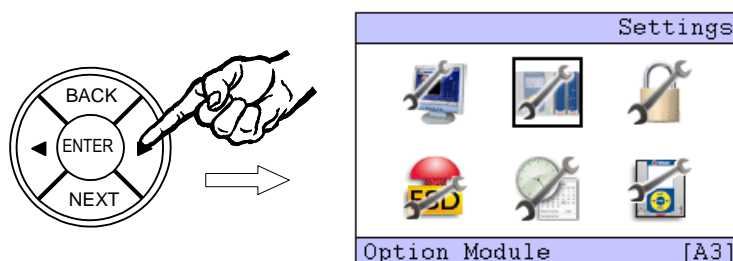

The Option choice screen appears where the module to be set can be selected. The Pakscan Wireless is always in the Option 1 slot and this is highlighted as the page is entered.
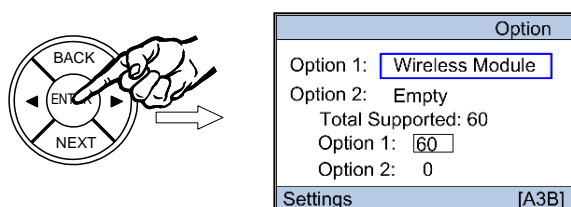
The Wireless network Settings screen is split over two pages, as indicated by the small arrow (↓) on the right side of the screen, so the **NEXT** and **BACK** buttons are used to jump between the two.

Once a setting box is highlighted, by using the left (◄) or right (▶) arrow key, press the **ENTER** key to make a change to the value. This will make the security screen appear for the PIN number entry.   The default value for the system security requires a PIN to be entered before any settings can be changed. This setting can be altered from the Security Setting menu.

The default PIN number is 0000. To enter a PIN, or accept the number, press **ENTER** and the first digit will flash. The value can be changed by using the left or right arrow keys (◄ or ▶). Once the number is correct, press **ENTER** once more. When all 4 digits of the PIN are entered correctly, select the OK button with the arrow keys (◄ or ▶).

	Wireless Network
Lowest FCU addr.:	1
Num of FCU:	60
PAN ID:	DA15
Data Retain:	No
Lowest FCU Addr.	[A3B1]

Press **ENTER** and the screen will return to the settings screen and the Lowest FCU addr. will be highlighted. Press **ENTER** once more to select this parameter and the current value begins to flash. Use the arrow keys (◄ or ►) to change the value shown until the desired figure appears, then press **ENTER** and the new value will be set. The arrow keys can be used to navigate to other settings, and the **NEXT** button goes to the second setting page and the Network Reset function.

❑ Set Lowest FCU addr. to the lowest address used for a Wireless field device. This will be where the addressing starts from.

❑ Set the Num of FCU to the actual number of Field units in the network. The field units will be numbered from the lowest FCU address contiguously for the Number for field units fitted.

❑ Set the PAN ID to a value different from the default. This should be noted as this needs to be set in all the individual field units.

❑ Data Retain set to 'Off' clears all the field unit data if communication is lost. Some host systems want the data to be retained, in which case set the parameter to 'On'.

❑ Set the AES key to something different from the default. This should be noted as this needs to be set in all the individual field units.

❑ The most suitable channel for the system will have been selected during the site survey. This setting should be set to that value.

❑ Set the number of P3W repeaters used in the system – P3W repeaters may be required in the system to ensure redundancy or for improved communications.

The network can be reset from the second page. This will need to be done if network changes have been made and these are required to be uploaded to all field units. Note that changes to network parameters will only be loaded to those devices currently communicating on the network.

When the settings are as required, use the **BACK** key to return to the top Settings menu.

	Settings
Option Module	[A3]
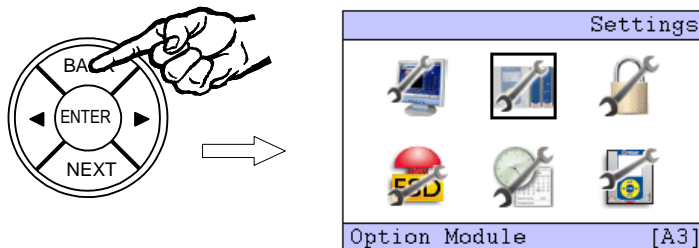
6.5 Setting the Master Host Communications Parameters

Select the Host icon using the arrow keys (◄ or ►) and press **ENTER**. The Host Settings menu choices screen appears.
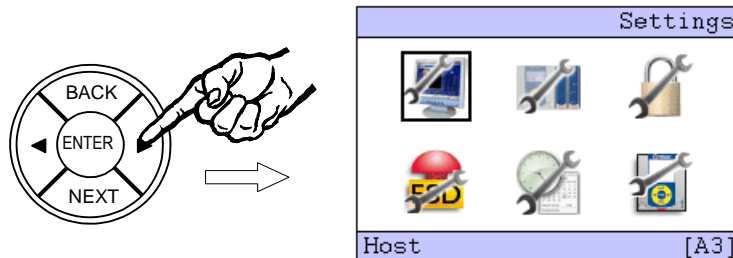
Select 'Ethernet Settings' using the arrow keys (◄ or ►) and press **Enter** once more. The Ethernet settings screen appears, note that there are two pages to the menu as indicated by the small arrow (↓) on the right side of the screen.
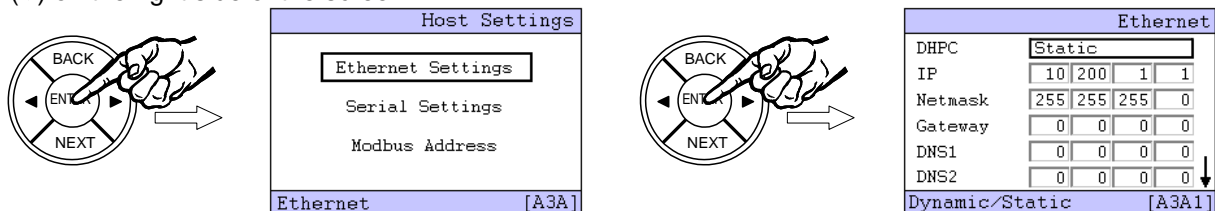
Use the **NEXT** button to move to the second page, the **BACK** button returns to the first page.
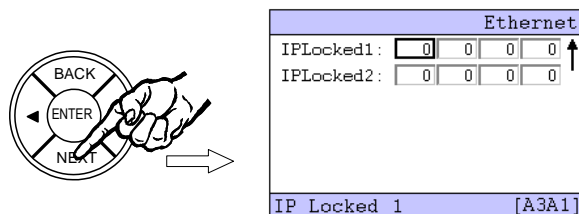
It is usually only necessary to change the IP address and Netmask to match the requirements of the network connected to the master station. When making any change it will be necessary to enter the PIN number for the master station as shown in the previous section.

To return to the previous Host Settings screen, press **BACK** and then select the Serial Settings using the arrow keys (◄ or ►) and press **ENTER**. The communications port speed (default 9600), and parity are changed here.
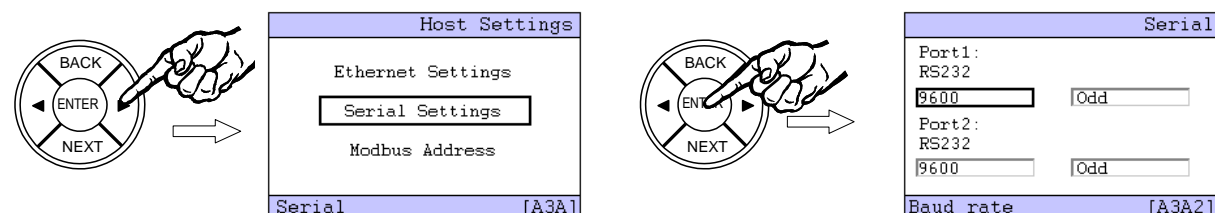
The port type is determined by the DIP switch settings on the main chassis behind the PS710 CPU module and the setting is reflected in the message on the screen. If the port is set to RS-485 and cross connected, the description changes to show these settings. This is particularly useful when determining the settings already in place. Select the option to be changed by using the arrow keys (◄ or ►), then **ENTER** (the PIN screen may appear before a change can be made). Once the PIN is entered, the value of the parameter can be altered by the arrow keys (◄ or ►). The speed can be varied from 2400 to 115,200 and the parity may be Odd, Even, Zero or None. Once the value is as required, press **ENTER** to set the value.

When the parameters are all as required, press **BACK** to return to the Host Settings screen, then select the Modbus Address using the arrow keys (◄ or ►) and press **ENTER**.
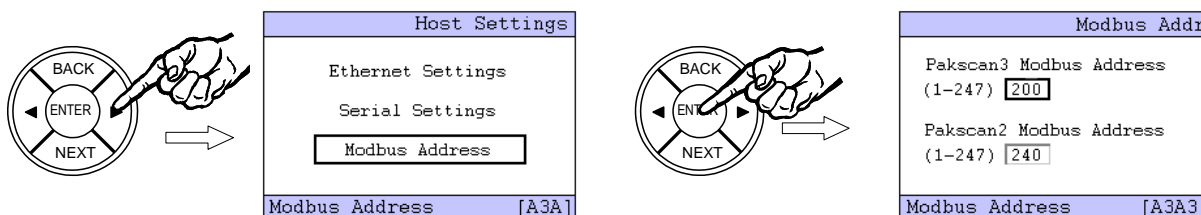
- ❑ The **Pakscan 3 Modbus address** is for accessing the **Wireless** database.
- ❑ The **Pakscan 2 Modbus address** is for accessing the **Wired** (current loop) database.
- ❑ *The Pakscan 2 and Pakscan 3 Modbus addresses MUST NOT be the same value*.

The Modbus address for the communication to the actuators on the Pakscan 2 current loop (via the module in option 2 slot) is altered in the lower window. It is recommended that this is altered to a value other than the generic Modbus default address of 247 and the master Station defaults to ensure that any new stations introduced do not conflict with this address.

Change this address for communication with the actuators connected to the current loop module

Do not change unless a Pakscan 3 option module is fitted
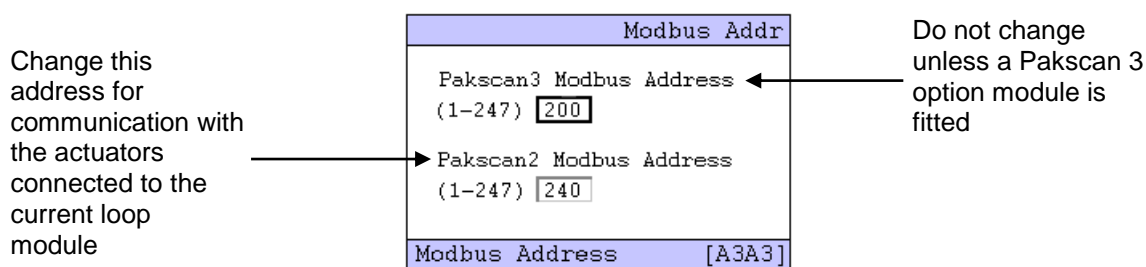
The address is changed by first selecting it with the arrow keys, then pressing **ENTER** (if the PIN requires entry the prompt page then appears). Use the arrow keys to change the number to the new value, and then press **ENTER** once more. The new address becomes active once the screen has been changed to a new one.

The Pakscan 3 wireless Modbus address is modified in the same way.

Once the settings are as required, use the **BACK** key to return to the top Settings menu.
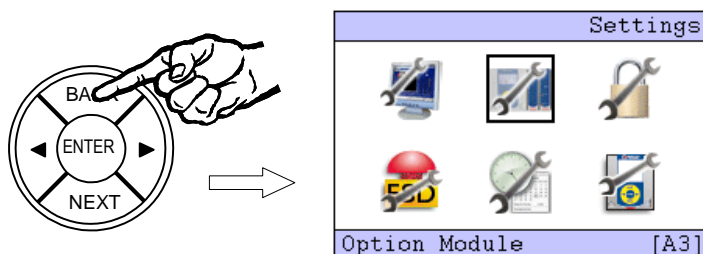
6.6 The Other Settings

There are menus for setting all the parameters of the system. These are more fully explained in the system manual and, in general, the default settings will allow most systems to operate with reasonable success.

6.6.1 Security

Security is used for setting the PIN number to be used, plus the actions permitted from the keypad and the serial ports via the Interlocks. The Security setting default requires a PIN for adjusting the settings for system performance, but not for issuing actuator commands.

Interlocking controls the serial communications that are permitted to operate the actuators. The default grants permission to all the serial ports and the Ethernet ports, but prevents the web page facility from moving the valves.

❑ The default PIN = 0000.

6.6.2 ESD

The default condition is to disable all the possible Emergency Shut Down routes. ESD can be enabled from the serial ports, Ethernet ports, Web page, hard-wired input or keypad on an individual actuator selection basis. If this ESD function is not required, ensure that a shorting link is fitted across pins 4 and 5 of the PS710 CPU module connector.

6.6.3 Date and Time

The date and time, plus the use of an NTP server are set from this menu. The time stamp is used for the logging facility.

6.6.4 Master Station Parameters

The master station parameters include the Tag for the master station and the setting for data transferred between the two CPU modules on a hot standby system along with several other parameters. Most of the default settings are suitable on most systems, though there is one particular set of parameters that must be correctly set in the case of hot standby systems.

```
                              M/S Settings
              ┌─────────────────────────┐
              │    Changeover Master     │          ↑
              └─────────────────────────┘
          Serial Port1: Passive
          Serial Port2: Active
          Ethernet      Active                       ↓
          Port1 Standby              [A3F]
```

The Serial Ports should appear as Passive if the Cross Connect DIP switch is set to 'cross connect'. If the port is set to RS-485 highway and is being used on a multi-drop highway it must be set to passive. If it is not shown correctly it probably means the DIP switch is incorrectly set.

Remember, the default setting is Standby Active.

7.   INTERNAL WEB PAGES

The master station includes a set of web pages that may be remotely accessed via Ethernet. They can be used for setting up the system, examining the system for any faults or alarms and also for controlling the actuators on the network (provided the Interlock permission is set to allow this feature).

If the master station is connected to an Ethernet Network it will act as a web server and any computer within that network can connect to the master station. The master station can also be configured and the field network set up by using these web pages. The host system or computer connected via the Ethernet Network or directly will need a web browser such as Internet Explorer to access the master station web pages.

7.1 Making an Internet / Intranet Connection

Connect the master station to an Ethernet host as described in section 5, or connect via a suitable router to the internet / intranet. A computer can be connected directly to the master station using the configuration port.

Start the browser and enter the IP address of the master station. The default address is 10.200.1.1, so the address is **http://10.200.1.1**. The browser will then access the master station and bring up the opening page of the master station. In order to log in as a verified user, enter a user name of **admin** and a password of **admin**. (The default password should be altered as soon as convenient to prevent unauthorised access to the system.)

Default IP address	10 . 200 . 1 . 1
Default User	admin
Default Password	admin

Once entry to the web pages has been made, if no changes to the display or information is made for a few minutes, the system will automatically log out and the user/password must be re-entered.

7.2 Connecting a Computer Directly to the Master Station

The simplest direct connection to the master station is by using the Ethernet port on the front of the CPU module. A standard Ethernet patch cable or crossover cable can be used to link the two directly. A permanent connection can also be made directly to one of the underside connectors (port 3 or 4). In order to establish a connection it is probably necessary to adjust the settings of the computer's Internet connection.
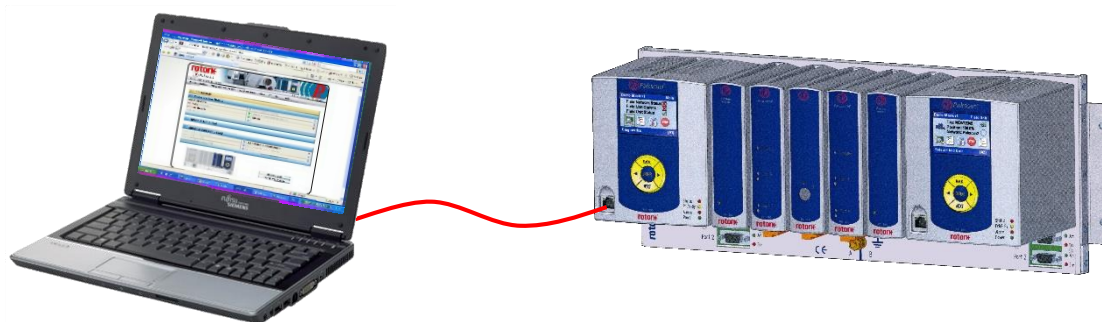
Fig 33:   Connecting a Laptop to the Pakscan P3 Main Module

7.3 Adjusting the Network Settings of the Computer

❑ Ensure that nothing is connected to the Ethernet port of the computer.

❑ Open the Control Panel and select Network Connections (XP) or Network and Sharing Centre (Windows 7).

❑ Select Change Adaptor settings (Windows 7 only).

❑ In the 'Network Connections' window, double-click on the appropriate 'LAN or High Speed Internet' icon and the 'Local Area Connection Status' window will open.

❑ Click on the 'Properties' button, and a second window will open. Select 'Internet Protocol TCP/IP' ('Internet Protocol Version 4 (TCP/IPv4)' for Windows 7) and click on the 'Properties' button in this window.

❑ The 'Internet Protocol TCP/IP Properties' window will open. Next, change the setting to force the computer to adopt a fixed IP address and enter an address of 10.200.1.3 and a subnet mask of 255.255.255.0. Click on the 'OK' button and the window will close.
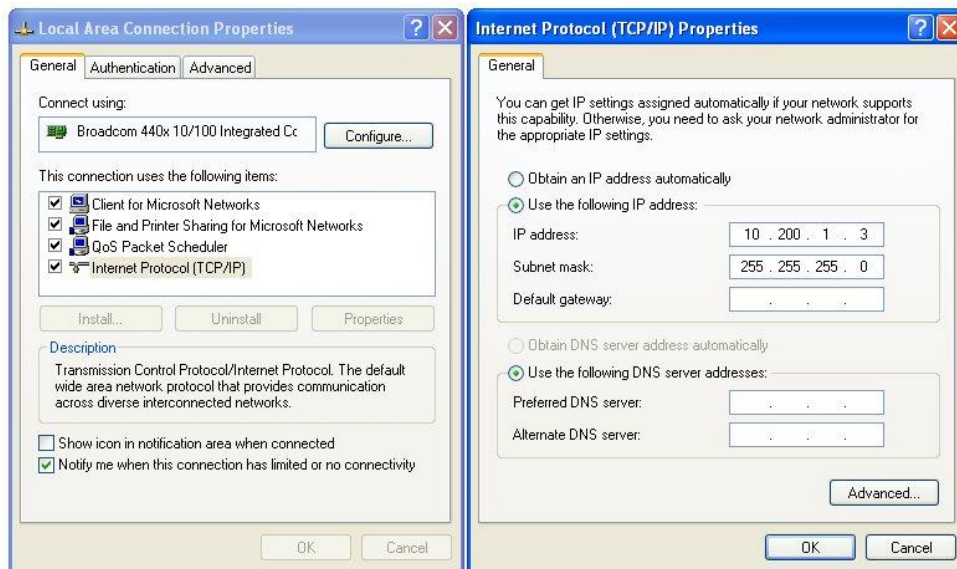
Fig 34:   Changing the Network Connections TCP/IP Properties – Windows XP

❑ Click OK on the 'Local Area Connection Properties' window and then close the status window.

❑ Finally, close the 'Network Connections' window and the Control Panel.

❑ It may be necessary to reboot the computer to be sure that the new settings take effect correctly.

❑ Connect the cable between the computer and the Pakscan master station.

❑ Start the browser and enter the IP address of the master station. The default address is 10.200.1.1, so set the address to **http://10.200.1.1**. The browser will then access the master station and bring up the opening page of the master station. In order to log in as a verified user, enter the username of **admin** and the password **admin**.

Note: If the IP address of the master station has been changed from the defaults, then the settings above will not work and will have to be modified to suit the actual settings.

7.4 Web Page Structure

The web pages have three access levels, each requiring a password with the correct level set. A user enters the web server with a particular degree of access to the functions of the server and the master station.

7.4.1   User Levels

Access Level		Function
Lowest level	Read	Allows access to read master station status and settings, plus the option module status and settings, plus the actuator and field unit status on the option module network. No commands or alterations to the system are permitted.
	Write	As for read access with the addition of the ability to issue network commands, swap masters and command actuators on the option module network to change position.
Highest Level	Administrator	As for the two lower levels plus the ability to configure the master station, option modules and all system settings. Set and remove user names and passwords; set alarm reporting parameters, change system addresses and test system communications.

The Administrator level sets all other user names and passwords. As soon as the system is set up the default password should be changed. Make sure all changes made to log in details are recorded.

7.4.2   Overview of Web Page Layout

The web pages are organised using a menu structure with the primary menu on the top of each page. Within a page there are other controls for parameter alteration or to reveal extended information on the topic of the particular page.

Navigation between the pages is by selecting another topic on the main menu.

