Honeywell

Experion PKS

Honeywell Modbus TCP Firewall User's Guide

EPDOC-X162-en-431A
February 2015

Release 431

Document	Release	Issue	Date
EPDOC-X162-en-431A	431	0	February 2015

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Contents

1 About This Document

Revision history

Revision	Date	Description
A	February 2015	Initial release of document.

2 Introduction

Related topics

"About the Honeywell Modbus TCP Firewalls" on page 8

"Modbus TCP Firewall Certification" on page 11

"Modbus TCP Firewall in the Experion Network" on page 13

2.1 About the Honeywell Modbus TCP Firewalls

The Honeywell Modbus TCP Firewall (HMTF) and Honeywell Modus Read-Only Firewall (HMRF) are security appliances designed specifically for use in an industrial control environment. These devices, when deployed between a Honeywell Experion system and MODBUS/TCP devices, protect the Experion system. For R301 releases the firewalls support detailed displays and alarming in Station while allowing SCADA communication over Modbus/TCP. For R310 releases, the firewalls add support for Modbus/TCP communication over Honeywell Peer Control Data Interface (PCDI). The terms 'Modbus TCP Firewall ' and its variations used throughout this document refer to both the HMTF and the HMRF. Any differences in behavior or operation between the two devices are specifically noted where applicable.

2.1.1 Modbus TCP Firewall pre-configuration

To protect the Experion system, the Modbus TCP Firewalls are preconfigured to block unnecessary traffic on both its secured and unsecured ports. The HMTF allows MODBUS/TCP traffic through on TCP Port 502, which is the only port allowed for the Experion system connection. The HMRF only allows read-only MODBUS/TCP traffic through on TCP Port 502. All Modbus write function codes are blocked by the HMRF. They further ensure that only MODBUS Master Command traffic is allowed from the Experion system, blocking any unsolicited traffic from MODBUS devices. Additionally, the Modbus TCP Firewall only allows Ethernet management traffic that is necessary for keeping the network operational, and limits that traffic to a rate of 1mbit per second.

Attention

The HMRF (Read-Only Firewall) blocks all Modbus write functions codes. When using an HMRF, Modbus write function codes can be detrimental to the control system. If an HMRF is utilized, Modbus write functions codes should not be present in the control strategy. The intent to use the HMRF to detect and block write function codes should be strictly avoided. The expected response from blocked write function codes is a timeout. Timeouts can cause delays, retries and device/FTE failovers. These conditions adversely affect system performance. It is especially important when adding new function blocks to running strategies to ensure they DO NOT have write function codes. This can cause the failure of the operating functionality due to the timeouts. In addition, when configuring a PCDI block, it is strongly recommended that all write function codes remain disabled in the Slave Configuration tab.

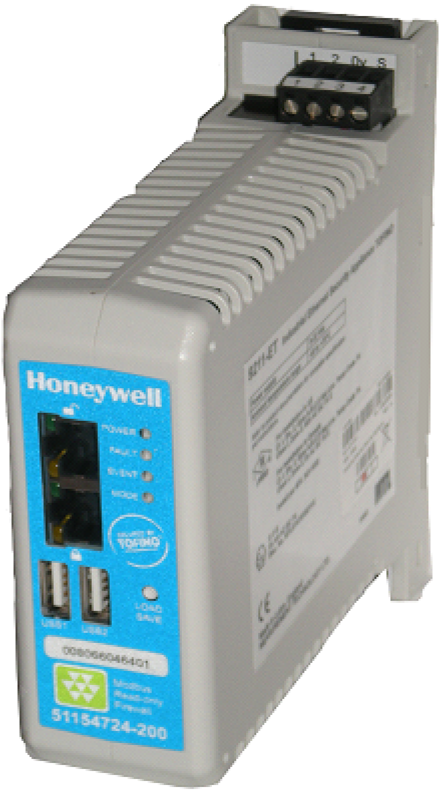


Figure 1: Honeywell Modbus Read-Only Firewall (HMRF) - Honeywell Modbus TCP Firewall (HMTF)

1 2 0v S
Honeywell
Pwr
Fault
Event
Mode
BYRES security enabled
USB1
USB2
00806604642E
0000118D9910
Modbus TCP Firewall
51154724-100
9211-ET Industrial Ethernet Security Appliance TOFINO
Made in Luton, England
MEASUREMENT TECHNOLOGY LTD.

2.2 Modbus TCP Firewall Certification

Related topics

"Europe" on page 11
"USA" on page 11
"Canada" on page 12

2.2.1 Europe

Authority	Standard	Approved for	Certificate No.
MTL	EN 60079-15:2005	Ex II 3G Ex nA nC IIC T4 -40°C ≤ Ta ≤ +70°C.	MTL07ATEX9211X
Conditions for safe use 1. *The apparatus must be installed in an enclosure or an environment that provides a degree of protection not less than IP54.* 2. *The module must not be inserted or removed unless either:* • *the area in which the apparatus is installed is known to be non-hazardous, or* • *the circuit to which it is connected has been de-energized.* 3. The 9-32V supply that provides the input to the module must be derived from a regulated power supply complying with the requirements of European Community Directives.			

2.2.2 USA

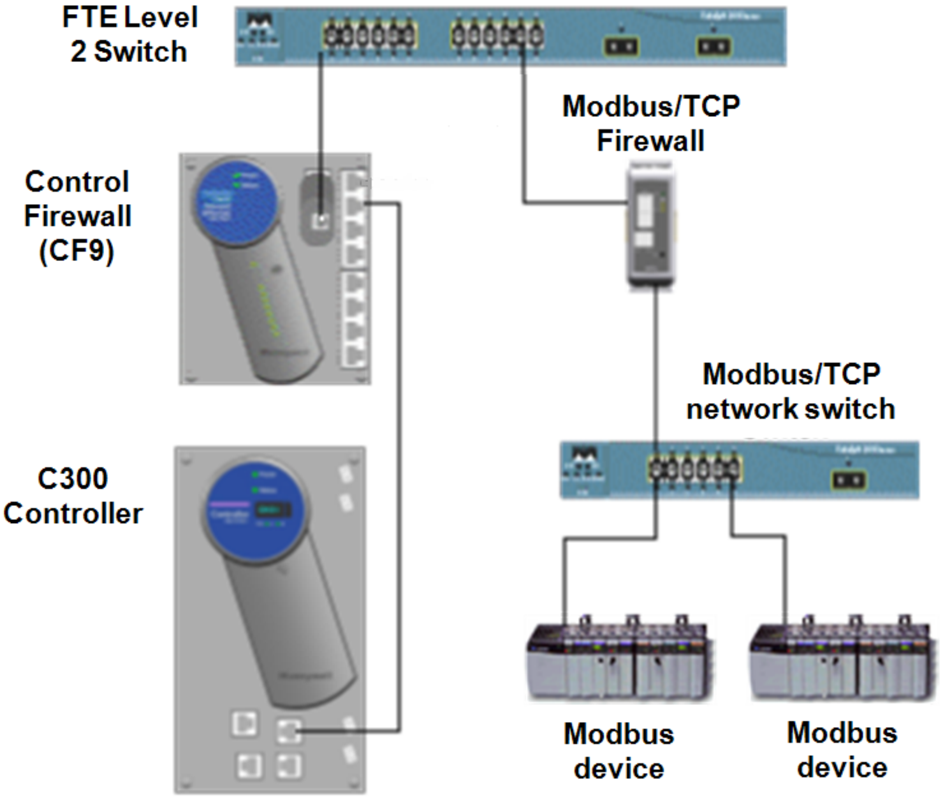
Authority	Standard	Approved for	Certificate No.
FM	FM 3600, FM 3611 FM 3810	NI/1/2/ABCD/T4 Ta = 70°C 1/2/AEx nC/IIC/T4 Ta = 70°C	3029914
Equipment Ratings: Non-incendive for Class I, Division 2, Groups A, B, C and D; Zone 2, AEx nC IIC T4 Ta =70°C; in accordance with Control Drawing No. SCI-1032, indoor hazardous (classified) locations.			
Special Condition of Use: 1. *In Class I, Division 2 installations, the subject equipment shall be mounted within a tool-secured enclosure which is capable of accepting one or more of the Class I, Division 2 wiring methods specified in the National Electrical Code (ANSI/NFPA 70).* 2. *In Class I, Zone 2 installations, the subject equipment shall be mounted within a tool-secured enclosure which is capable of accepting one or more of the Class I, Zone 2 wiring methods specified in the National Electrical Code (ANSI/NFPA 70). Where installed in outdoor or potentially wet locations, the enclosure shall, at a minimum, meet the requirements of IP54. Where installed in dry indoor locations, the enclosure shall, at a minimum, meet the requirements of IP4X.*			