If there is no activity with the mouse to change the display or update the information or selection for a few minutes, the system automatically logs out the user. The username and password must be re-entered to continue using the pages.
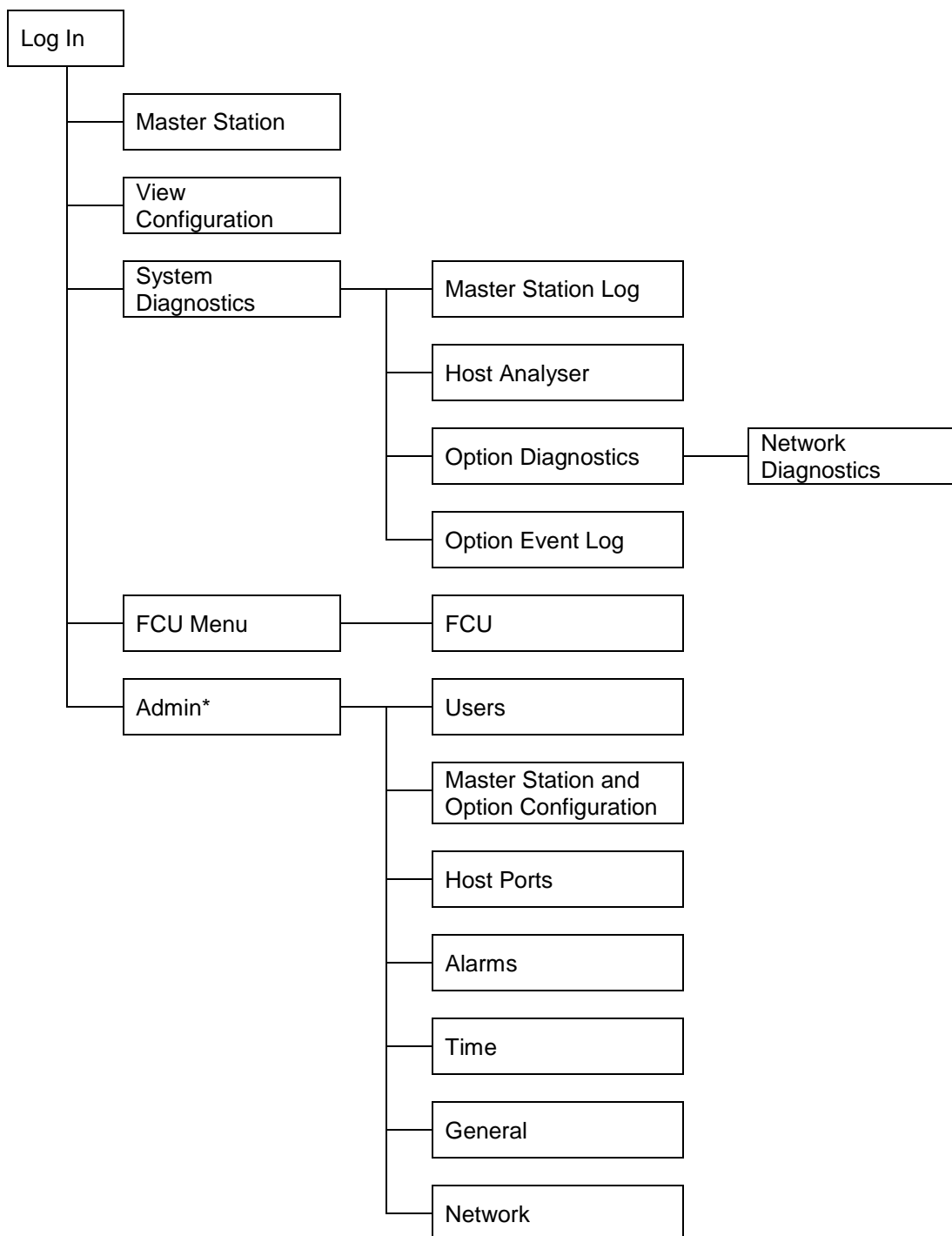
* requires Admin level log in
Fig 35:   Web Page Menu Layout

7.5 The Web Pages in Detail

7.5.1   Log In Screen

Fig 36:   Web page Log In Screen

The first screen is the Log In screen on which the user must enter a **Username** and **Password***.*

❑ **Username** - a <u>case sensitive</u> identification for an individual or group used to give access to the system. User names are listed for administrators to see on the 'Add User' page.

❑ **Password** - the <u>case sensitive</u> confirmation required before a username is accepted by the system. Passwords are not listed on any page in the system and cannot be retrieved, even at the administrator level.

Select the box with the mouse and enter the appropriate name or password, then click on the **login** button. The system will move to the next page if the login is accepted. If it fails, the data is cleared from the boxes and must be re-entered correctly in both boxes before access is granted.

The default user name is **admin** and default password is **admin**. The password should be altered as soon as convenient to prevent unauthorised access to the system.

User name and access level.

Menu of available screens to visit (changes to blue when selected) for Read and Write access levels

Log out when finished by clicking here (changes to red when selected).
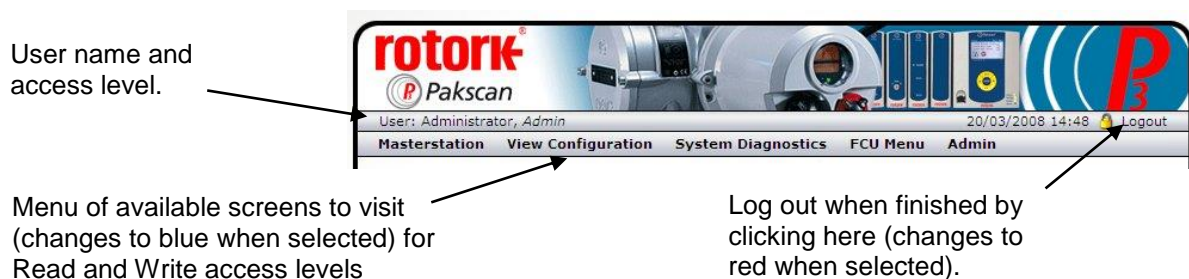
Fig 37:   Web page Header Navigation

7.5.2   Master Station

Fig 38:   *Master Station Overview web page and Option 1 data, if a Wireless module is fitted*

This screen is accessible to Read, Write and Administrator user levels.

This screen reports the current status of the master station and the option modules fitted. The picture shows the master station, single or hot standby version. The green, orange and red lights show the condition of the associated parameter. Greyed out text and lights are not applicable or else in a safe (normal) condition.

Master station CPU Module

Site name   : The name of the site where the system is located, as entered during
                     configuration.

Tag name   : The master station tag, as entered during configuration.

Status

Location A/B   : Indicates the CPU module currently in communication over the Ethernet.

Primary/Standby	: Shows the condition of the CPU with regard to controlling the option modules. The Primary CPU is in control. A Standby CPU is prepared to become the Primary and take control if the partner unit fails.
Module Health	: Indicates the absence (green light) or presence (red light) of a fault on the CPU.
ESD Presence	: Shows a yellow light if an Emergency Shut Down signal is active.
Redundancy Option	: Shows a green light if there is a partner module fitted.
Other Master Station health	: Indicates the absence (green light) or presence (red light) of a fault on the partner CPU.
Alarm	: Indicates the presence of an alarm (red light) somewhere on the system.

Option 1 and Option 2 - Show the type of Option module fitted, either:

Pakscan 2 Loop Option Module

Loopback in Progress	: A blue light shows whilst the master station is reconfiguring the loop.
Loopback in Use	: A yellow light shows when the master station has detected a loopback fault on the system.
Auto Loopback occurred	: If a fault occurs on the network and an automatic reconfiguration of the loop occurs, then a yellow light is shown here.
Common Field Unit Alarm	: A red light shows if any field unit on the network has an alarm bit present.
Common Actuator Alarm	: A red light shows if any actuator on the network is unavailable due to its monitor relay having tripped.
ESD Active	: If there is an Emergency Shut Down signal present on the system a red light shows.

Pakscan 3 Wireless Option Module

Configuration in Progress	: A blue light shows whilst the master station is reconfiguring the network.
Network Healthy	: A Green light shows when the master station has detected **NO** faults in the network and it is healthy.
Field Unit Alarm	: A Red light shows when the master station has detected an alarm on any of the field units.
Field unit Comms fail	: A Red light shows when the master station has detected a communications failure to a field unit.
ESD Active	: If there is any Emergency Shut Down signal present for that network on the system a red light shows.

Controls - Not Available for Read level users

Network ESD	: Click here to issue an ESD to all actuators connected to both option modules. The resulting action will depend on the individual actuator settings. A confirmation screen appears to verify or cancel the instruction before the action occurs.
Changeover Master	: Only applicable to hot standby systems. Click this button to make the master station CPU in control; change from A to B or B to A.

7.5.3 View Configuration

Fig 39: *System Configuration Overview web page*

> This screen is accessible to Read, Write and Administrator user levels.

The screen shows the settings for the control of the option module networks and the CPU control capability, software fitted and various options selected. All of these settings can be modified elsewhere, but only by users with Administrator level access. There are no controls on this page.

The settings are explained in the Master Station Configuration page section.

7.5.4 System Diagnostics
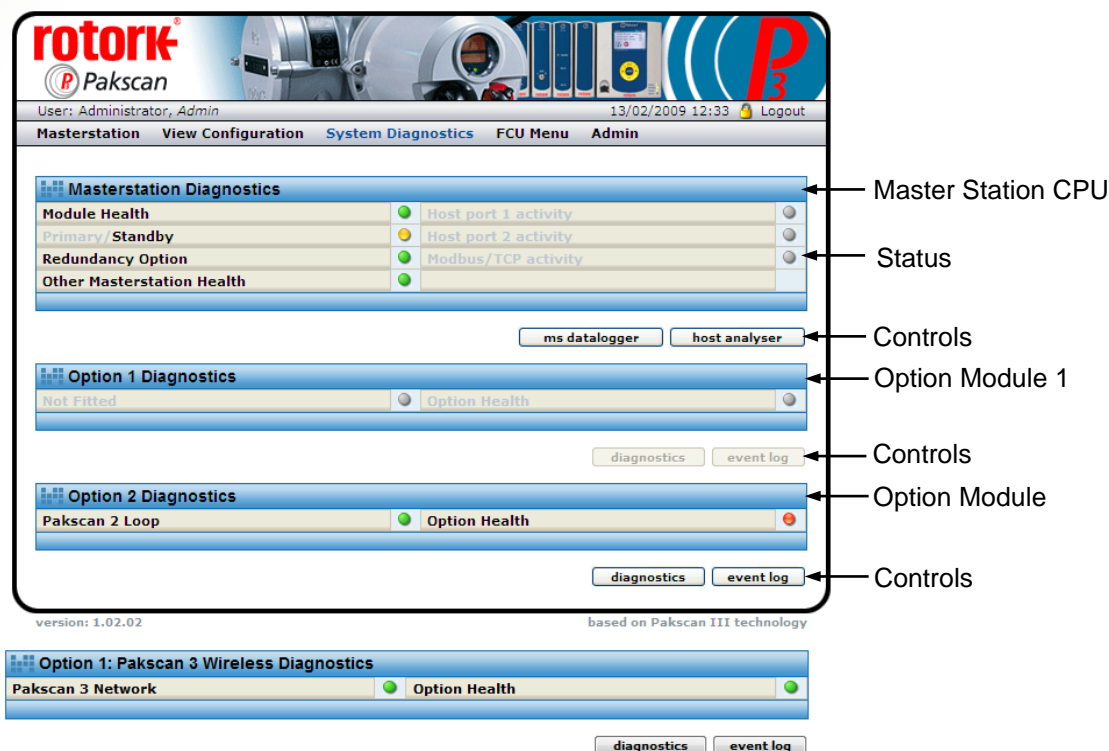
Fig 40: System Diagnostics web page wired only and option 1 data, if wireless fitted

> This screen is accessible to Read, Write and Administrator user levels.

The System Diagnostics screen shows an overview of the status of the fitted modules and also provides access to further information.

Master Station Diagnostics

Module Health	:	A green light shows if the module is operating correctly, changes to red if there is a fault.
Primary/Standby	:	Indicates which module is being accessed. A green light indicates Primary, a yellow light indicates Standby and a red light indicates a fault.
Redundancy Option	:	Shows a green light if there is a partner module fitted.
Other Master Station Health	:	Indicates the absence (green light) or presence (red light) of a fault on the partner CPU.
Host port 1 activity	:	Indicates when there is serial communication taking place on communications port 1.
Host port 2 activity	:	Indicates when there is serial communication taking place on communications port 2.
Modbus/TCP activity	:	Indicates when Ethernet control using Modbus/TCP is present on either Ethernet port.

Controls - Available to all user levels

ms datalogger	:	Reveals a pop-up showing a log of the activity on the master station and the source of requests or commands received. See section 7.5.5 for details.
host analyser	:	Reveals a pop-up with the data logger data and the additional controls required for using the inbuilt data analyser for commands and data sent to the host system. See section 7.5.6.

Option 1 Diagnostics

Pakscan wireless network	:	Shows module type and status, or 'Not Fitted' when there is nothing in the slot.
Option Health	:	Shows a green light when healthy and a red light if there is a fault on the module.

Option 2 Diagnostics

Pakscan 2 Loop	:	Shows module type and status, or 'Not Fitted' when there is nothing in the slot.
Option Health	:	Shows a green light when healthy and a red light if there is a fault on the module.

Controls - Available (when module fitted) to all user levels

diagnostics	:	Reveals the diagnostic page for the option module fitted. See section 7.5.7 Pakscan 2 Loop and section 7.5.8 Pakscan Wireless.
event log	:	Shows the option module event recorder. See section 7.5.9 Pakscan 2 Loop and section 7.5.10 Pakscan Wireless.

7.5.5 Master Station Data Logger [ms datalogger]
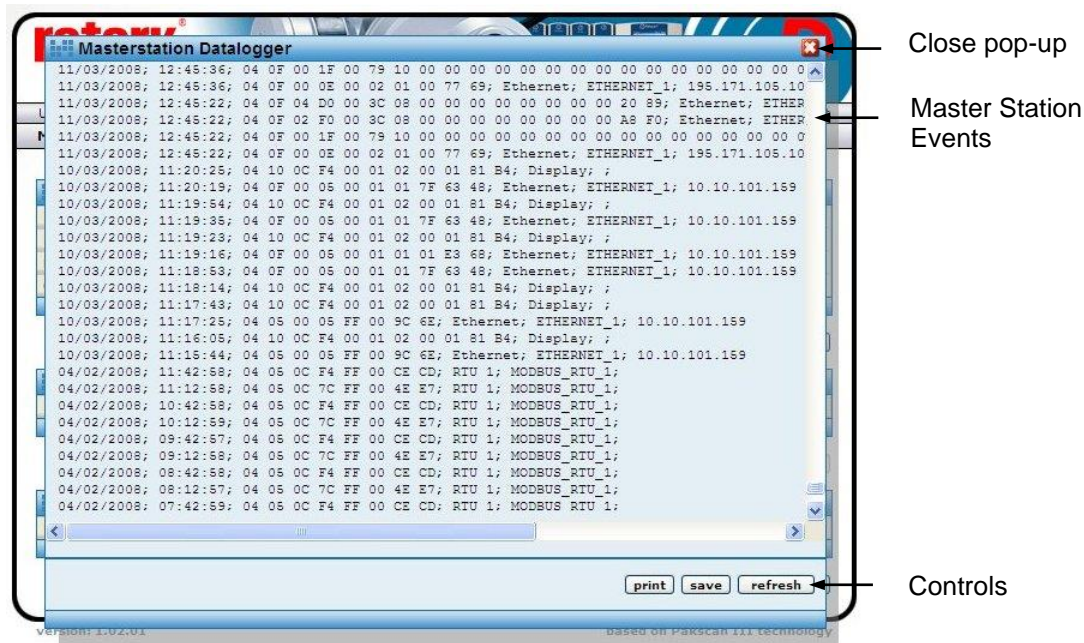
Fig 41:   *Master Station Data Logger pop-up*

This screen is accessible to Read, Write and Administrator user levels.

The data logger displays Modbus instructions received by the master station to carry out commands such Alarm Accept or commands to move a valve. Each event is prefixed by a date and time and they are listed in time order. They are followed by the source from which the command originated. Once full the log rolls over and rewrites over the oldest events, the log is 1Mbyte in size.

Date and Time	Modbus Message	Message Source / Address

```
10/03/2008; 11:16:05; 04 10 0C F4 00 01 02 00 01 81 B4; Display; ;
10/03/2008; 11:15:44; 04 05 00 05 FF 00 9C 6E; Ethernet; ETHERNET_1; 10.10.101.159
04/02/2008; 11:42:58; 04 05 0C F4 FF 00 CE CD; RTU 1; MODBUS_RTU_1;
```

Fig 42:   *Close up of Master Station Data Logger Information*

Date and Time
    Formatted Day/Month/Year or Month / Day / Year.

Modbus Message
    Standard Modbus RTU format for all 'write' messages.

Message Source and Address
    Display   : Keypad on the master station CPU.
    Ethernet   : Ethernet input and IP address of the source.
    RTU   : Serial port 1 (RTU 1) or serial port 2 (RTU 2).
    Webpages   : Web page Log In name and IP address.

Controls - Available to all user levels

Print   : Prints the logger data to a printer attached to the computer.

Save   : Saves the logger data to a file on the computer.
               The saved file is of the type cmdlog.log and can be opened in the Notepad
               on the computer. It can also be imported into a spreadsheet, such as
               Excel, for analysis as required.

Refresh   : Updates the screen with any new data.
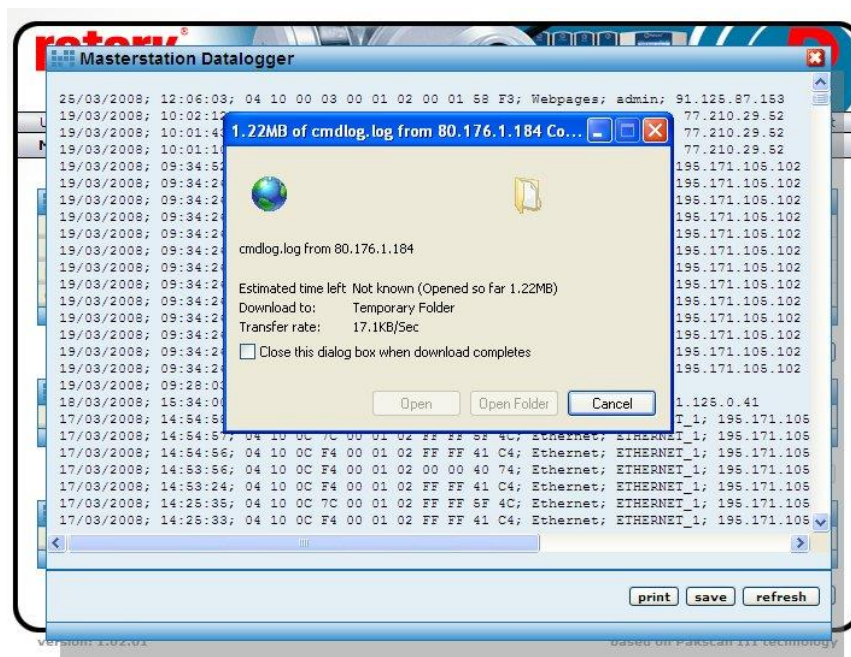
Fig 43: Saving the master station log file

7.5.6   Master Station Host Analyser [host analyser]
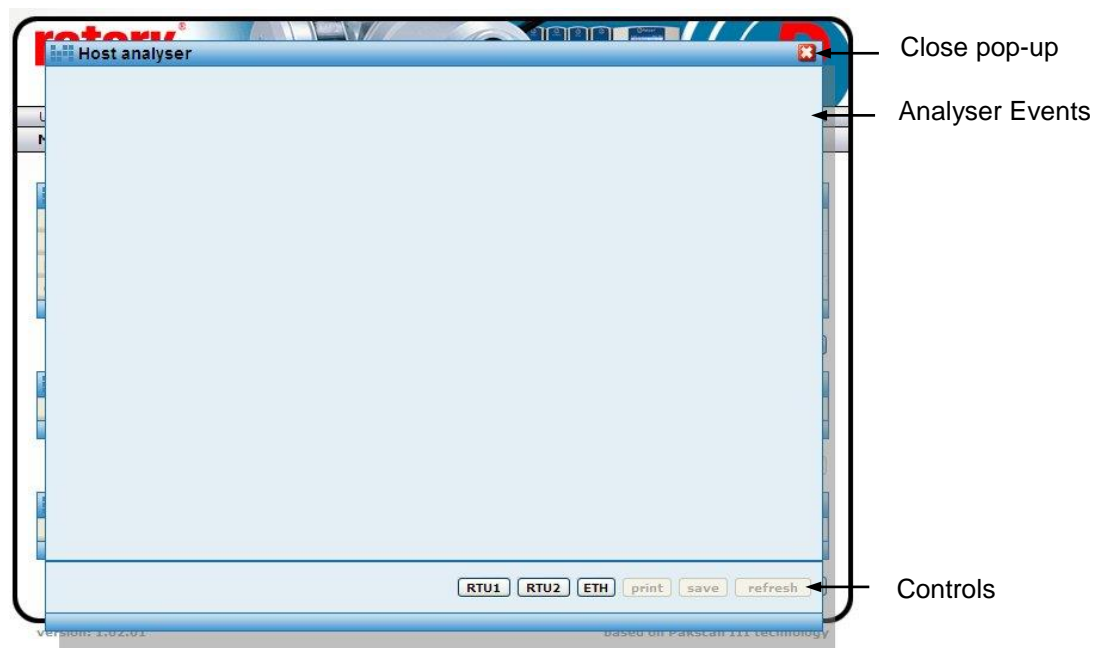
Fig 44:   Host Analyser pop-up

This screen may be used by Administrator user level only.

The Host Analyser is a real time system analyser that can be used with either a Modbus RTU serial data control source, acting through one of the serial data ports (Port 1 or 2), or a Modbus TCP Ethernet control source, acting through the Ethernet ports.

The analyser will record up to 100 messages (requests and responses) on the data line between the two points. It is especially useful for debugging a host control system to ensure that messages are correctly formatted and that the required control or data points are being accessed. In particular, the use of correct offsets in the Modbus protocol can be checked.

Controls - Available to Administrator user level

RTU1	:	Selects Serial Port 1 host input.
RTU2	:	Selects Serial Port 2 host input.
ETH	:	Selects the Ethernet port host input (all Ethernet ports are monitored).
Print	:	Prints the analyser data to a printer attached to the computer.
Save	:	Saves the analyser data to a file on the computer.
Refresh	:	Updates the screen with any new data.

7.5.7 Pakscan 2 Loop Diagnostics [diagnostics]

Fig 45: Pakscan 2 Loop Diagnostics web page

This screen is accessible to Read, Write and Administrator user levels.

The Pakscan 2 Loop Diagnostics screen gives diagnostic information on the 2-wire loop option module and the network connected to it. The top part of the screen shows the information about the option module itself, whilst the lower part shows the loop map. This is the order in which the field units on the 2-wire loop are connected. It also shows the device type and tag name for each address and position.

Network Diagnostics

No. Of Devices On Network
: This is the number of field units that are expected to be located on the network. It is the highest address that the network will scan up to when locating field units. All field units need to be consecutively addressed, and there should be no gaps in the addresses.

No. Of FCUs Found
: This is the total number of field units located on the network. If all the field units are powered on and connected, then the number will equal the No. Of Devices On The Network above.

Configuration Status
: This field shows any fault that exists on the network cabling and the stages passed through as network configuration takes place.

During configuration the following sequence can be displayed -
1. Wait for Loopbacks 1   (first wait for loopbacks to come on)
2. Find FCUs on Port A   (finding FCUs on port A)
3. Test Loop   (testing for complete loop)
4. Find FCUs on Port B   (finding FCUs on port B)
5. Wait for Loopbacks 2   (second wait for loopbacks to come on)
6. Loopbacks off on A   (removing loopbacks from port A)
7. Loopbacks off on B   (removing loopbacks from port B)

(The normal sequence for a fault-free loop would be 1, 2 and 3. A sequence for a break in the loop, anywhere except at port A or port B, would be 1 to 7. Some of the phases may be very quick, particularly at higher baud rates, and so may not be seen on the browser display.

Whilst the configuration is taking place, the master station web page shows 'Loopback in Progress' and a blue light on the Option module.

If the configuration process detects a fault on the loop and switches on the loopback circuits of two field units, the master station web page shows 'Loopback in Use' and illuminates the yellow light.

Last Network Reset Initiated By
: The loop can be reconfigured for a number of reasons and this field will show the cause of the last reset/reconfigure that occurred.
The possible reasons are:

Power on Reset - loop configured because the master station powered up.

Fault Found - fault detected on the loop whilst it was running without loopbacks present.

Fault Found A - fault detected on the A side of broken loop whilst running with loopbacks on.

Fault Found B - fault detected on the B side of broken loop whilst running with loopbacks on.

Reset Command - loop Reconfigure command entered from keypad or serial port.

Return wire fault - fault detected in the return current path whilst the loop was running at double speed.

Doubling failed - fault detected after loop assumed double speed.

Network Fault Type : This field shows the type of fault detected that caused the loopback to occur, or an addressing fault on the field units. The types are:

Zero Address	- a field unit has been found with an address of zero.
Address too High xx	- a field unit has been found with an address higher than that set up within the master station; xx is the address.
Same Address xx	- two field units found with the same address; xx is the address.
Loop Open Circuit	- an open-circuit fault found on the loop.
Loop Short Circuit	- a short-circuit fault found on the loop.

If two field units are found with the same address, or there is an address outside the range of addresses expected (as set by No. of Devices on Network), the network will continue to operate and miss out the faulty field units.

Loop Baud Rate : Shows the current speed selected. The speed can be 110, 300, 600, 1200, or 2400 baud.

No. Of FCUs On Side A : This is the total number of field units connected to the option module Port A and communicating via Port A.

No. Of FCUs On Side B : This is the total number of field units connected to the option module Port B and communicating via Port B. Port B is only used if there is a loopback present on the network.

Controls - Available to all user levels

Reset network : Causes the option module to reconfigure the 2-wire network. This should be used after a loop fault has been corrected.

Network Map

The map shows the order in which the field units have been identified and found by the option module during the last loop reconfiguration process (reset). Each time the loop is reconfigured the map is regenerated and repopulated. Any field unit that is not powered-up at the time of reconfiguration will be absent from the map.

Position : The position in the loop. Number 1 is nearest to Port A.

Address : The address of the field unit.

Failures : Shows a count of communication errors with the field unit. The count has a range of 0 to 255, after which it rolls around to zero and it increments for every communication error. The system will only announce a 'Comms failure' when 3 successive tries have failed to locate the field unit. This counter therefore reflects the communications condition and can be used as an indicator of the health of the field unit to assess the probability of failure in the future.

Type : The type of field unit depends on the actuator and function required.
Current types are -

IQ - IQ or IQT actuator
Integral - Non IQ actuator
Flowpak - Flowpak actuator
GPFCU - GP - General Purpose Field Unit
GPFCU - Act - General Purpose in Actuator mode
IQA - IQ Analogue card
ROMpak - ROMpak actuator

Tag Name : The associated identification Tag assigned to this field unit.

7.5.8   Pakscan Wireless Diagnostics [diagnostics]
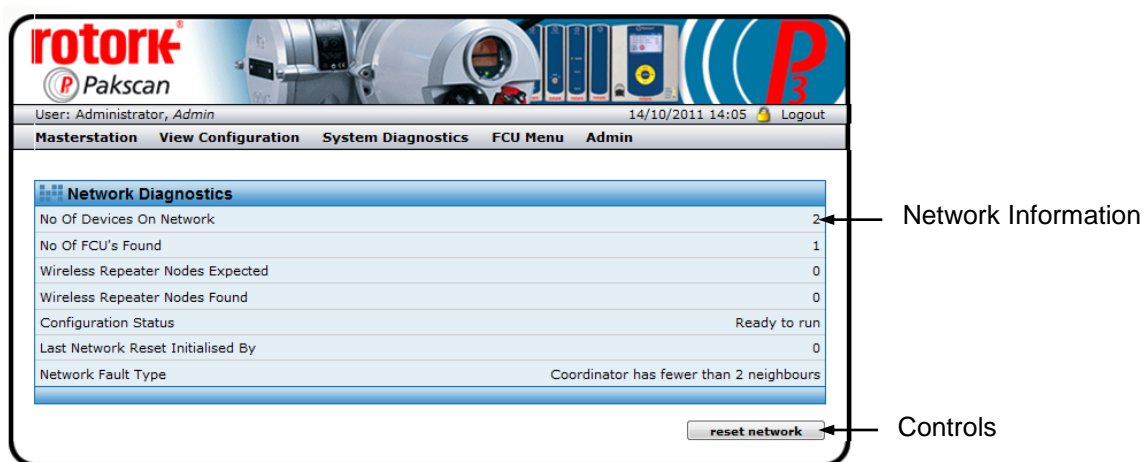
Fig 46:   Pakscan Wireless Diagnostics web page

This screen is accessible to Read, Write and Administrator user levels.

The Pakscan Wireless Diagnostics screen gives diagnostic information on the wireless option module and the network connected to it.

No of Devices
On Network
: This is the number of wireless field units that are expected to be located on the network. This is set up in the master station configuration web page.

No of FCUs
found
: This is the total number of field units found on the network. If all the field
units are powered on and able to communicate, the number will equal the number expected on the network.

Wireless
repeater nodes
expected
: This is the number of P3W repeater modules that are expected to be located on the network. This is set up in the master station configuration web page.

Wireless repeater nodes found	:	This is the total number of P3W repeater nodes found on the network. If all the P3W repeater nodes are powered on and able to communicate, the number will equal the number expected on the network.
Configuration Status	:	During configuration of the wireless network the network goes through various stages as indicated below. Some of the stages can be quite quick and therefore may not be seen:

- Uninitialised.
- Initialised / starting up.
- Detecting field units.
- Building map of field units.
- Detecting field units complete.
- Obtaining initial field unit data.
- Field unit data collection complete.
- Network Ready to run.
- Master station updating RF parameters.

After a reset network command is sent from the web page, the normal sequence seen would be: Initialised / starting up, Detecting Complete, Obtaining initial Data, Data collection complete, Ready to run.

'Ready to run' is the normal state of a good network.

Last Network Reset Initialised By	:	This field indicates the cause of the last reset, this can either be due to a power cycle (value will be 00), as a result of receiving a reset network command, due to a parameter change causing the P3W coordinator to reset or due to a Radio communications parameter change.
Network Fault Type	:	This field indicates any faults on the network. Faults reported can be:

- P3W coordinator fault.
- Insufficient wireless neighbours for the P3W coordinator or the field units, the intention is always to have at least 2 neighbours.
- RF parameter change failed.
- Duplicate field unit address detected.

7.5.9   Pakscan 2 Loop Option Module Event Logger [Event Log]
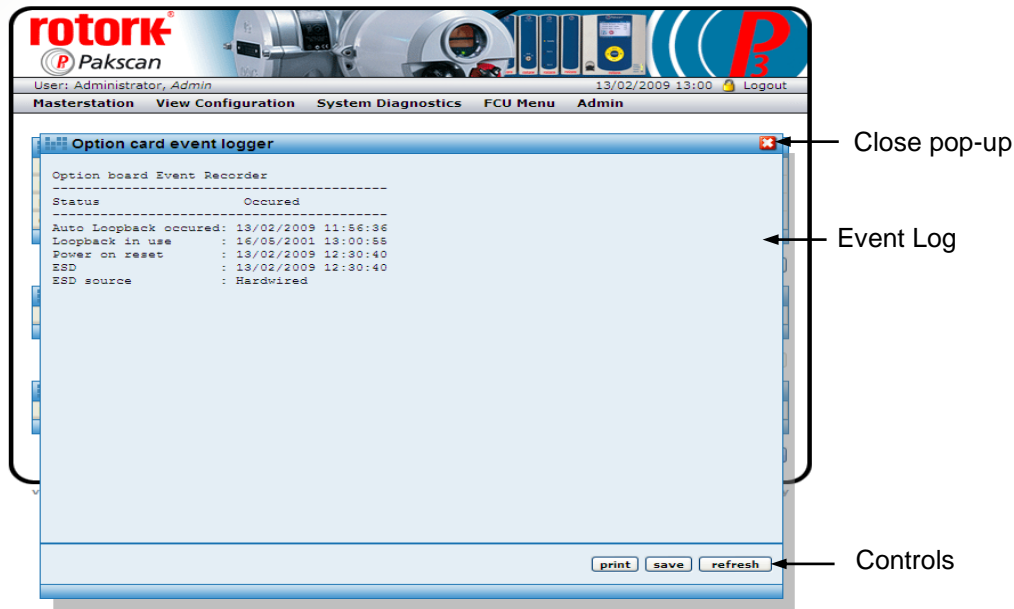
Fig 47:   Wired Option Module Event Logger pop-up

This screen is accessible to Read, Write and Administrator user levels.

The event logger shows the last occurrence of the listed events and, in the case of an ESD, where the signal originated.

Controls - Available to all user levels

Print   : Prints the logger data to a printer attached to the computer.

Save   : Saves the logger data to a file on the computer.

Refresh   : Updates the screen with any new data.

7.5.10 Pakscan Wireless Option Module Event Logger [Event Log]
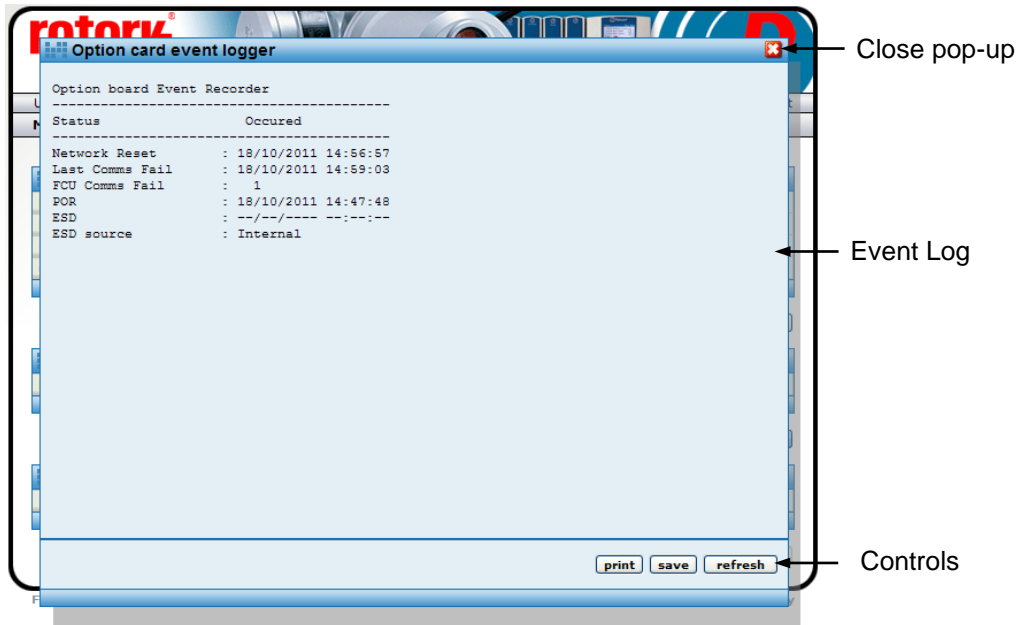
Fig 48:   *Wireless Option Module Event Logger pop-up*

This screen is accessible to Read, Write and Administrator user levels.

The event logger shows the last occurrence of the listed events. In the case of an ESD, where the ESD signal originated is reported. In the case of the last field unit comms fail, it also indicates which field unit lost communications.

Controls - Available to all user levels

      Print   : Prints the logger data to a printer attached to the computer.
      Save   : Saves the logger data to a file on the computer.
      Refresh   : Updates the screen with any new data.

7.5.11   FCU Menu

Fig 49:   FCU Menu web page

This screen is accessible to Read, Write and Administrator user levels.

The FCU Menu lists all the field units in address order (which may not be the same as the order in which they are connected together on the wired loop).

For each address, the Tag name and Type of field unit is listed. Field unit types are described in section 7.5.7. The Network column shows which option module network each actuator is connected to; this will be Pakscan 2 for the 2-wire loop option module and Wireless for the wireless option.

The next two columns show critical alarm conditions that will prevent remote control of the actuator. An Alarm present will generally prevent operation, whilst Comms Fail indicates that the actuator is no longer in communication with the field network.

The final column has Navigation controls to the individual FCU screens.

Controls - Available to all user levels

FCU Control   : Click here to show the selected FCU individual control panel web page. The different types of devices each have different screens and only the relevant data and controls for each type are included on the screen, together with a picture identifying the type of device.

When not in communication the screen may still be visited, but the actuator picture will have a large red cross over it to show that a problem exists.

7.5.12   FCU Control – IQ / IQT Actuator
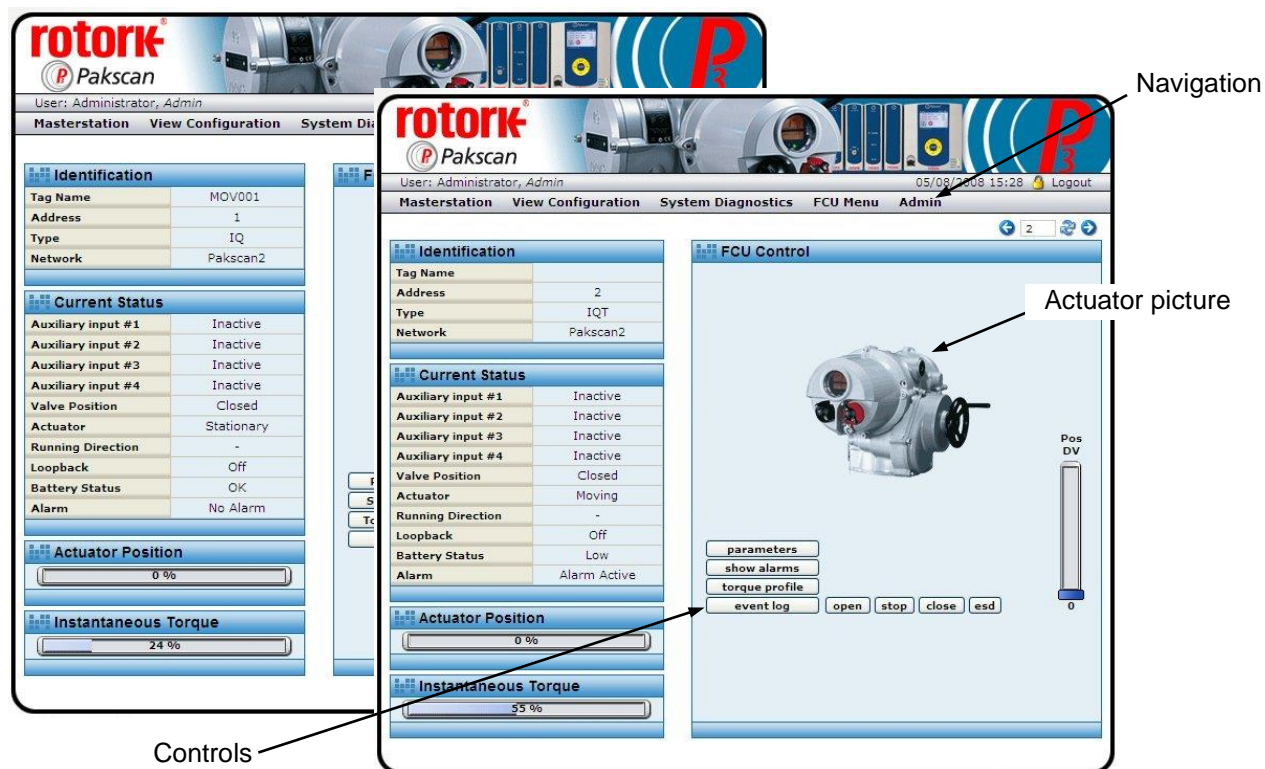
Fig 50:   *IQ and IQT actuator FCU Control web pages*

This screen is accessible to Read, Write and Administrator user levels.

The IQ and IQT control screens are similar and show a picture to identify the actual type of actuator at this FCU address.

The FCU Control screen shows a control and status page for the selected field unit and actuator. The screen has information relating to the device, its current condition and system parameters. It also includes the ability to change the actuator's position by means of the control buttons. When not in communication the screen may still be visited, but the picture has a large red cross over it to show a lack of communication.

Navigation

Navigation between the field units is either by returning to the previous screen, or by using the navigation buttons on this screen. Entering an address directly in the 'Address' box and clicking Refresh moves directly to the selected field unit.

Identification

Tag name : Identification tag given for this device.

Address : Network address.

Type : Shows the identified actuator type as IQ or IQT.

Network : The network to which this device is connected (Pakscan 2 for 2-wire loop).

Current Status

The real-time status of the actuator is listed in this pane on the screen:

Auxiliary Input : Active or Inactive, shows the status of the input.
1 to 4

Valve Position : Current position, Closed, Open or Stopped Mid Position.

Actuator : Moving or Stationary.

Running direction : Opening or Closing.

Loopback : Off or On.

Battery Status : OK or Low.

Alarm Status : No Alarm or Alarm.

Actuator Position

A bar graph shows the current actuator analogue position between 0 (closed) and 100% (open).

Instantaneous Torque

A bar graph shows the current torque value between 0 and 120% of actuator rated torque.

FCU Control web page Controls

Parameters (2-wire loop Field unit) - Available to all user levels
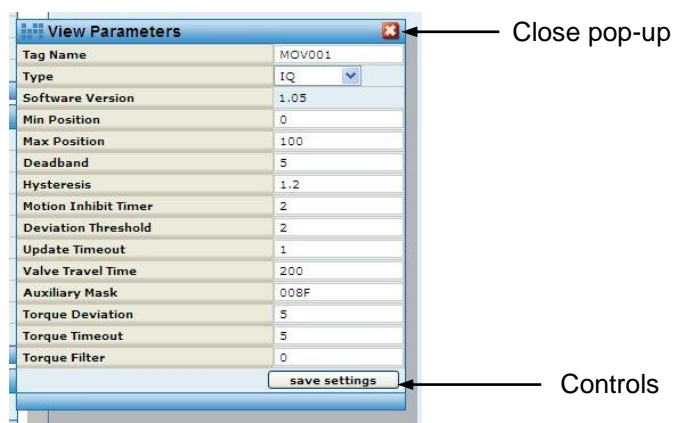
Fig 51:   Wired IQ / IQT Parameters pop-up

Pop-up screen shows the settings for all the parameters relating to the IQ / IQT actuator field unit. For users with Administrator level rights, the values can be edited and, for later version field units, the type of actuator can be modified. The parameters are used to determine the way in which the actuator responds to commands and reports data. Information on how to set

these fields is contained in the actuator field unit manuals. This screen is used for changing the Tag Name.