2.2.3 Canada

<table>
<tr><th>Authority</th><th>Standard</th><th>Approved for</th><th>Certificate No.</th></tr>
<tr><td>FM</td><td>CAN/CSA E60079-0
CAN/CSA E60079-15
C22.2 No. 1010-1</td><td>IPA/1/2/ABCD/T4 Ta = 70°C
1/2/Ex nL/IIC/T4 Ta = 70°C</td><td>3029914C</td></tr>
<tr><td colspan="4">Equipment Ratings: Non-sparking for Class I, Division 2, Groups A, B, C and D; Zone 2, Ex nL IIC T4 Ta =70°C; in accordance with Control Drawing No. SCI-1032, hazardous indoor locations.</td></tr>
<tr><td colspan="4"><i>Special Condition of Use</i>:
1. <i>In Class I, Division 2 installations, the subject equipment shall be mounted within a tool secured enclosure which is capable of accepting one or more of the Class I, Division 2 wiring methods specified in the Canadian Electrical Code (C22.2).</i>
2. <i>In Class I, Zone 2 installations, the subject equipment shall be mounted within a tool-secured enclosure which is capable of accepting one or more of the Class I, Zone 2 wiring methods specified in the Canadian Electrical Code (C22. 1). Where installed in outdoor or potentially wet locations, the enclosure shall, at a minimum, meet the requirements of IP54. Where installed in dry indoor locations, the enclosure shall, at a minimum, meet the requirements of IP4X.</i>
3. <i>The user shall take necessary measures to ensure that the supply voltage transients do not exceed 45V.</i>
4. <i>The user shall ensure that the field wiring insulation temperature is rated for 70°C.</i>
5. <i>The material used in the construction of the final enclosure, shall not contain, by mass, more than 7.5% magnesium.</i>
6. <i>It is the responsibility of the manufacturer to provide warning markings in French where required by local jurisdictions.</i></td></tr>
</table>

2.3 Modbus TCP Firewall in the Experion Network

The Modbus TCP Firewall can only connect to the Experion network through a Cisco Level 2 switch.



2.3.1 Connecting to a Cisco switch

Connect the protected side of the Modbus TCP Firewall to Level-2 FTE switch or dedicated non-FTE switch.

- The interfacing switch port configuration must be changed to be auto-speed/auto-duplex.
- When connecting to a Level-2 FTE switch, the interfacing port configuration must be changed from the configuration template.

When Modbus devices connect to a Modbus TCP Firewall through the switch, only one level of switch is allowed. No switch cascading is allowed under a Modbus Firewall.

Honeywell recommends all the ports of the downstream Modbus switch in auto-speed/auto-duplex.

3 Installing the Modbus TCP Firewall

Related topics

3.1 Preparing for installation

Unpacking

Unpack the Modbus TCP Firewall and check it for damage. Do not use any parts that show evidence of damage.

Tools and Equipment

To install the Modbus TCP Firewall, you need:

- A 3mm straight blade screwdriver
- 9…32V DC supply with 350mA current (@24V) per firewall. A second (redundant) supply is optional. (Note: 22V DC minimum is required for 18V power fail detection option)
- Wire for DC power & power-fail connections
- Two ScTP Cat5, Cat5e or Cat6 cables to connect the Modbus TCP Firewall between the network and the equipment being protected
- A suitable 35mm DIN rail location to mount the firewall (optional - see mounting details)

3.2 Mounting the Modbus TCP Firewall

Use the following procedure to mount the firewall.