Controls

Save Settings   : Edited fields may be saved to the FCU; accessible by **Administrator** level users only.

Show Alarms (2-wire loop Field unit) - Available to all user levels
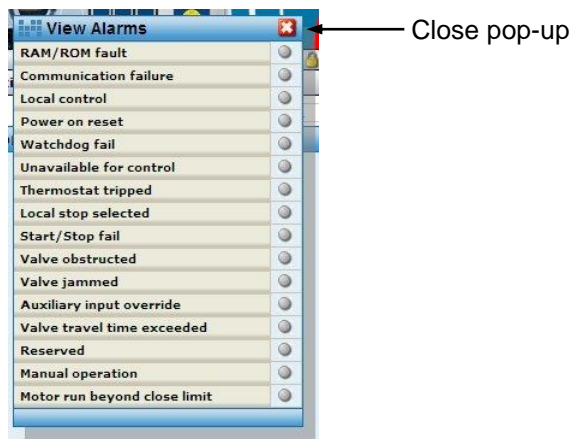
Fig 52:   *Wired IQ / IQT Alarms pop-up*

Pop-up screen shows the alarms on the actuator as red lights; grey is no alarm. Additional information on the meaning of these alarms is contained in the individual field unit manuals.

Torque Profile (2-wire loop and Wireless Field unit) - Available to all user levels
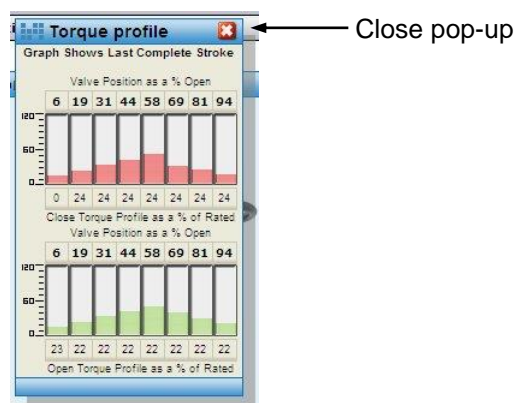
Fig 53:   *Wired and Wireless IQ / IQT Torque Profile pop-up*

Pop-up screen shows the last complete stroke torque profile generated by the actuator.

Event Log (2-wire loop Field unit) - Available to all user levels

Close pop-up
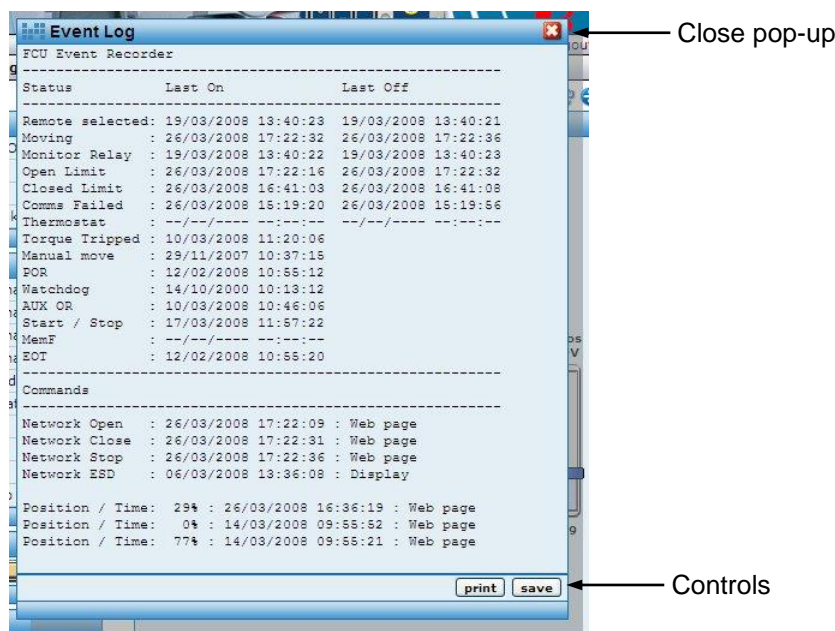
Controls

Fig 54:   Wired IQ / IQT FCU Event Log pop-up

Pop-up screen showing a log of the last occasion on which the various control and alarm events occurred. For commands, the source of the command is also given.

Remote selected - local / remote selector in remote position.
Moving   - actuator centre column moving.
Monitor Relay   - monitor relay alarm.
Open Limit   - open position limit switch.
Closed Limit   - closed position limit switch.
Comms Failed   - loss of network communication.
Thermostat   - motor thermostat tripped.
Torque Tripped   - torque limit level exceeded.
Manual move   - actuator moved by the handwheel.
POR   - power on reset.
Watchdog   - field unit watchdog alarm.
AUX OR   - auxiliary input present.
Start / Stop   - failure to respond to a remote control input.
MemF   - FCU memory chip RAM or ROM fault.
EOT   - motor running at end of travel.
Network Open   - open instruction over the control network.
Network Close   - close instruction over the control network.
Network Stop   - stop instruction over the control network.
Network ESD   - ESD instruction over the control network.
Position / Time - last position control event.
Position / Time - last but one position control event.
Position / Time - last but two position control event.

Controls

Print   : Prints the logger data to a printer attached to the computer.
Save   : Saves the logger data to a file on the computer.

Parameters (Wireless Field unit) - Available to all user levels

Fig 55:   Wireless IQ / IQT Parameters pop-up

Pop-up screen shows the settings for all the parameters relating to the IQ / IQT actuator field unit. For users with Administrator level rights, the values can be edited. The parameters are used to determine the way in which the actuator responds to commands and reports data. Information on how to set these fields is contained in the actuator field unit manuals.

Controls

Save Settings   : Edited fields may be saved to the FCU; accessible by **Administrator** level users only.

Show Alarms (Wireless Field unit) - Available to all user levels

Close pop-up

Fig 56: Wireless IQ / IQT Alarms pop-up

Pop-up screen shows the alarms on the actuator as red lights; grey is no alarm. Additional information on the meaning of these alarms is contained in the individual field unit manuals.

Event Log (Wireless Field unit) - Available to all user levels

Fig 57:   Wireless IQ / IQT FCU Event Log pop-up

Pop-up screen showing a log of the last occasion on which the various control and alarm events occurred. For commands, the source of the command is also given.

Rmt control OK   - On means that the local / remote selector in remote position.
General Alarm   - Any Alarm present on the actuator e.g. Stall.
ESD Active   - ESD signal active on the actuator.
Open Limit   - open position limit switch.
Closed Limit   - closed position limit switch.
Comms Failed   - loss of network communication.
Torque Tripped   - torque limit level exceeded.
Mid travel stop - motor stopped between open and close limits.
Network Open   - open instruction over the control network.
Network Close   - close instruction over the control network.
Network Stop   - stop instruction over the control network.
Network ESD   - ESD instruction over the control network.
Position / Time - last position control event.
Position / Time - last but one position control event.
Position / Time - last but two position control event.

Controls
Print   : Prints the logger data to a printer attached to the computer.
Save   : Saves the logger data to a file on the computer.

Misc (Wireless Field unit) – Downloads available to all user levels, Upload only available to Admin user level

Fig 58:   *Wireless IQ / IQT Downloads pop-up*
Pop-up screen with controls to extract the Actuator Datalogger and Actuator Configuration files. It is also possible to load a configuration file to an actuator using this facility, assuming Admin login. The files that this facility creates are for viewing with the Rotork In-sight software, available on the Rotork web site.

Neighbour Table (Wireless Field unit) - Available to all user levels
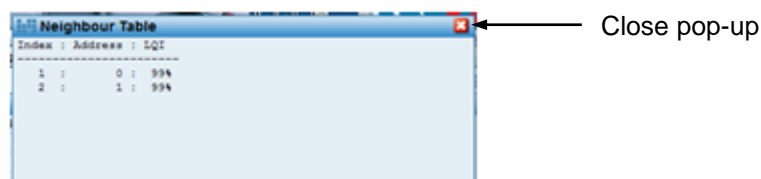
Fig 59:   *Wireless Neighbour tables pop-up*
Pop-up screen that shows, for the field unit selected, the wireless neighbours that it has. It indicates the address of that neighbour and the Link Quality Index (LQI) of the signal from the device to its neighbour. The LQI is represented as a percentage value and is a good indication of signal quality and strength. A good signal would be in the range 93% to 100%. A reasonable signal would be in the range 61% to 92%; reasonable means that if environmental conditions deteriorate there is a greater potential for message retries and message failure.

It should be noted that rain, humidity and fog have a negligible effect on the wireless network. The greatest effect can be seen for heavy snow. By this, we mean snow that has settled on and around the antenna, i.e. 2 inches of snow packed around the antenna can cause a loss of about 10dBs.

Actuator Controls - Available to Write and Administrator user levels only

Open	:	Command to open the valve fully.
Stop	:	Command to stop the actuator in its present position.
Close	:	Command to close the valve fully.
ESD	:	Command to put the valve in its Emergency Shut Down position. (This can be 'stayput' or move to either the open or closed position).
Pos DV	:	A slider control that is used to generate a setpoint position (Desired Value) for the valve in the range 0 - 100%.

All the controls have a confirmation pop-up, so that the action has to be confirmed before it takes place. Web page control must be enabled for these controls to work.

7.5.13   FCU Control - Integral Actuator (2-wire loop only)

Fig 60:   Q actuator FCU Control Web page

This screen is accessible to Read, Write and Administrator user levels.

The Integral actuator FCU Control screen shows a control and status page for a Q type actuator. The screen has information relating to the device, its current condition and system parameters. Control of the actuator is permitted via the control buttons for users with write level access or higher. When not in communication, the screen may still be visited, but the picture has a large red cross over it to show a lack of communication.

Navigation

Navigation between the field units is either by returning to the previous screen, or by using the navigation buttons on this screen. Entering an address directly in the 'Address' box and clicking Refresh moves directly to the selected field unit.

Identification

Tag name	: Identification tag given for this device.
Address	: Network address.
Type	: Shows the identified actuator type as Q.
Network	: The network to which this device is connected (Pakscan 2 for 2-wire loop).

Current Status

The real time status of the actuator is listed in this pane on the screen:

External Input   : Active or Inactive, shows the status of the input.

Valve Position   : Current position, Closed, Open or Stopped Mid-Position.

Actuator   : Moving or Stationary.

Running Direction : Opening or Closing.

Loopback   : Off or On.

Alarm Status   : No Alarm or Alarm.

Actuator Position

For actuators fitted with position feedback facilities, a bar graph shows the current actuator analogue position between 0 (closed) and 100% (open).

FCU Control web page Controls

Parameters - Available to all user levels

Fig 61:   Q Parameters pop-up

Pop-up screen shows the settings for all the parameters relating to the integral field unit. For users with Administrator level rights the values can be edited.

Controls

Save Settings   : Edited fields may be saved to the FCU, accessible by **Administrator** level users only

Show Alarms - Available by all user levels

Close pop-up
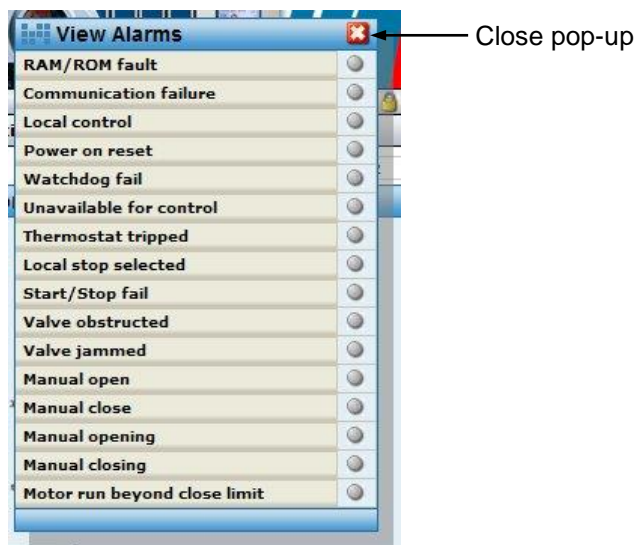
Fig 62:   *Q Alarms pop-up*

Pop-up screen shows the alarms on the actuator as red lights, grey is no alarm. Additional information on the meaning of these alarms is contained in the individual field unit manuals.
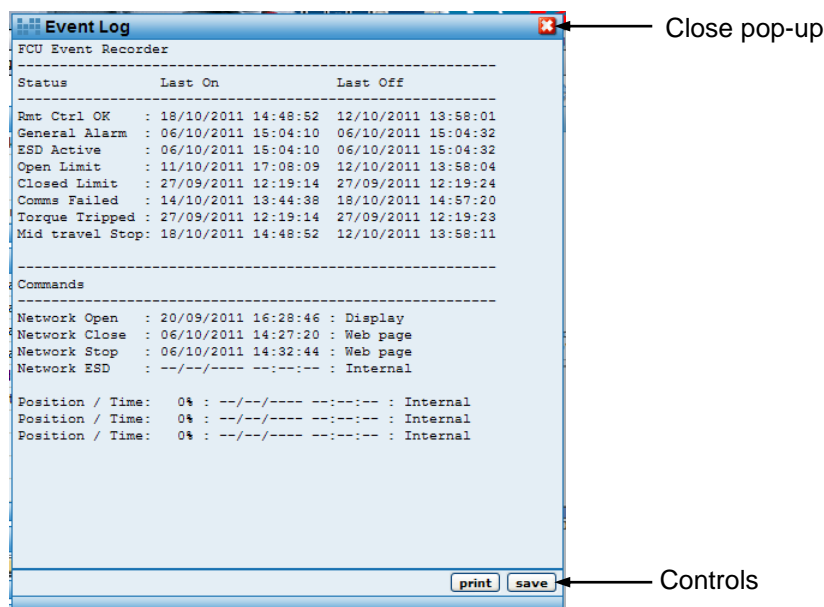
Event Log - Available to all user levels

Close pop-up
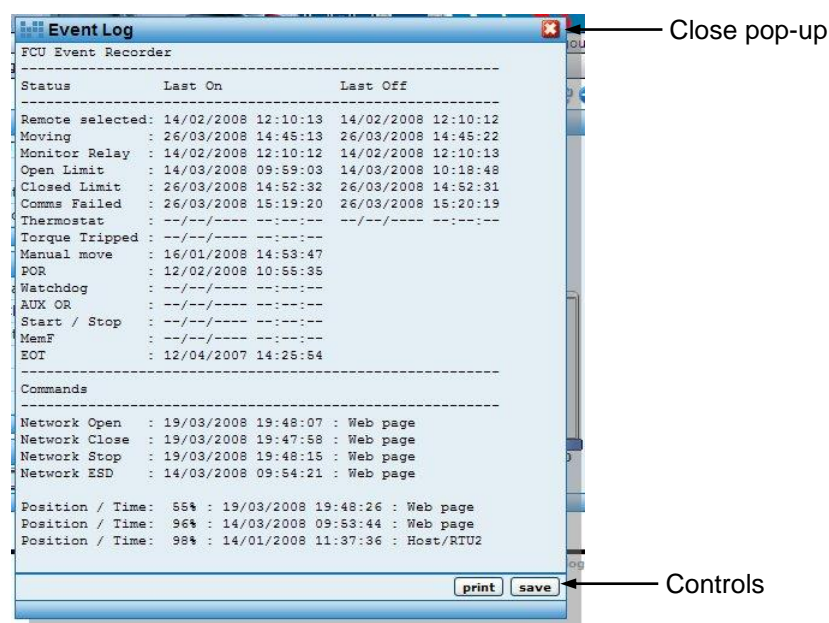
Controls

Fig 63:   *Q FCU Event Log pop-up*

Pop-up screen showing a log of the last occasion on which the various control and alarm events occurred. For commands, the source of the command is also given.

Remote selected - local remote selector in remote position.
Moving   - actuator centre column moving.
Monitor Relay   - monitor relay alarm.
Open Limit   - open position limit switch.
Closed Limit   - closed position limit switch.
Comms Failed   - loss of network communication.
Thermostat   - motor thermostat tripped.
Torque Tripped   - torque limit level exceeded.
Manual move   - actuator moved by the handwheel.
POR   - power on reset.
Watchdog   - field unit watchdog alarm.
AUX OR   - auxiliary input present.
Start / Stop   - failure to respond to a remote control input.
MemF   - FCU memory chip fault.
EOT   - motor running at end of travel.
Network Open   - open instruction over the control network.
Network Close   - close instruction over the control network.
Network Stop   - stop instruction over the control network.
Network ESD   - ESD instruction over the control network.
Position / Time - last position control event.
Position / Time - last but one position control event.
Position / Time - last but two position control event.

Controls

Print   : Prints the logger data to a printer attached to the computer.

Save   : Saves the logger data to a file on the computer.

Actuator Controls - Available to Write and Administrator user levels only

Open   : Command to open the valve fully.

Stop   : Command to stop the actuator in its present position.

Close   : Command to close the valve fully.

ESD   : Command to put the valve in its Emergency Shut Down position. (This can be 'stayput' or move to either the open or closed position).

Pos DV   : A slider control that is used to generate a setpoint position (Desired Value) for the valve in the range 0 - 100%.

All the controls have a confirmation pop-up, so that the action has to be confirmed before it takes place. Web page control must be enabled for these controls to work.
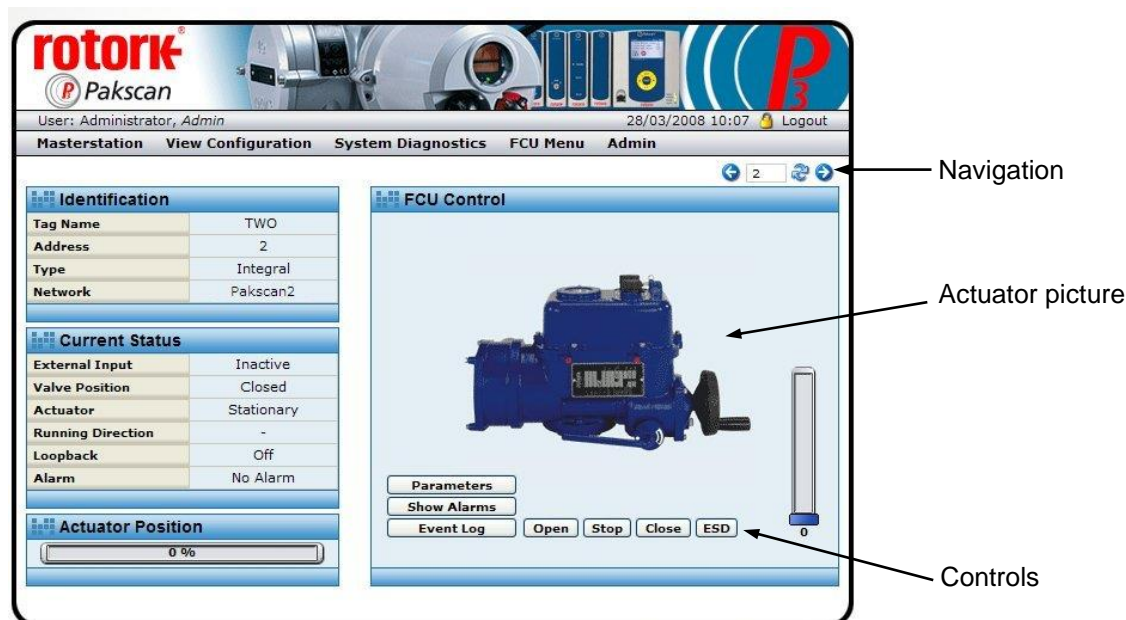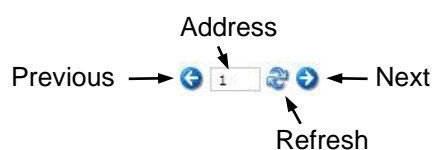
7.5.14   FCU Control - General Purpose Field Control Unit (2-wire loop only)
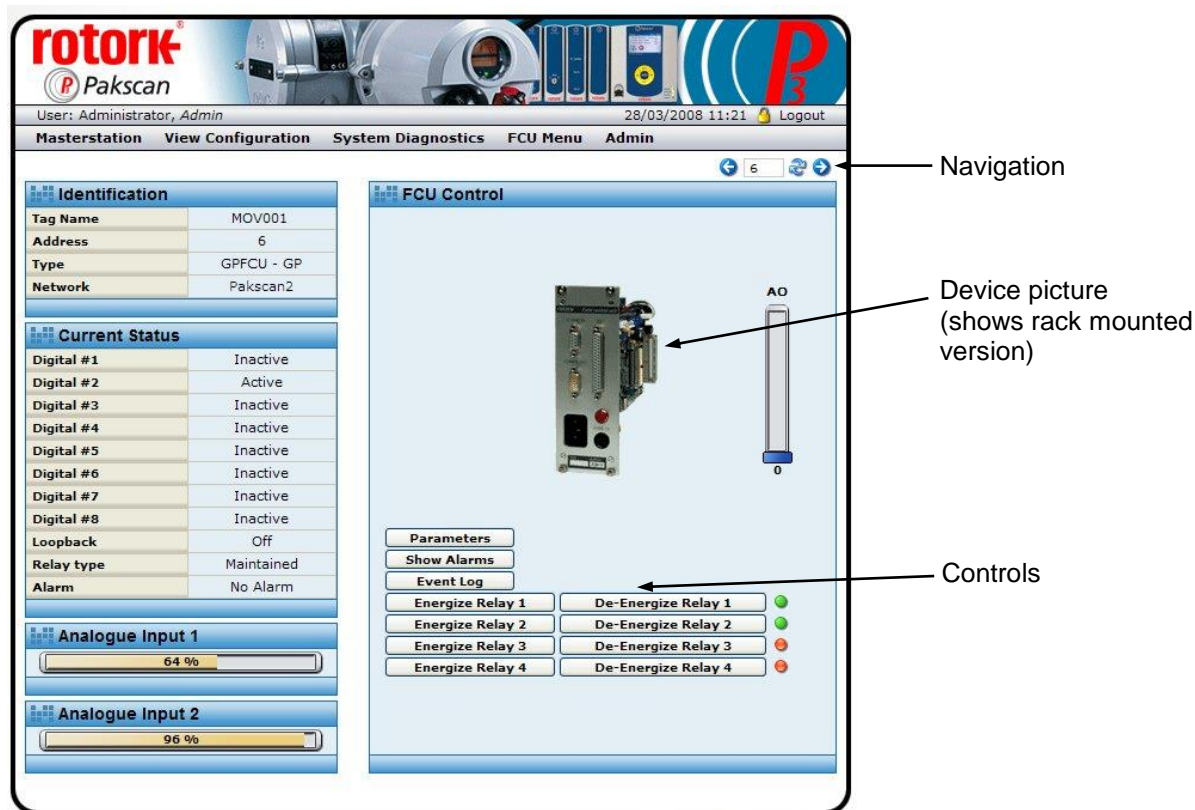
Fig 64:   *GPFCU Control web page*

This screen is accessible to Read, Write and Administrator user levels.

The GPFCU Control screen shows a control and status page for a general purpose field control unit. The screen has information relating to the device, its current condition and system parameters. Control of the outputs is permitted via the control buttons for users with write level access or higher. When not in communication, the screen may still be visited, but the picture has a large red cross over it to show that a problem exists.

Navigation

Navigation between the field units is either by returning to the previous screen, or by using the navigation buttons on this screen. Entering an address directly in the 'Address' box and clicking Refresh moves directly to the selected field unit.

Identification

    Tag name   : Identification tag given for this device.

    Address   : Network address.

    Type   : Shows the identified device type as GPFCU - GP.

    Network   : The network to which this device is connected (Pakscan 2 for 2-wire loop).

Current Status

    The real time status of the actuator is listed in this pane on the screen.
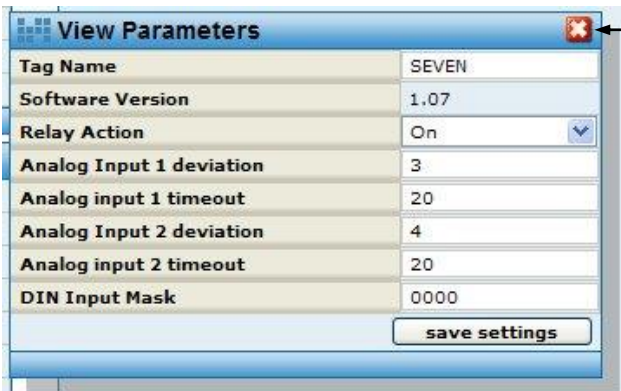
    Digital # 1 to # 8 : Digital input signal status, Active or Inactive.

    Loopback   : Off or On.

    Relay Type   : Fleeting or Maintained outputs from the relays.

    Alarm Status : No Alarm or Alarm.

Analogue Input 1 and 2

    For the two analogue input channels a bar graph shows the current analogue input value between 0 (closed) and 100% (open).

FCU Control web page Controls

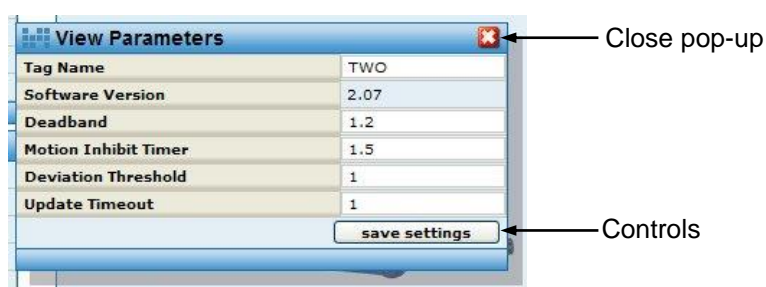**Parameters - Available to all user levels**

Fig 65:   GPFCU Parameters pop-up

    Pop-up screen shows the settings for all the parameters relating to the general purpose field control unit. For users with Administrator level rights, the values can be edited.

Controls

Save Settings   : Edited fields may be saved, accessible by **Administrator** level users only.

Show Alarms - Available to all user levels

                                    —— Close pop-up

Fig 66:   *GPFCU Alarms pop-up*

Pop-up screen shows the alarms on the actuator as red lights; grey is no alarm.

Event Log - Available to all user levels

                                    —— Close pop-up
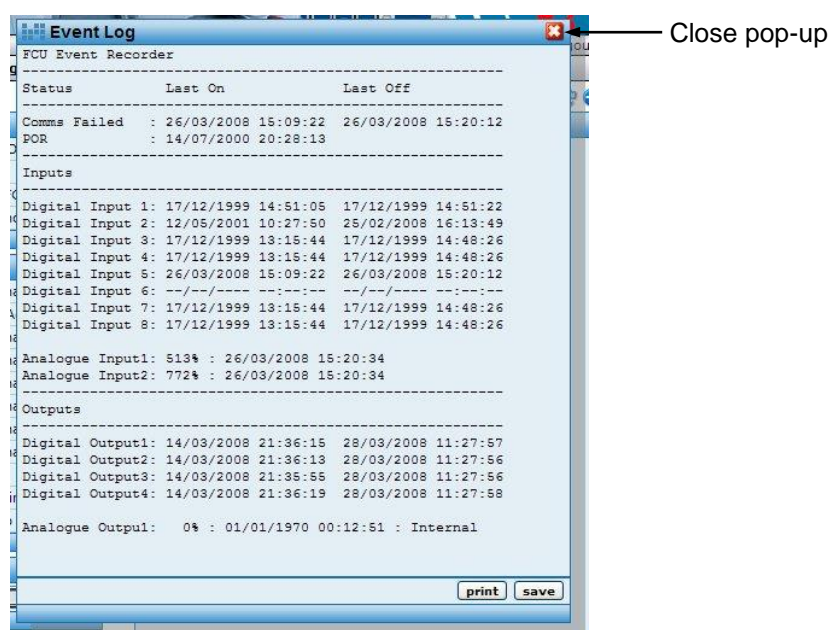
Fig 67:   *GPFCU Event Log pop-up*

Pop-up screen showing a log of the last occasion on which the various alarms, input and output events occurred. For commands, the source of the command is also given.

Comms Failed   - loss of communication with the field unit.
POR   - power on reset.
Digital Input 1-8   - when turned on and off.
Analogue I/P 1-2   - when last updated.
Digital Output 1-4 - when energised and de-energised.
Analogue Output   - when last altered and by which source.

Controls
Print   : Prints the logger data to a printer attached to the computer.

—— Controls

Save   : Saves the logger data to a file on the computer.

GPFCU Controls - Available to Write and Administrator user levels only

Energise   : Command to energise the relays (green light when energised).
Relay 1-4

De-energise   : Command to de-energise the relays (red light when de-energised).
Relay 1-4

AO   : A slider control that is used to generate a 0-5volt analogue output. Slider
                      range 0 - 100%.

All the controls have a confirmation pop-up, so that the action has to be confirmed before it
takes place.

7.5.15 Admin

Fig 68:   Administrator Level

This screen is only accessible to Administrator user levels.

When logged in at Administrator level, the top of the screen menu list includes the Admin button. Clicking on this button gives entry to the Administrator level screens.

7.5.16 Users
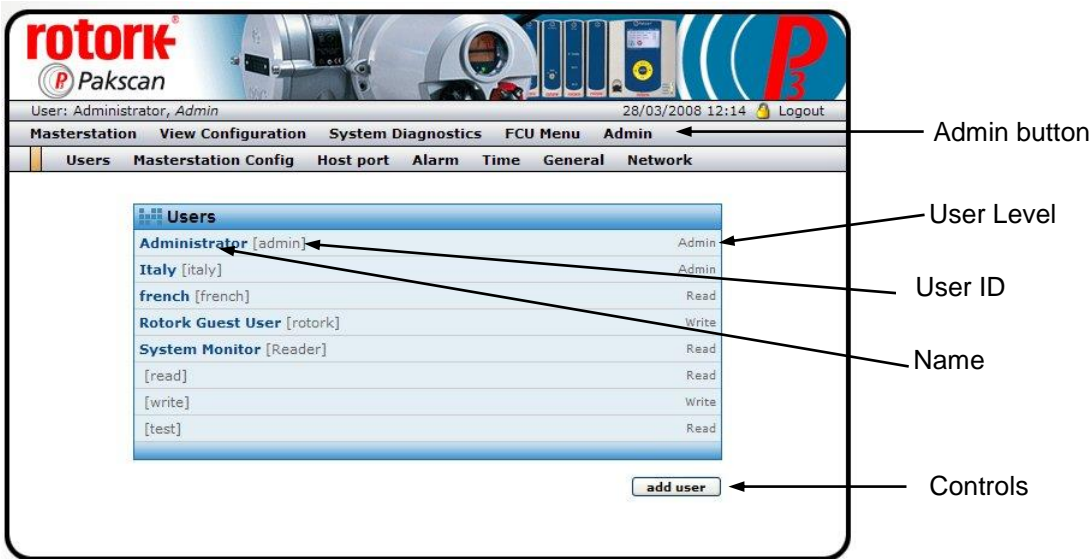
Fig 69:   Users web page

This screen is only accessible to Administrator user level.

The 'Users' screen shows all the users currently entered into the system. The actual user at any time is shown on the top left of the menu bar.

Each user has a Name, a User ID, a User Level and a Password. When logging in to the system, to gain entry, the User ID and Password are required. The screen shows the Name, User ID and User Level; the password is not shown and cannot be revealed on any of the screens.

Every system includes a default User ID of 'admin' and Password of 'admin' on delivery, in order that the system can be set up and commissioned. The user ID 'admin' cannot be removed, but the Password should be changed as soon as possible to protect the system against unauthorised access.

Name	Name of the current user, displayed on the top bar.

User ID	Identification used to gain entry to the system, shown in user list.
Password	Secret code of letters (and numbers) used to gain entry to the system. Not shown on the system.
User Level	Indication of access level permitted for this user, shown on the top bar.

Controls - Available to Administrators only

Add user : Click this button to bring up the screen to add a user.

Username : Click on a user name (e.g. Administrator) to bring up the Modify User screen for editing user details.

Fig 70: Add User web page

The Add User screen contains the fields to be completed for each permitted user, either by completing the data box, selecting from a drop-down box or selecting a radio button.

User ID : Enter a unique name to use when logging in to the system.

Name : Enter a name to be used in all emails and on the system logs.
Several users can have the same name, but this is not recommended.

Email : If Email messages concerning the system alarms are to be sent to this user, enter a valid Email address.

Mobile : If text messages are to be sent to a mobile phone associated with this user, enter the complete phone number here.

Alarm User : Select 'Yes' or 'No' for the choice of sending Emails and Text messages to this user.

Email Master station Log	: Select 'Yes' or 'No' for the choice of sending the master station log file via Email.
Language	: Select the language to be used on the screens. Choices are English, Spanish, French, German and Italian.
User Level	: Select between Read, Write and Admin levels.
Password	: Enter a unique password of letters and/or numbers kept secret by this user.
Repeat Password	: Enter the same password as above.
Back	: Exit the screen without saving anything and return to the previous screen.
Save Settings	: Save the details of this user (either new or edited values).

Fig 71:   Modify User web page

The Modify User screen allows user details to be altered or a user to be removed. A User cannot delete himself from the system. So, here in the example, the User ID of 'admin' is greyed out, since this is the actual user.

Remove	: Delete this entry on the system. A User cannot delete themselves, only those with less access rights. If the User selects his own entry to modify the button is greyed out.

7.5.17   Master station Configuration

The master station configuration page is used to set the parameters required for successful operation of the system and the parameters for the option modules fitted. In addition, it may be used to enter the site name and tag name of the system and various security settings. The values set in these parameters can be viewed under the 'View Configuration' button, but they may only be altered by users logged in at Administrator level.

The Master station settings relate to the overall performance of the system and common features and actions, irrespective of the option module fitted. Where these settings are relevant, they apply to all the option modules in the master station.

The Option module settings relate to the particular option module fitted in the Option 1 and Option 2 slots.

Fig 72:   Master station configuration web page: General Settings

This screen is only accessible to Administrator user level.

Masterstation Configuration [General Settings]

Site Name : A text field in which a description of the site can be entered for identification purposes.

Tag Name : A text field in which a tag identifier for this particular master station on the site can be entered.

Option 1 and Option 2 Modbus Address : A numeric field for the address number. When addressing the P3 master station using a host, the user must use the appropriate Modbus address. It is possible to fit up to 2 network option modules to the P3 master station. Each option module will have its own Modbus address, therefore there are up to 2 Modbus addresses to set up, one for each option module fitted. In a system with only 1 option module fitted, only the address for the appropriate option module fitted is required to be set up.

The default value is **240** for a Pakscan 2 Loop option module and **200** for a Pakscan wireless option module. It is recommended that his is changed to avoid conflict with any new system added

Note for Pakscan 2 Loop module Modbus Addressing

In some cases when using Pakscan Generic Modbus protocol settings, the master station will respond to more than one address; and the setting here is the Base address. There is more information on the base address and offset addresses in the Pakscan Modbus Protocol document (PUB059-003 formerly S171E).

Monitoring wireless and Control wired : Only in a system where each actuator has a wired and a wireless Pakscan module fitted, should this be enabled. This feature will pair up the wired and wireless modules and enable them to be shown together in the FCU menu web page. The pairings will be:

- **the first wired address with the first wireless address,**
- **the second wired address with the second wireless address,**
- **...... and so on.**

Therefore in a system where the wireless addresses start at 61 (wired always start from 1) the pairings would be:

- Wired address 1 with wireless address 61
- Wired address 2 with wireless address 62
- Wired address 3 with wireless address 63
- ..... and so on.

The FCU menu will appear as below:

Address	Tag Name	Type	Network	Alarm	Comms Fail	Navigation
1	-	IQT	Pakscan2	●	●	fcu control
61	-	IQT	Wireless	○	○	fcu monitoring
2	-	IQ	Pakscan2	●	●	fcu control
62	-	IQ	Wireless	○	○	fcu monitoring

Hot Standby Module	:	Either 'Enabled' or 'Disabled'. When there is a partner module acting as a standby unit this option should be set to 'Enabled' to allow exchange of data between the two modules.
ESD Settings	:	These five drop-down boxes can each be set to 'Enable' or 'Disable' the related Emergency Shut Down signal, depending on the particular site requirements. In general the settings should be 'Disabled' unless the particular Emergency Shut Down function is required. The action for each individual actuator has to be set locally on the actuator to either close, open or stay put (no movement on receipt of the ESD signal), as required for each valve; refer to individual actuator manuals.
Command Settings	:	These five drop-down boxes can each be set to 'Enable' or 'Disable' the host system commands to the actuators and field units from the indicated source of the signal. For example, commands over the Ethernet connection can be disabled, whilst those from Serial Port 1 can be enabled. Ethernet commands are those sent via the Ethernet ports from the host system using Modbus TCP. Commands on the individual field unit web pages can also be disabled. Serial Port 1 and Serial Port 2 are the RS-232/RS-485 Modbus RTU ports, which are commonly used for control and monitoring. The Keypad is the control source on the front panel of the CPU module.
Copy Options	:	These four drop-down boxes can each be set to 'Enable' or 'Disable' the copying of information between the A side and B side CPU and Option modules in a hot standby system. They do not appear in a single module system.

Settings   - Enable to copy *all* the settings, except those listed below, between the units.

Address   - Enable to copy the Modbus addresses of the CPU (P3 option) and Pakscan Loop option module between the units.

Tag   - Enable to copy the Site name and system Tag name between the units.

IP   - Enable to copy the IP address and Ethernet settings between the units

Display Language	:	This drop-down box contains the options enabling the system language to be chosen. The options are English, Spanish (Espanol), French (Francais), German (Deutsch), Italian (Italiano) and Hungarian.
Security Settings	:	A text box is provided in which the system PIN can be entered, and a drop-down box provides the options for access permission when using the CPU keypad and screen.

Note that the 'Command Settings' above can be used to prevent keypad commands under all circumstances, but when the keypad is enabled the security settings below will apply.

PIN - The Password number is a variable between 0 and 9999. When a number is entered, it indicates that the PIN must be used   for settings or commands to be allowed from the CPU keypad in accordance with the associated drop-down box setting.

Security - The drop-down box contains the options for selecting the protection afforded against inappropriate actions when using   the CPU keypad.

> **None** : All settings and control commands accessible via the keypad without protection by a PIN.

> **Set up** : Control commands accessible via the keypad without a PIN, but all setting changes via the keypad require the PIN to be entered first.

> **Set up and Control** : Any control command action or setting changes via the keypad require the PIN to be entered.

> **Locked** : No keypad access permitted for any control commands or setting changes whilst there is host activity on any of the serial or Ethernet data links. [If all serial and Ethernet communication links are inactive for 5 seconds then keypad commands can be entered provided the PIN is entered (as with the Set up and Control level)].

Software Version	:	The version of software fitted to the CPU module. In hot standby systems the modules in both the A and B side should have the same version of software.
Country Code	:	This setting relates to the wireless option only. Whilst the frequency band over which the wireless communicates is a globally available band, there are frequencies within this band that certain countries do not allow. This parameter is set up during the first 5 times that the master station is powered up or by using the HMI menu A3F. This setting will ensure that that the channels made available for selection within the wireless option module are only those legally available within that particular country.
Number of Channels	:	This value is derived from the actual hardware of the CPU and indicates the maximum number of actuators or field units that can be connected to this system. The field units can be split between the option modules fitted.
FCU distribution between Option Slots	:	Using the slider bar the user is able to select the number of field units connected to each option module fitted in batches of 60. Simply select and drag the bar to the appropriate setting with the mouse, the text above the bar will indicate what has been selected.

The bar will only allow selection up to the maximum number of field units available on the master station in question.

This bar only selects the **number of field units** allocated to the two option slots and **not** the address range of the field units on the option slot network. The Pakscan 2 loop actuators will always start at address 1. In the example shown on the next page, where there are 180 devices on the Pakscan 2 loop module, the addresses 1 to 180 will be for the Pakscan 2 loop units. The starting address for the wireless devices is set up in the wireless configuration section and this would logically (but not necessarily) be set to 181. This would mean that the addresses for the 60 wireless devices can range between 181 and 240.

Slider bar for selecting
the number of units
for each option

Indicates the number of
field units selected for
the option in slot 1

Indicates the type of
option fitted to slot 1

Indicates the number
of field units selected
for the option in slot 2

Option slot 1   Wireless   60 Channels
Option slot 2   Pakscan2   180 Channels

Indicates
the type of
option fitted
to slot 2

| 60 | 60 | 60 | 60 | 60 |

240   300

Indicates the
maximum number of
devices possible on
option slot 1 (1 x 60)

Indicates the
maximum number of
devices possible on
option slot 2 (3 x 60)

Indicates the
absolute limit of
a Pakscan
system

Indicates the limit of **this** Pakscan master
station system, this will be the same as
the **Number of channels field**

Fig 73:   Web page Field unit distribution bar

Controls

    print page   : Prints the settings to a printer attached to the computer.

    save settings   : Saves the settings to the master station CPU module. Until they are saved
                             any alterations to the settings will not take effect.

Masterstation Configuration [Pakscan 2 Loop]

The Pakscan 2 Loop option module controls the actuators and field units over a 2-wire cable wired in a ring or loop, visiting each actuator in turn. The data signal is a modulated 20 mA current and the system includes automatic cable failure protection and detection.

Fig 74:   Master station configuration web page: Pakscan 2 Loop

Software Version :   The version of software fitted to the Pakscan 2 Loop option module. In hot standby systems the modules on both the A and B side should have the same version of software.

Highest FCU   :   This text box contains the setting for the highest address used for an actuator (or field unit) on the 2-wire loop. The Pakscan 2 Loop module polls all field units from address 1 up to this highest address. The loop scan time is minimised by restricting the polling to only those field units that should be present and scanning up to the highest address. All the addresses in the selected range should be used and gaps in the address range should be avoided. Gaps or unused addresses cause the system to run more slowly as the unused addresses are still checked. In addition, unused addresses will generate a communication failure alarm.

Loop Speed   :   This shows the current loop scanning speed (loop baud rate) and the drop-down box allows a desired loop speed to be selected. The choices are 2400, 1200, 600, 300 and 110 baud. When a new speed is entered it will take effect as soon as the values are saved. The setting applies to the Pakscan 2 Loop option module only and the actuators must be changed individually.

New Loop Speed : The drop-down box allows a new scanning speed (loop baud rate) to be selected for the field units in the actuators. The new speed will be adopted next time the loop is reconfigured. A change here should be mirrored by a change in the loop speed setting above. It is possible to select rates in the range one step up or two steps down from the current speed.
If the loop communication is not stable, it is often necessary to reduce the speed to improve reliability. If the field units are all in communication with the master station, this facility to globally change the speed of all the field units can be used to assist in improving the reliability.

Loop Speed Doubling : On a stable loop it is possible to halve the loop scan time by doubling the data speed using this setting. Care is needed to ensure that the loop continues to be stable, since the use of this feature slightly reduces the system's capability to reject interference from pumps and motors.

Retain Data on Loss of Communication : Normally the database information about an actuator is cleared to zeros if communication with the actuator is lost. This ensures that the false valve position information is not transmitted to the host system during the loss of communication. A single 'Comms Fail' data bit is set. This system setting allows the data to be kept at the last value received from the actuator. Note that the data is retained indefinitely and does not necessarily reflect the true actuator status.

DV Convert : This option can be used to ensure that 100% and 0% Desired Value outputs to the IQ, IQT, Skil and EH actuators are transformed into actions to make the actuator run to the fully open (100%) and fully closed (0%) positions. The message is converted from a DV command to an Open or Close command. This is useful for positioning actuators, where it is possible that the valve will not fully shut or open when moved by only a small amount. When used for tight shut-off valves, with analogue position control only, the setting should be ON; the default is OFF.

If limited range positioning is selected, only enable DV Convert if you wish the valve to travel to the fully open and fully closed positions.

Host Port 1 Database Selection : The drop-down box allows the database organisation use on this port to be selected. The choices are Generic Modbus, Honeywell EPLCG Modbus, Yokogawa Modbus and Honeywell SI Modbus.

Host Port 2 Database Selection : The drop-down box allows the database organisation used on this port to be selected. The choices are the same as for Host Port 1.

Ethernet Database Selection : The drop-down box allows the database organisation use on the Ethernet ports to be selected. The choices are the same as for Host Port 1.

Port Alarms : This drop-down box allows port alarm handling to be configured. Alarms can either operate completely independently ('separate') for each port, or can be linked such that the same alarm information is always reported, regardless of which port is used.
Alarms must be read and accepted before they can clear and return to normal. If configured as separate, alarm reading and acceptance must be done separately for each of the three ports. This ensures that the different hosts see all the alarms. When the alarms are linked, accepting an alarm on one port accepts the alarm on all the other ports as well.

The status screen displays for alarm indication cannot be linked to the serial communications alarm handling.
Linking the port alarm operations is useful in dual redundant serial link configurations between the master station and the host computer.

Controls

Save Settings : Saves the settings to the Pakscan 2 Loop option module. Until they are saved, any alterations to the settings will not take effect.

To print out the settings use the Print Page button below the Master station Configuration section of the screen.

Masterstation Configuration [Pakscan 3 Wireless]

The Pakscan 3 Wireless option module controls the actuators and field units over a wireless network.

Option 1: Pakscan 3 Wireless	
Software version option 1	**1.3.8**
Coordinator Software Version	**6E.1.3**
Lowest FCU address on this option card	1
Total FCU's expected on this option card	2
Total Wireless Repeaters expected on this option card	None
Wireless Network PAN ID	DA15
Retain data on loss of communications	OFF
AES Key	0F1571C947D9E8590CB7ADD6AF7F6798
RF Channel	24
Third party devices fitted	No
Third party devices are disabled	
	save settings

Fig 75:   Master station configuration web page: Pakscan 3 Wireless

Software version : The version of software fitted to the Pakscan 3 option module. In hot standby systems the modules on both the A and B side should have the same version of software.

Coordinator Software version : The version of software fitted to the Pakscan 3 option module / P3W coordinator, relating to the radio functions. In hot standby systems the modules on both the A and B side should have the same version of software.

Lowest FCU address on this card : This field indicates the starting address of the field units connected to this option module. It is important to ensure that there is no overlap of addresses between option modules. Where the wireless module is the only module fitted the address can be '1'. If a wired option network module is fitted, the wireless address should be a value above the wired network limit. For example, where there are 180

wired devices and 60 wireless devices (as shown in Fig 66), the lowest wireless address would be set to 181.

Total FCU's expected on this option card	:	The total number of field units that are expected to be found on this network associated with this module. The master station will expect to find this number of field units on the network starting at the address set.
Total Wireless Repeaters expected on this option card	:	The total number of P3W Repeaters that are expected to be found on the network associated with this module. There can be a maximum of 15 P3W repeaters fitted to a wireless network.
Wireless Network PAN ID	:	The PAN ID is the Personal Area Network Identification number of the network attached to this option module. For a device to connect to the master station it must have a PAN ID the same as the master station. The default value is DA 15 and the range is 00 00 to Hex FF FF. Where there are multiple networks in close proximity, the PAN IDs should be set to unique numbers.
Retain Data on Loss of Communication	:	Normally the database information about an actuator is cleared to zeros if communication with the actuator is lost. This ensures that the false valve position information is not transmitted to the host system during the loss of communication. A single 'Comms Fail' data bit is set. This system setting allows the data to be kept at the last value received from the actuator. Note that the data is retained indefinitely and does not necessarily reflect the true actuator status.
AES Key	:	Pakscan wireless employs the Advanced Encryption Standard (AES) as a method of protecting the command messages to devices on the network. The AES key must be the same on all devices on the network and the master station. To protect the commands the AES key should be kept secret. The AES key is a 128bit hexadecimal value, if a device does not have the same AES key as the master station, it will not be able to be commanded by the master station.
RF Channel	:	The range of frequencies in the 2.4GHz band over which the Pakscan wireless network communicates is split into channels. Some countries will not accept communication over certain frequencies. Therefore, the country code chosen in the general settings will ensure that the channels available to be selected using this drop-down box are only those that are legal.
Third party devices fitted	:	Using a P3W Modbus Adapter (WMA) it is possible to connect other manufacturers' devices into the Pakscan Wireless network. If 'yes' is selected in the drop-down box and the setting is saved, the web page will change to show the following:

The user may then select the Modbus address of the device or devices that are connected to the P3W WMA, It is possible to have 47 Modbus devices integrated into the network using addresses 201 to 247. It is possible to have more than one Modbus device connected to a P3W WMA. All Modbus devices must have unique addresses that must not clash with other Modbus devices in the network. For Modbus devices fitted in the Pakscan wireless network, the master station system is effectively used as a transparent transport mechanism i.e. the host sends Modbus requests to the master station as though addressing the device directly.

Controls

Save Settings : Saves the settings to the Pakscan 2 Loop option module. Until they are saved, any alterations to the settings will not take effect.

To print out the settings use the Print Page button below the Master station Configuration section of the screen.

7.5.18   Host Port Configuration

Fig 76:   Host Port Configuration web page

This screen is only accessible to Administrator user level.

The host port configuration page allows the settings for the serial and Ethernet ports to be made. The two serial ports (ports 1 and 2) are independent from one another whilst the Ethernet ports (ports 3 and 4) are linked together.

Host Port 1

Baud Rate : This drop-down box allows the communication speed (baud rate) for the serial port to be selected. The choices are 115200; 57600; 38400; 19200; 9600; 4800 or 2400.

Parity : This box sets the message parity used by this port. The choices are None; Always 0; Odd or Even parity.

Standby Mode : The performance of the port when the CPU module is in standby mode is set by this drop-down box. The Serial Port should appear as Passive if the Cross Connect DIP switch on the system back plane is set to 'cross-connect'.
If the port is set to RS-485 highway and is being used on a multi-drop highway, it *must* be set to passive. If it is not shown correctly it probably means the DIP switch is incorrectly set.
When the port is set to 'Active' it will respond to incoming messages with a reply; when set to 'Passive' it will not reply. If the highway is multi-drop, then these replies will conflict with those from the CPU in Main mode.
Note that a CPU in main mode is active and always replies to incoming messages.

Cross Connected : Either Yes or No, indicating the status of the cross-connect DIP switch on the back plane. A system using RS-485 communication and a Hot Standby pair should be set to 'Cross-Connect' and display 'Yes'.

Physical Interface : Either RS-232 or RS-485, showing the switch setting for the physical interface from the CPU module.

Host Port 2

Baud Rate : This drop-down box allows the communication speed (baud rate) for the serial port to be selected. The choices are 115200; 57600; 38400; 19200; 9600; 4800 or 2400.

Parity : This box sets the message parity used by this port. The choices are None; Always 0; Odd or Even parity.

Standby Mode : The performance of the port when the CPU module is in standby mode is set by this drop-down box. The Serial Port should appear as Passive if the Cross Connect DIP switch on the system back plane is set to 'cross connect'.
If the port is set to RS-485 highway and is being used on a multi-drop highway, it *must* be set to passive. If it is not shown correctly, it probably means the DIP switch is incorrectly set.
When the port is set to 'Active' it will respond to incoming messages with a reply; when set to 'Passive' it will not reply. If the highway is multi-drop, then these replies will conflict with those from the CPU in Main mode.
Note that a CPU in main mode is active and always replies to incoming messages.

Cross-Connected: Either Yes or No, indicating the status of the cross connect DIP switch on the back plane. A system using RS-485 communication and a Hot Standby pair should be set to 'Cross-Connect' and display 'Yes'.

Physical Interface: Either RS-232 or RS-485, showing the switch setting for the physical interface from the CPU module.

Ethernet Port

Standby Mode : The performance of the port when the CPU module is in standby mode is set by this drop-down box. The Ethernet Port should be set as Passive if the system includes a hot standby CPU to avoid conflicts in communications.

When the port is set to 'Active' it will respond to incoming messages with a reply, when set to 'Passive' it will not reply.

Note that a CPU in main mode is active and always replies to incoming messages.

IP Authentication : The two IP addresses that can be set here are to do with system access permission. When controlling the system via Ethernet and Modbus TCP, it is possible to increase the system security and only permit access from specified IP locations. If both the values set here are 0.0.0.0 then any IP address can access the system.

When a specific IP address is entered in either IP Number 1 or IP Number 2, the system only allows access for Modbus messages originating from those addresses. Note that all access, including Read only access, is restricted by the entries.

Controls

Save Settings : Saves the settings for the ports. Until they are saved any alterations to the settings will not take effect.

Modbus Message: Brings up the Modbus test screen where specific messages can be sent to the system via the web page.

Fig 77:   Modbus Message Generator web page

The Modbus Message screen allows a specific query to be sent to the system and the response to be viewed.

Modbus Message Query

Address	: The CPU master station Modbus address (in the range 0 -247).
Function Code	: Modbus function code to read or write register, discrete or coil.
Data	: Modbus data relating to the query message. There is no need to include the CRC in the data field as the system generates this automatically. There should be no spaces in the data field.

Controls

Send Query	: Transmits the message to the master station.

Modbus Message Response

Address	: The address of the responding system. It will match the query address.
Function Code	: Modbus function code to read or write register, discrete or coil.
Data	: Modbus data reply, without a CRC. There will be no spaces in the data field.

Example:

Read the number of field units connected to the system; generic database is set up. Refer to PUB059-003 (formerly S171E) for the mapping of the Modbus registers. Number of FCUs is at master station register 0007. Function code 03 (holding register read) can be used. The Modbus function would be:

Modbus Address	function code	register to start read	number of registers to read
01	03	00 07	00 01

The address and function code should be entered in the relevant spaces and the data field should contain the rest of the function, this field should be entered with no spaces. When the send query button is pressed the result will be shown.

Fig 78:   Modbus Message Example web page

Here the data shows that 2 bytes of data are present in the message (02) and the data is 00 19. The 19hex is the number of field units fitted to the A side of the loop.

7.5.19   Alarms

Fig 79:   Alarm Reporting Set up web page

This screen is only accessible to Administrator user level.

This page is used to set up the email alarm reporting from the system to the dedicated recipients as specified in the user set up screen. Each system user may be specified to receive alarm messages as emails or by text when their log-in credentials are specified. Refer to the section on Users to see how this is set up. The Alarm page has two sections. The first deals with the way emails are to be generated and the specifying of a suitable SMTP server, whilst the second specifies which events will cause messages to be sent.

Alarm Email Settings

Email Alarm	: Set to Enable or Disable the whole process.
SMTP Server	: Specifies the server that the master station will use for forwarding emails. This is either a domain name or IP address for the server on which the email account has been set.
SMTP Authentication	: If the domain server supports SMTP authentication, then set this to Enable and complete the Authentication parameters. (More information on SMTP Authentication can be found in RFC 4954 available on the internet.) Authentication Method - auto, plain, login or cram-md5; usually set to login. Username - the email user name for the master station or an identifier. Password - the chosen verification password for authentication of the messages from the master station to the server.
Sender	: A name to identify the master station, it could be the tag name.
Reply Path	: The email address of the master station or an alternative reply address for return messages.
Test Email :	Enter a valid email address to send a test message to in order to ensure the system is working correctly; then click on 'Test'.

Controls

Test	: Sends a test email to the specified address.
Save Settings	: Saves the 'Alarm Email' Settings.

FCU Alarm

This table lists the devices on the field network by address and tag number. The right hand side box, when clicked, toggles between a tick and no tick. A tick indicates that if any alarm occurs on this field unit, it will be reported by the email or text facility.

Controls

Clear All	: Removes any ticks from all the boxes in the list.
Set All	: Adds a tick in all the boxes in the list.
Save Settings	: Saves the FCU Alarm list settings.

Event List

This table lists all the Master station and Option module alarms that can be used to initiate an alarm email or text. The list is split into two parts relating to the CPU module and the Option module(s).

Controls

Save Settings	: Saves the Event List settings

7.5.20 Time
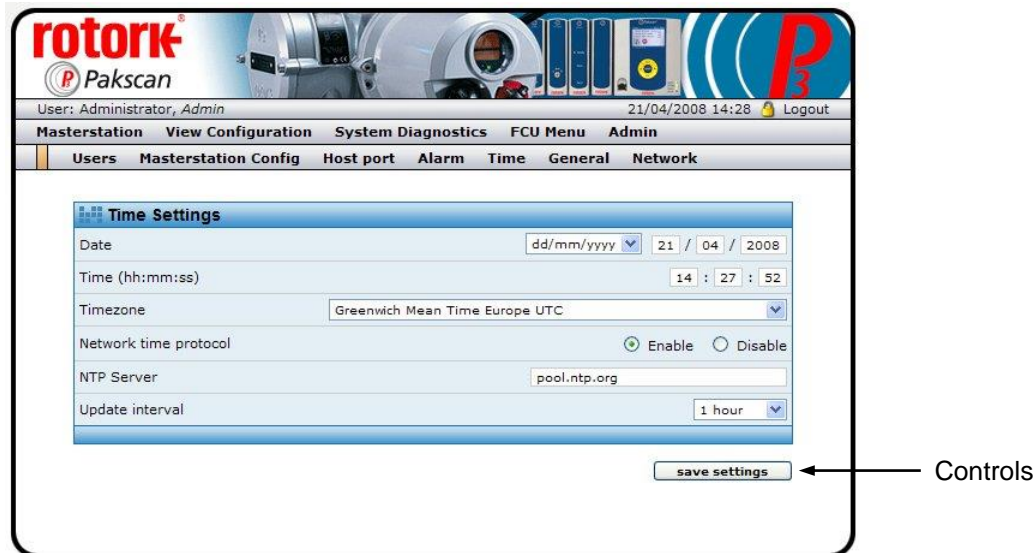
Fig 80:   *Time Settings web page*

This screen is only accessible to Administrator user level.

The master station keeps track of time and date in order to correctly mark events in the logs and to timestamp the emails sent. The date can be in European or American format and the clock can be synchronised with a network time server when an Internet connection is provided.

Time Settings

Date	:	The date can be displayed as Day/Month/Year or Month/Day/Year by choosing from the drop-down box.
Time	:	Shows the current time. This can be altered by clicking in the box and entering the new time (hr, min, sec) as required. If NTP has been set up and enabled this will update automatically, otherwise the time can be checked periodically and corrected here.
Timezone	:	Select the desired time zone from the drop-down box. A new time zone entry requires that the master station reboots.
Network Time Protocol	: :	NTP is a protocol designed to synchronize the clocks of computers over a network. If this feature is being used it needs to be 'Enabled' by selecting the correct setting here.
NTP Server	:	The time server selected is pool.ntp.org which selects from a pool of time server volunteers. Other NTP servers are available and can be used, in which case the entry here should be altered.
Update Interval	:	This drop-down box allows the interval between time checks with the server to be altered between 10 minutes and 2 hours.

Controls

Save Settings	:	Any changes are not implemented until the Save Settings button is clicked. Changes to these settings will require a reboot of the system. The web page will prompt this.

7.5.21   General
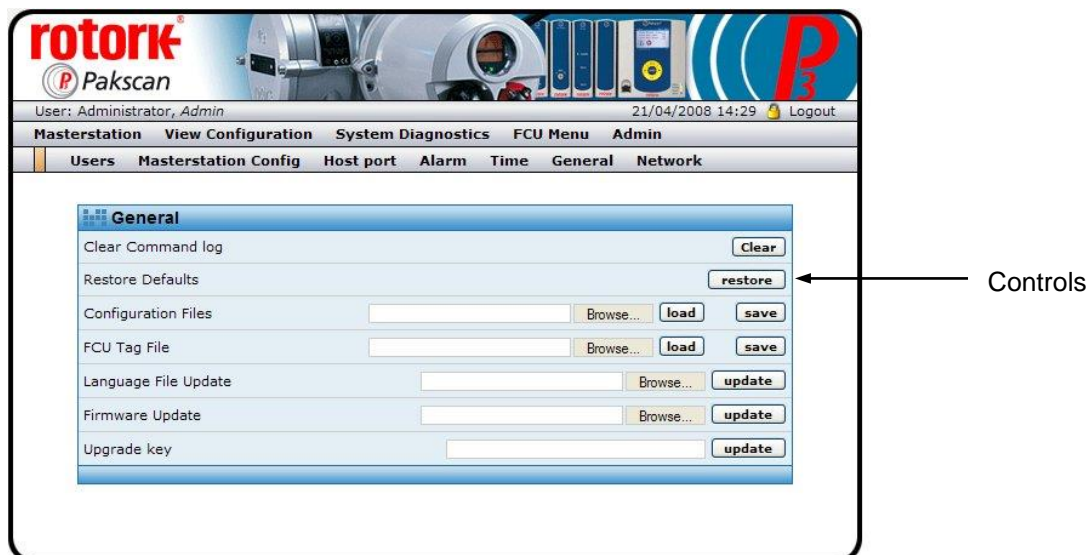
Fig 81:   General web page

This screen is only accessible to Administrator user level.

The General screen contains facilities for upgrading and maintaining the master station.

General

Clear Command Log	: The master station data logger (which can be found under System Diagnostics, ms datalogger) creates a file for all the recorded events. The Clear Command button empties this file. If required, the file can be saved before this process by going to the ms datalogger page and using the 'Save' facility.
Restore Defaults	: All the default settings can be restored by clicking the 'restore' button. This facility can help in setting the master station and option modules to a known state before altering the settings for a particular system.
Configuration Files	: The system configuration file can be saved by using the 'save' button. As default, the file will be named 'backup.nbb', but can be altered to a more meaningful name. It will be filed in a location chosen during the save routine. A previously saved file can be restored by browsing to the nbb file location and using the 'load' button.
FCU Tag File	: The list of tag names for the field units can be saved by using the 'save' button. The saved file name is fcuconfig.xml as default and is filed in a location chosen during the save routine. A previously saved file can be restored by browsing to the file location and using the 'load' button. Modifications to the tag file can be made using a web browser and selecting the source view.

In some cases the web browser will open the fcuconfig.xml file instead of saving it. Save the file by using the 'save as' facility under the File menu on the web page. When naming the file, it will appear as fcuconfig_xml and the option of file type is presented. Ignore the options and change the file name and extension to fcuconfig.xml, then click on save. The resulting file will be in the desired xml format.

Update	click on 'update'.
Firmware Update	: To update the firmware, browse to the location of the new file and click on 'update'.
Upgrade Key	: If a new key code has been purchased (to enhance the overall system capabilities) the new code must be entered here. Type the code into the box and click on 'update'.

7.5.22 Network

Fig 82:   *Ethernet Network Settings web page*

This screen is only accessible to Administrator user level.

In order to connect the master station to a network there are several settings and IP addresses that must be set. If that network extends onto the internet then additional settings for the gateway and DNS servers must also be added. This page allows these settings to be made.

Network Settings

MAC ID	: The unique identifier for this hardware. The Media Access Control number is embedded in the master station Ethernet port.
DHCP	: The Dynamic Host Configuration Protocol setting allows the master station to use a fixed (static) IP address or a dynamic address which it collects from the server. In practice, a fixed Static IP is usually preferred.
Host Name	: This is the identity of the basic module used in the system for reference on the Ethernet highway. The default of Pakscan3 is generally acceptable and need not be altered, even if several master stations are on the same network.
IP Address	: The Internet Protocol address that uniquely identifies this master station. This will generally be allocated by the network system administrator.

Netmask : The netmask is allocated by the system administrator and set here.

Gateway : When the master station is connected to a gateway or router onto the internet, the gateway IP address is entered here so that the master station and gateway can exchange data.

Primary DNS : When connecting to the internet, the Internet Service Provider (ISP) will have two server IP addresses that are needed by the system to complete the data routing. Usually, data is exchanged via the Primary Domain Name Server IP. The address is entered here.

Secondary DNS : The second IP address supplied by the ISP.

Controls

Save Settings : Any changes are not implemented until the Save Settings button is clicked. Changes to these settings will require a reboot of the system. The web page will prompt this.

7.6 Setting Up the Master station Configuration Using the Web Pages

This section describes some of the settings required to be made in the master station to be able to correctly commission the Pakscan system.

In order to set up the system by using the web pages, it is necessary to access the system from a computer. This can either be directly connected, as described earlier, or via an Internet connection. Once the computer is connected, it is necessary to log in to the system at Administrator level using the correct password. Systems are shipped with a default administrator username of **admin** and password of **admin**. See section 7.5.1 for details of the log in procedure.

Select **Admin** to go to the start of the system set up pages. See section 7.5.15 onwards for details of the options available on the Admin page.

Click on **Masterstation Config** to enter the main system configuration page - see section 7.5.17. Modify this page to set up the master station parameters by using the drop-down boxes for each parameter. Most default values will be suitable for getting the system started, though consideration should be made for every setting.

Once the settings for each section are as required, they must be downloaded to the master station CPU module. Click on the appropriate **save settings** button for the changes made, and wait for the web page to refresh before moving to the next task.

7.6.1   Masterstation Config - Modbus Address

The Modbus address for host communications is set on the master station configuration page. Change the Modbus address to match the desired serial communication and Modbus TCP address for access to the actuators on the current loop. The user may need to change both the option 1 and option 2 Modbus addresses depending on the system. The two Modbus addresses must not be the same and it is advisable to change the addresses from the default values. Care should be taken to ensure that in a system with P2 (current loop) and P3 wireless option modules, the P3 wireless address will not conflict with the P2 Modbus address range i.e. in a system with 180 P2 wired devices the P2 Modbus address range will be the address set for P2 Modbus address + 2, therefore the first address available for the P3 wireless Modbus address will be the P2 Modbus address + 3. In a mixed system Option 1 will be the P3 wireless network and Option 2 will be the P2 current loop network.

The FCU distribution bar must be set up correctly to ensure that communication to all devices is possible.

7.6.2   Masterstation Config - Pakscan 2 Current loop option

The master station configuration page is also used for setting up the Pakscan 2 Current Loop option module if one is fitted. Set the loop performance parameters in accordance with site requirements. Make sure the loop speed is compatible with the value of the loop capacitance, see section 2.1.

❑ Set the highest field unit address parameter equal to the actual highest address.

❑ Doubling can be set to 'On' if the loop performance is not fast enough. It has the effect of halving the time to collect data from the field units.

❑ DV Convert should be set to 'On' if analogue position control is being used on the IQ, IQT, Skil or EH actuators on the network.

❑ Data Retain set to 'Off' clears all the field unit data if communication is lost. Some host systems want the data to be retained, in which case set the parameter to 'On'.

❑ Select the desired host database type for each serial communications port and the Ethernet ports for access to the actuators on the current loop. Refer to document PUB059-003 (formerly S171E) for database details. On Hot Standby systems link the alarms if both serial ports go to the same DCS or PLC in a redundant communications configuration.

7.6.3 Masterstation Config - Pakscan 3 Wireless option

If a wireless module is fitted, the master station set up page is also used for setting up the Pakscan 3 Wireless Network. Set the network parameters in accordance with the network settings recommended during the sire survey.

❑ Set the PAN ID and AES key as chosen by the customer.

❑ Set the channel number as determined by the site survey.

❑ Set the lowest FCU address to the lowest address in the range of addresses possible for the wireless module, avoiding overlap of addresses.

❑ Set the number of FCU addresses to the number of field units to be connected to the network.

7.6.4 Host port settings

The physical parameters relating to the serial ports that may be altered are set by accessing the **Host Port** page see section 7.5.18.

The port type is determined by the DIP switch settings on the main chassis behind the PS710 CPU module and the setting is reflected in the message on the screen. The description changes to reflect the settings made. This is particularly useful when determining the settings already in place. In hot standby systems the Cross Connected status of both the serial ports also depends on the settings of the DIP switches behind the Key Switch module on the main chassis.

❑ For each serial port, set the Baud rate and Parity as required. The speed may be varied between 2400 and 115,200 baud, the parity may be Odd, Even, Zero or None.

❑ On hot standby systems the Standby mode will normally be correct, when cross coupled, ports should be Standby Passive.

❑ On hot standby systems the Ethernet port needs to be set Standby Passive if both Ethernet ports are on the same Ethernet highway to the DCS. If there are two routes to the host they may be set Standby Active.

For security, IP Authentication should be set to the IP address of the Modbus TCP host(s). On a private network it is unlikely that authentication will be required.

7.6.5 Network IP address settings

The IP address for web page and Modbus TCP communication is set on the **Network** page.   See section 7.5.22.

The MAC ID for each Pakscan 3 CPU module is unique and fixed at time of manufacture. The IP address and Netmask (subnet mask) can be altered to suit the individual application and match the needs of the network.

Note: When the IP address is changed, the comms link will fail when the new value becomes active in the master station following the master station reboot. The web browser must be restarted and directed to the new IP address.

> *Re-establishing Ethernet Communication with a new IP address:*
> *Because most computers associate a MAC ID to each IP address, it is possible that the computer will not be able to re-establish communication with the master station until the computer has been rebooted.*

(The rest of this page is intentionally blank)

8. MAKING THE SYSTEM WORK

> ## *Always ensure the plant is in a safe condition and all the actuator controls are placed in Local before commencing any commissioning or fault finding on the system.*

8.1 Commissioning the Wired System

The current loop needs to be commissioned to enable the system to locate and identify every actuator. The master station and computer can be used to perform the commissioning. At the time of commissioning the loop, all the actuators must be made available, though they may be locked in 'hand only' control. All field units must have a unique network address.

The 2-wire loop and all the actuators should be connected to the master station, with all the actuators left without power, except for the one furthest from port A. Disconnect the wires from port B and browse to the master station web pages on the computer; go to **System Diagnostics** page – see section 7.5.4.

Select **Option 2 Diagnostics** by clicking on the **diagnostics** button - see section 7.5.7.

Reset the network (current loop) by clicking the **reset network** button. The status information will change and show the configuration stages. Once complete, the actuator furthest from port A should be shown on the Network Map.

Power on the next nearest actuator to port A and reset the network again. This actuator should appear on the list. Continue to power on the actuators and reset the network working back towards port A until all the actuators are connected and appear on the map.

Now connect the port B wires and disconnect the port A wires. Reset the network and check that all the actuators are still on the map. Having verified the loop wiring and the connection of all the actuators in both directions; finally reconnect the port A wires, reset the loop and all the actuators will be ready for control.

The commissioning sequence can also be carried out using the master station HMI screens using the Option Module 2 Diagnostics. This is a 2 page menu and contains similar information to the web page.

Once the system is working with actuators connected and no loopbacks present, the diagnostic and control pages can all be used.

See also the Quick start guide document: PUB059-026.

8.2   Commissioning the Wireless network

When an actuator with a wireless module is shipped from the factory, it will be set with default values for its PAN ID (Private Area Network Identifier), Channel number, AES (Advanced Encryption Standard) Key and Address.

These default values are:
- PAN ID   DA 15
- Channel   22
- AES key   0F 15 71 C9 47 D9 E8 59 0C B7 AD D6 AF 7F 67 98
- Actuator wireless module Address   300

These settings can be changed at the actuator using an infra-red setting tool or when communication has been established with the master station using the master station web pages / HMI. The actuator's wireless address cannot be set using the master station and must be set using the infra-red setting tool; each actuator must have a unique address.

It is best practice to setup the network such that the lower numbered devices are closest to the P3W coordinator. This is because the reset of the network has been set up to be staggered, allowing those devices nearest the P3W coordinator to join first, and more remote to join later.

At the start of commissioning the wireless network, leave all the wireless actuator modules powered down, power up the master station and set the desired PAN ID and AES key. These are to be decided by the customer. Set the channel number to the one determined during the site survey. It is recommended that at least the PAN ID is modified from the default setting. This will simplify commissioning by ensuring that actuator modules only appear on the network when the correct PAN ID has been set locally in them.

The PAN ID, AES key and channel number of the network can be set in the master station using the HMI screen or using the master station config web page.

Once the master station has been set up, the wireless actuators can be powered up and set up with the infra-red setting tool. If the master station settings are different from the default (as recommended) none of the modules will appear at the master station. At the actuator, the address should be set first then the PAN ID and the AES key. Refer to PUB002-008 for details of how to find the settings.

When these have been set up correctly, the new device will appear on the master station FCU menu page. It is preferable to set up the actuators one at a time, starting with those devices closest to the P3W coordinator and working outwards to the unit furthest away.

See also the wireless quick start guide: PUB059-004.

8.3 Monitoring and Controlling the Actuators from the HMI or web pages

The web browser and HMI include the capability to control and monitor all the actuators on the Pakscan network. This assumes the actuators are in remote mode and correct permissions have been set up in the master station config web page – see section 7.5.17.

Using the web pages, go to **FCU Menu** to open the page showing all the connected actuators and their status – see section 7.5.11.

This screen lists the FCUs in address order, their type and current condition. The **FCU Control** button will bring up the page showing the information in more detail – see sections 7.5.12 onwards.

The actuator can be moved by the **Open** and **Close** buttons and any alarms present can be displayed by clicking **Show Alarms**. The page will automatically refresh if the valve is moved. The buttons at the top of the page can be used to move to the next or previous actuator on the network.

Control and monitoring can also be achieved using the master station keypad and screen. Select Field Unit Menu and the connected field units will appear in turn.
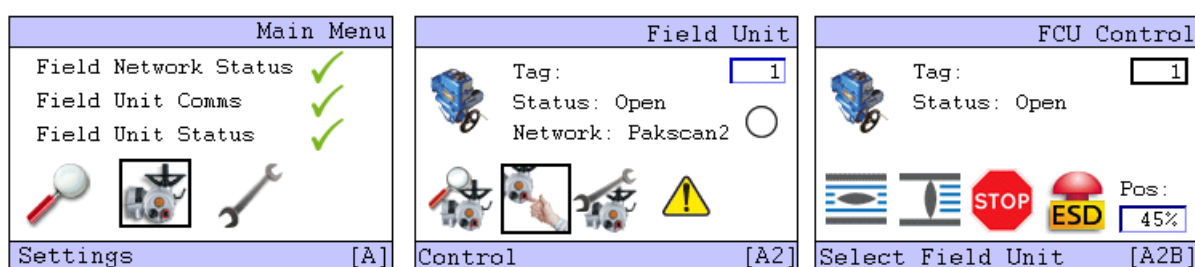

Fig 83:   *Detailed Actuator Condition HMI pages*

Once the system is running correctly, make a note of all the settings and field unit parameters for future reference.

The Pakscan Current Loop network and associated actuators will now be available for the host DCS or PLC to control and monitor the plant.

(The rest of this page is intentionally blank)

9. LONG TERM DATALOGGER (LTD)

P3 master stations, delivered after May 2011, will contain a Long Term Datalogger (LTD) module. In the case of the hot standby master station, the LTD and the key switch are contained in the same module. For a single channel unit the module will be in the middle slot, which previously contained a blank module.

Fig 84:   Hot standby master station with Long Term Datalogger (LTD)

The LTD independently captures and stores all messages directed to the master station from the host connections and all the messages that occur between modules connected on the master station back plane. This information includes host Modbus commands and changes in field unit status information.

Information is stored on a microSDHC (Secure Digital High Capacity) memory card located at the front of the module for easy extraction. A 4 GByte memory card is supplied as standard. One file is created on the memory card for each day. The size of each file is dependent on how often the master station is accessed by the host. In practice, each day file is generally about 1 MByte.

The data is viewed on an application called LTD Viewer, which can be downloaded from the Rotork web site.   A memory card reader is required to connect the memory card to a computer to enable the data to be viewed.

The information monitored and recorded by the LTD can be saved for future reference and gives total visibility of every command and status update for every Pakscan device on the network. This information can be used by site engineers as part of their asset management function.
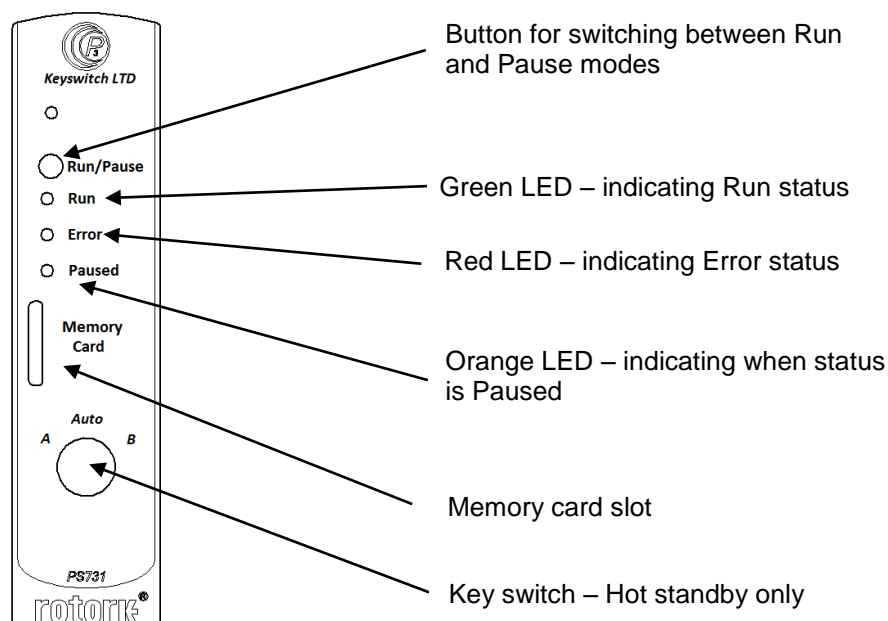
Fig 85:   Front view of the LTD

9.1 Removing the memory card and copying data

Before removing the memory card it is necessary to stop the LTD from logging. Press the 'Run / Pause' button once; the orange 'Paused' LED will start flashing. Once it has stopped flashing and is solid orange, it is OK to remove the memory card. This is achieved by pressing lightly on the card then letting go - the card should pop out enough for you to grab it. The card can then be placed in a card reader or USB carrier for extraction of the files into a computer. The card will contain the LTD Viewer software and also a folder with data inside:
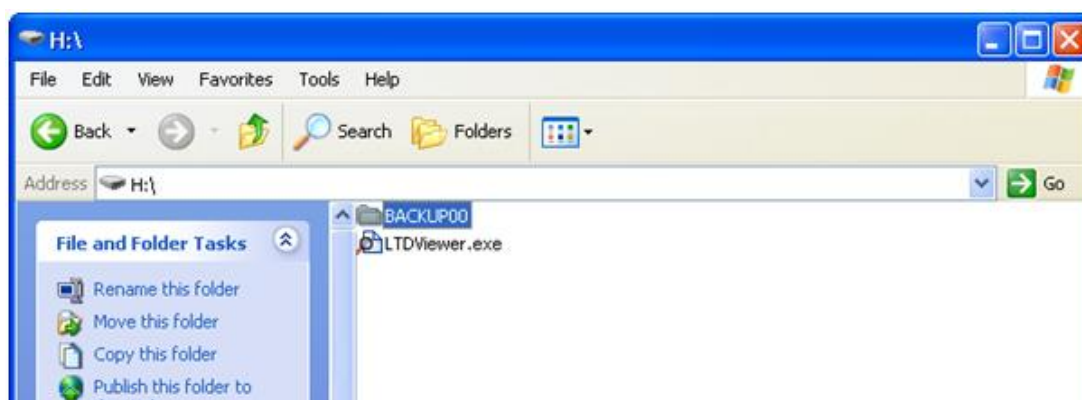
Inside the data folder will be a number of files containing the logged data, these files are not readable using a text file reader as they are in a Binary format.
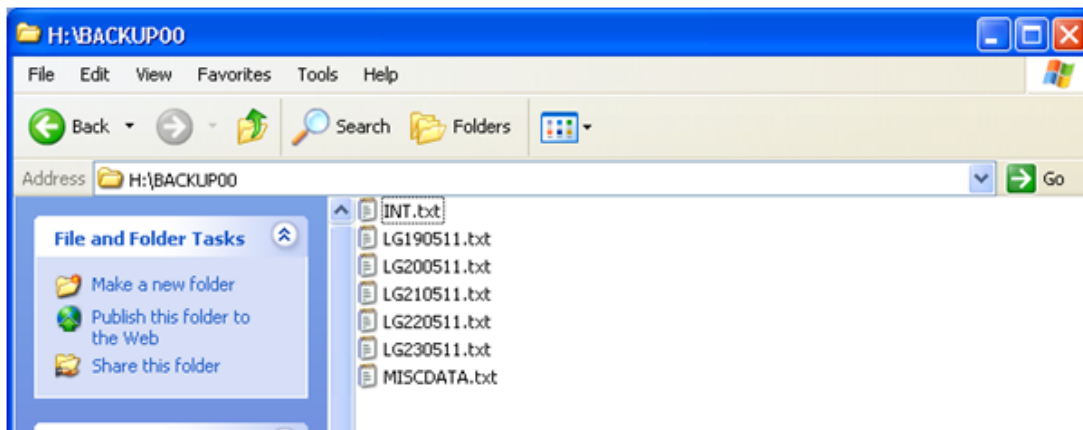
Each file is date stamped i.e. LG210511 is from 21st May 2011.

The complete data folder and the viewer software should be copied into a computer for viewing. The data folder can be renamed appropriately. Once the files have been copied from the memory card it can be replaced back into the LTD module. It should be replaced in the same orientation that it was removed (metal contacts to the left), gently push into place – it will click to indicate correct placement. If the card remains in place when pressure is removed then it has been successfully replaced.
Once the memory card is back in place, the 'Run / Paused' button should be pressed once again and the datalogger will continue to log – the Run LED will flash Green.

> ***It is important to handle the memory card gently when removing and placing the card in the module.***

9.2 Viewing the data with the LTD Viewer software

The LTD Viewer software is started by double clicking the icon.

LTDViewer.exe
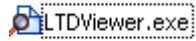
The software will open with this following page:
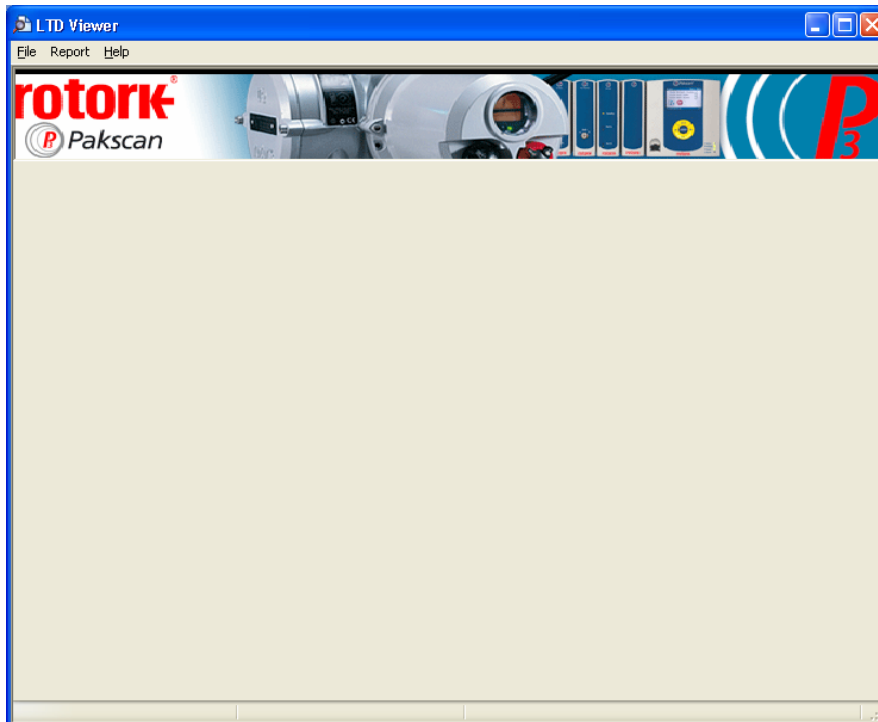
Click on File, then 'Select Folder', navigate to the folder containing the datalogger data.
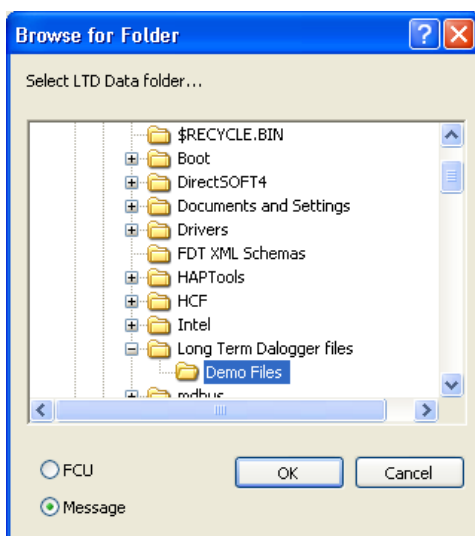
Using the radio button select either 'Message' or 'FCU' to view the all the messages recorded by the LTD or the FCU data.

9.2.1 Messages

When 'Message' is selected the following page will be displayed:
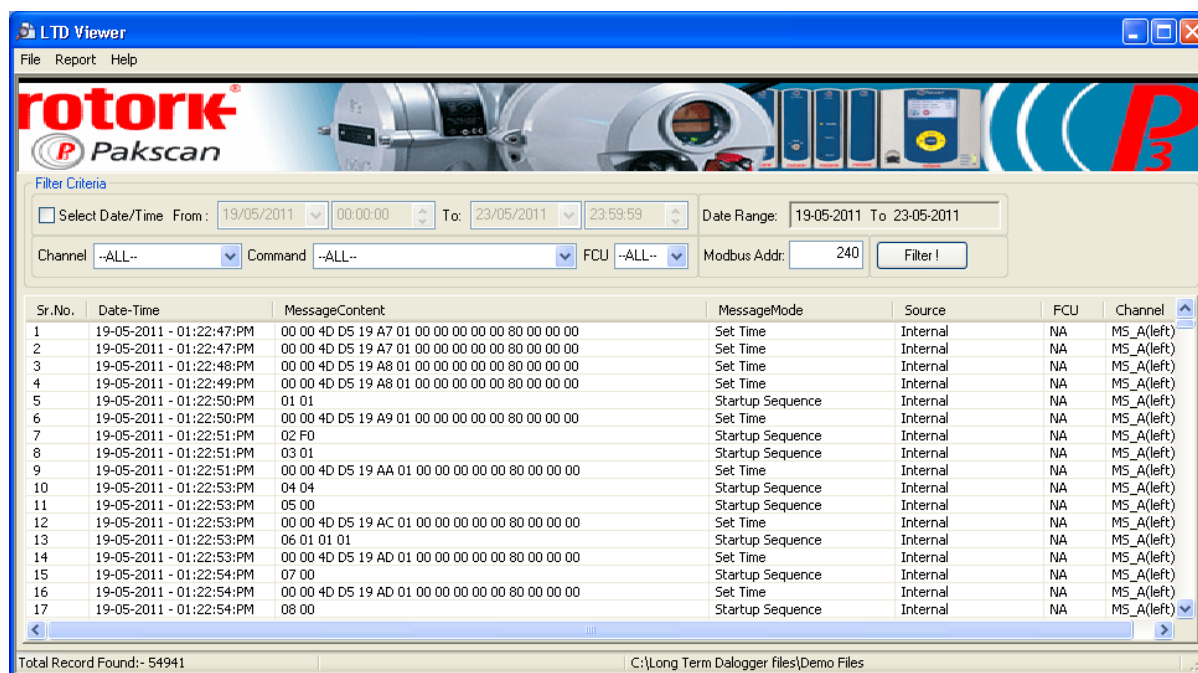
From here the user is able to filter the messages in the datalogger. The datalogger records all messages that appear on the back plane of the master station including messages between the CPU module and the option card and in a hot standby system, the messages that are passed between each master.

The Date Range field shows the range of data that is held in the files. In this example we are able to see data in the datalogger between the dates of 19th May – 23rd May 2011.

9.2.2 Messages – Filter Options

It is possible to filter the messages to pinpoint the exact view you require. After each selection it is necessary to press the 'Filter !' button for the selected filter to take effect.

By selecting the 'Select Date / Time' check box, the user is able to restrict the data that is viewed between 2 dates. The date range is changed using the drop-down boxes and to update the data the filter button must be pressed:
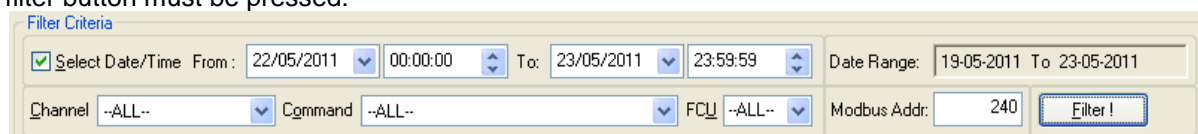
In a hot standby system the user can filter on the A or the B side of the master station to only view data sent to the side selected:

The user can filter on a particular command or event:

The data can be filtered on the FCU address using the FCU drop-down box.

The data can be filtered on the Modbus address:

For example: to see all Modbus messages for all the FCUs on the A side of a hot standby master with Modbus address 240 between 19th May and 23rd May, the following filter would be set up:

Example data:

Sr.No.	Date-Time	MessageContent	MessageMode	Source	FCU	Channel
1	20-05-2011 - 07:44:08:AM	F0 10 0C 7C 00 01 02 00 01 A9 F8	Modbus - Open	WebPage (Generic)	1	MS_A(left)
2	20-05-2011 - 07:44:12:AM	F0 10 0C B8 00 01 02 00 04 79 7F	Modbus - Stop	WebPage (Generic)	1	MS_A(left)
3	20-05-2011 - 07:44:13:AM	F0 10 0C F4 00 01 02 00 02 F7 71	Modbus - Close	WebPage (Generic)	1	MS_A(left)
4	20-05-2011 - 07:44:16:AM	F0 10 0C B8 00 01 02 00 04 79 7F	Modbus - Stop	WebPage (Generic)	1	MS_A(left)

The data is displayed in a number of columns with the following headings:

Sr.No.	Date-Time	MessageContent	MessageMode	Source	FCU	Channel

❑ Sr.No: this is the serial number of the information within the display.

❑ Date – Time: Date and Time of the event / message.

❑ MessageContent: shows the complete message content i.e. complete Modbus message.

❑ MessageMode: shows the type of message and decodes it where possible.

❑ Source: indicates where the message came from and, for Modbus, which database is being used.

❑ FCU: The address of the FCU which the message is aimed for.

❑ Channel: indicates which side of the master station the message appear on.

There is a lot of internal status data passed on the back plane which is decoded by the LTDViewer. For example, in the command drop-down box, selection of Parameter Block Transfer and selecting 'Filter !' will enable these internal status messages to be seen. A lot of useful information is in there including status of the standby master station.

In this example we can see the position of one of the FCUs being reported.

9.2.3   Reports

If the user requires a report of the data in CSV / xls or html format, select the 'Report' menu item and then 'Messages'.
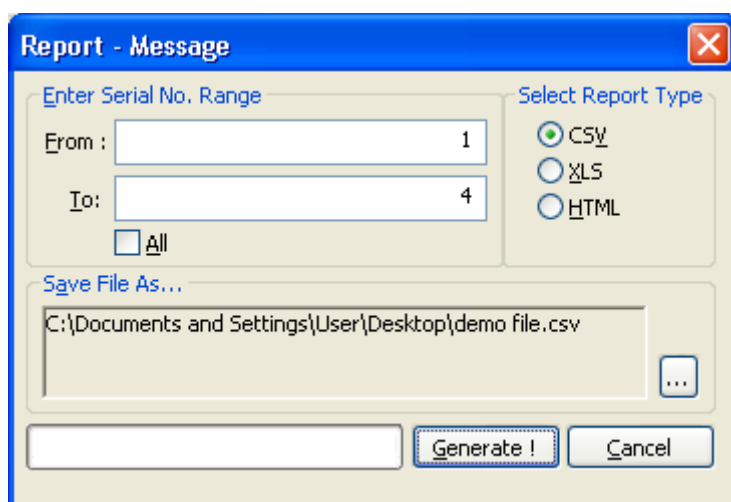
In the message box that appears select the range of data that is required – the range field uses the serial numbers i.e. in the example above there are only 4 lines of data so the serial numbers for those are 1 to 4. Click the 'All' radio button for all the data.

Select the format required and select a file name.

Select the 'Generate !' button and a pop-up box will appear to indicate success of generation.

The data can then be viewed in the chosen format i.e. CSV:

9.2.4   FCU Data

Select the 'FCU' radio button and then 'OK' to view the FCU data.
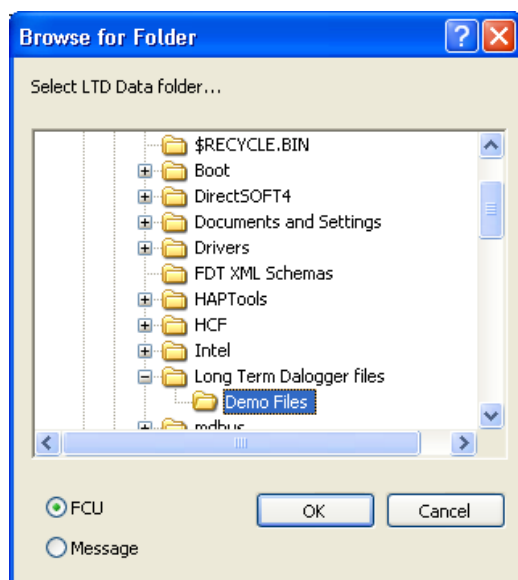
The FCU data page shows which devices are connected to the network and to which side of the master station they are connected. Here we have 2 devices; one is an IQT at address 1 and the other an IQ analogue card at address 61. Both are connected to the master CPU on the left hand side of the master station:
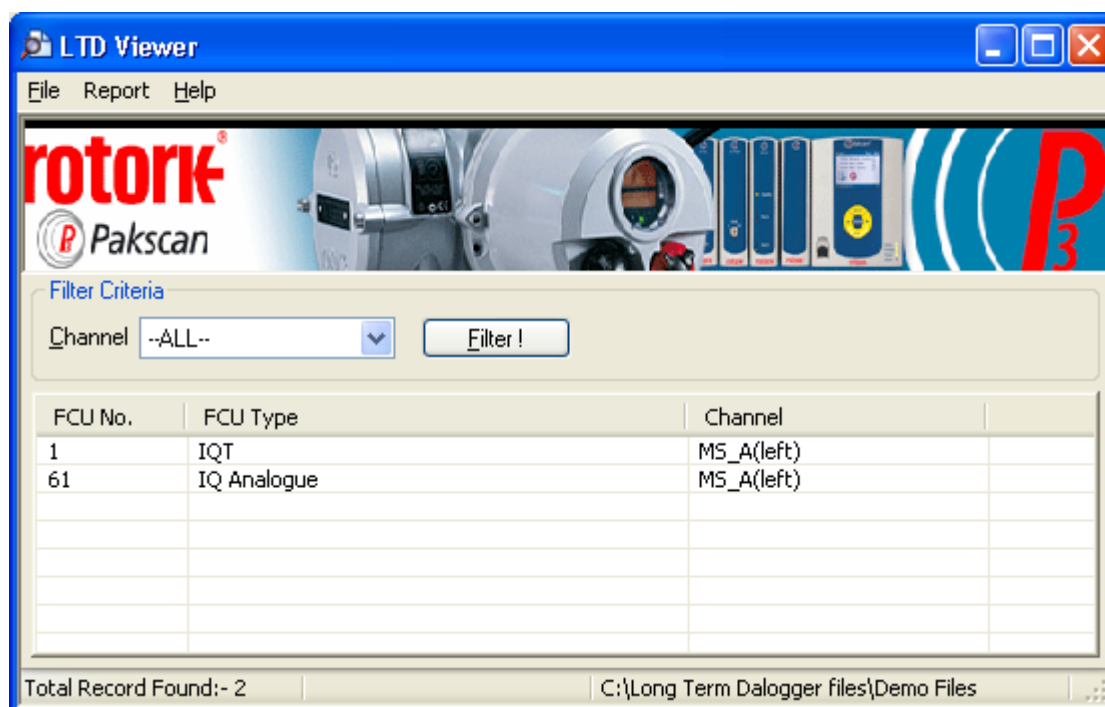
10. RESETTING THE MASTER STATION TO DEFAULT VALUES

> ### *It is important that anti-static precautions are observed*
> ### *while performing this operation.*

This section details how to reset a P3 master station CPU module to default settings using the hardwired link which is on a circuit board in the CPU.

❑ If the CPU module is part of a hot standby unit and control of the network is required during this process, use the key switch to force the 'other' side of the master station to be the primary unit.

❑ Isolate the power to the master CPU module that requires defaulting.

❑ Remove all connectors plugged into the CPU module.

❑ Remove the CPU module. For this operation the module removal tool supplied with the master station should be used to detach the master station from the back plane. The module is then removed by pulling it down and out from the back plane, then unhooking the hooks at the base of the module from the back plane.

❑ When removed, the default link is visible from the underside of the module, shown circled red in the picture below:

❑ The 'handbag' link will be across the 2 pins (of the 3 pin connector) furthest from the edge of the board.

❑ Carefully move the handbag link to the position shown below, such that it is linking the 2 pins closest to the edge of the board:

❑ Replace the module on the master station back plane and power up the module. Note: for a hot standby system, if the copy settings have been enabled, when you replace the module you may find that the module re-boots more than once whilst the settings are copied across from the primary unit. Leave the unit powered-on for at least 5 minutes.

❑ Isolate the power to the same master module again.

❑ Remove the master CPU module and return the link to the standard position, as shown below – **It is imperative that this is done:**
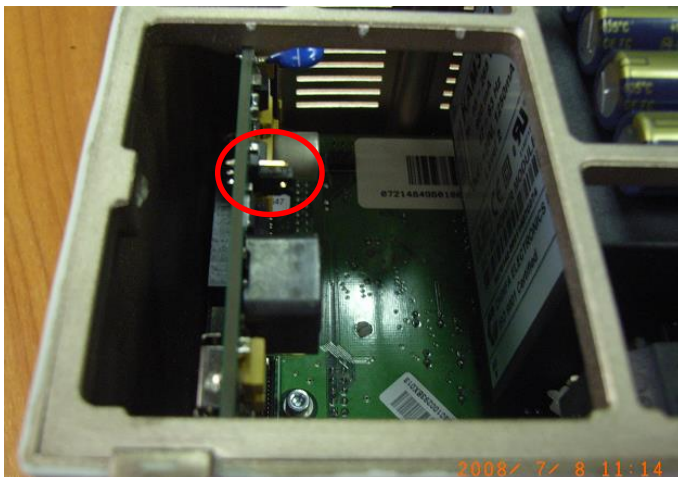
❑ Replace the CPU module on the master station backplane and power up the module.

❑ If the system is a hot standby, reset the switch to the auto position.

11. REPLACING THE P3 MASTER STATION BATTERY

> ***It is important that anti-static precautions are observed
> while performing this operation.***

The Pakscan P3 master station has a small battery fitted in each PS710 CPU Module. This battery maintains the internal clock. The battery type is a CR1225, a 3 volt coin cell, and should be replaced with a similar type of cell. Take anti-static precautions when attempting this procedure.

You can check the voltage of the battery by removing the PS710 CPU Module from the master station backplane. Follow the procedure in Section 4.1. on page 31, to remove the module.

Then use a multimeter to measure the voltage between the battery holder (positive) and the end contact of J13 (negative), as shown in the picture below.

The battery should last about two years and should be replaced after this time as a matter of course. It should also be replaced if the measured voltage is less than 2.7 volts.

If the battery needs replacing, remove the seven cross-head countersunk screws and pull out the PCB support frame. Next, pull out the CPU PCB. Now carefully push out the battery and replace with a similar new part.

Replace the CPU PCB into the socket on the front panel PCB and carefully refit the support frame. Replace the seven screws and refit the CPU Module to the master station backplane assembly. Check and reset the clock if necessary in the CPU Module. Finally, dispose of the discharged battery in a suitable place.

GENERAL SAFETY INFORMATION

❑ **Health and Safety**

This manual is produced to enable a competent user to install and operate a P3 Pakscan Master Station and its associated equipment. Only persons competent by virtue of their training or experience should install and maintain this equipment.

Work undertaken must be carried out in accordance with the instructions in this and any other relevant manuals. The user and those persons working on this equipment should be familiar with their responsibilities under any statutory provisions relating to the Health and Safety of their workplace.

Due consideration of additional hazards should be taken when using the P3 Pakscan master station and it associated equipment with other equipment.

The electrical installation, maintenance and use of the P3 Pakscan Master Station and its associated equipment should be carried out in accordance with the National Legislation and Statutory Provisions relating to the safe use of this equipment, applicable to the site of installation.

For the UK: Electricity at Work Regulations 1989 and the guidance given in the applicable edition of the 'IEE Wiring Regulations' should be applied. Also the user should be fully aware of his duties under the Health and Safety Act 1974. For the USA: NFPA70, National Electrical Code® is applicable.

Care should be taken to ensure that the voltages or currents do not exceed those specified for the Master station and that the correct polarity is applied. Only the following fuse types can be used in the P3W Coordinator, P3W Repeater and P3W WMA

> Bussman TDC11, Anti-Surge Glass, 250mA (Power PCB, P3W Repeater-AC & P3W WMA-AC only)
> Bel Type: 5MF 500R, 500mA, 250V (Field Control Unit PCB)
> Schurter Type: 0034.1513, 500mA, 250V (Field Control Unit PCB)
> Littlefuse Type: 216.500P, 500mA, 250V (Field Control Unit PCB)
> Littlefuse Type: 217.500P, 500mA, 250V (Field Control Unit PCB)

Galvanically isolated input or output signals circuits are provided by certain products. A competent person must decide upon any earthing arrangements for such circuits and users should regard them as carrying a hazardous live voltage, unless they are earthed locally.

The mechanical installation should be carried out as outlined in this manual and also in accordance with any relevant codes of practice.

❑ **Hazardous Area**

The P3W Coordinator, P3W Repeater and P3W WMA modules can be supplied certified for use in a hazardous area. If the modules are for use in a hazardous area, then the relevant hazardous area marking will be stated on the nameplate and the modules should only be installed in hazardous area locations compatible with the gas and dust groups stated on the nameplate.

The P3W Coordinator, P3W Repeater and P3W WMA has the following hazardous area approvals

USA Hazardous Area

Class I, Division 1, Groups C & D, T4
Class II, Division 1, Groups E, F & G, T4
Tamb -40°C to +60°C, Type 6.

Class I, Division 1, Groups B, C & D, T4
Class II, Division 1, Groups E, F & G, T4
Tamb -40°C to +60°C, Type 6.

❑ **Batteries**

Batteries must not be short circuited, or disposed of by burning. They must not be opened, punctured or crushed. Large batteries should only be used in well ventilated places. Their cases are generally ABS plastic resin and as such should be cleaned only with a damp cloth and not exposed to organic solvents.

❑ **Electromagnetic Compatibility**

To ensure conformance to the EC Directive 2004/108/EC, installation should adopt the following cable arrangements:

All digital data cables and all analogue signal cables operating at or below 50 Volts should be shielded either by braid, armouring or metal conduit. Such shields should be earthed at the point of entry to the product enclosure using cable glands designed for this purpose. If, for the avoidance of ground loops, it is not possible to earth these shields locally at low frequencies, they should nevertheless be so earthed via a capacitor effective at radio frequencies. If this technique is adopted, it is the users' responsibility to ensure that EMC is not compromised. A single shield may be shared by any number of analogue signal cables.

All Ethernet cables must be screened and of good quality. Many screened Ethernet cables of low quality have questionable screening efficacy.

❑ **Functional Reliability**

Reliability predictions, (including failure mode and effect analysis), are calculated by Rotork using statistical methods and the resulting figures should only be used for statistical purposes. These predictions are only valid if the maintenance procedures and maintenance intervals stated in Rotork documentation are observed.

❑ **Environmental**

Products should only be operated within the environment specified on the product data sheet. Take care not to obstruct ventilation paths.

In the event of ingress of any fluid or spray, products should be immediately switched off, and cleaned and dried by a competent person before re-use.

❑ **Chemical**

Specific hazards will be the subject of product data. As a matter of good working practice, oral contact should be avoided.

❑ **Independently Certified Products**

Such products must not be modified in any way by the user, and must be applied, operated and maintained in accordance with the relevant standards, certificates and reports.

❑ **Product Data Sheets**

These should be checked for information which supplements or replaces that given above.

❑ **FCC Warning Statement**
This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:

      (1) This device may not cause harmful interference, and
      (2) This device must accept any interference received, including interference that
      may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Contains Radio Module FCC ID: ZK4P3W-001.

❑ Power should always be removed from the master station before attempting to remove any modules from the backplane.

Publication formerly known as S720E

rotork

http://www.rotork.com

Rotork reserves the right to amend and change specifications without prior notice.

Published data may be subject to change. Check web site for latest version.

UK Head Office

Rotork Controls Ltd
Bath
England
BA1 3JQ

Tel: +44 (0) 1225 733 200
Fax: +44 (0) 1225 333 467
email: mail@rotork.co.uk

USA Head Office

Rotork Controls Inc
675 Mile Crossing Blvd
Rochester
New York 14624
USA

Tel: +1 585 247 2304
Fax: +1 585 247 2308
email: info@rotork.com