1 At the back of the firewall, push out the mounting clips - top and bottom.

2 Press the firewall firmly onto the DIN rail and push mounting clips back in. Check that the firewall grips the rail securely.

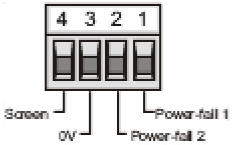
Note: An alternative fixing method is to use M4 screws through the holes in the clips (152mm between canters - see diagram) for mounting the firewall to a panel.

3 Record the ID number (see label) & the installation location for future reference.

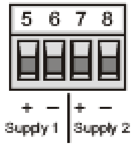
3.3 Wiring for DC Power

Note: These two plugs use cage-clamp screw terminals to accept a stripped wire, ranging in size from 24 to 12 AWG (0.2 - 2.5mm2).

One or two DC power supplies may be connected to the Modbus TCP Firewall using the four-position connector plug (5-8) at the bottom of the Modbus TCP Firewall. Two power supplies will not share the current; the higher voltage supply will take the load. Power fail signals from the supplies may be used by connecting them to the connector plug (pins 1 & 2) at the top of the firewall device - ground returns go to pin 3.



Power-Fail Connector



Power Connector

3.4 Starting up the Modbus TCP Firewall

Power on the firewall and allow it to complete its startup sequence *before you add it to the network*. The Modbus TCP Firewall will not pass network traffic until it has executed its startup sequence. At power ON, all four LED indicators light up. At the end of the startup sequence, (after approximately 1 minute) the Fault and Event LED indicators will be extinguished to show the sequence is complete.

3.5 Adding the Modbus TCP Firewall to the Network

Use the information in this section to add the Modbus TCP Firewall to the network. This assumes you have already started up the firewall and allowed it to complete its startup sequence.

3.5.1 Network requirements

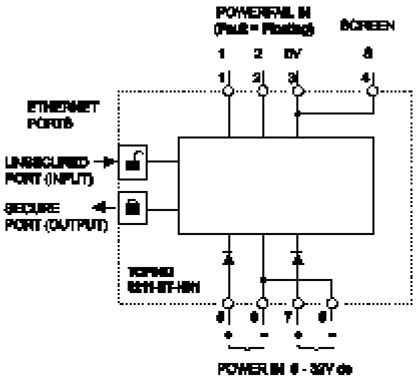
The following table summarizes the requirements for adding a Modbus TCP Firewall to the network.

Requirement	Further information
To connect the Modbus Firewall to the Modbus Device network	
Use the unsecured Modbus TCP Firewall port.	Connects to a Modbus device network switch or, less commonly, directly to a Modbus device.
If connecting to a Modbus device level switch, configure it correctly.	Have all the ports in auto-speed/auto-duplex.
Configure each switch to prevent loops from causing network storms	If the switch is capable, make sure of enabling the spanning-tree protection. For a Cisco switch, add the following command to all non-uplink ports: spanning-tree bpduguard enabled
To connect the Modbus Firewall to the Experion system	
Use the secured Modbus TCP Firewall port.	Connects to a Level 2 switch.
Verify that Modbus devices use a static IP address	The firewall blocks downstream communication, including DHCP.
All Modbus/TCP traffic must communicate on TCP Port 502.	This is preconfigured.
If connecting to a Level 2 switch, configure it correctly.	Use an uplink or PC switch port with the speed and duplex settings configured to auto. Use 100/full port setting for HMRF.

3.5.2 Connecting the firewall to the network

Note: The firewall must have completed its startup before any network connections are made.

1 Connect an RJ45 patch cable from the 'Unsecured ' Modbus TCP Firewall port (🔓) to an uplink port on the Modbus device network switch or directly to a Modbus device.



2 Connect an RJ45 patch cable from the 'Secure ' Modbus TCP Firewall port (🔒) to the Level 2 switch to allow connection to the Honeywell Experion system.

3 Check that the yellow 'Link activity ' light is flashing on both of the network sockets to show network traffic. The green 'Speed ' light comes on if the link is operating at 100Mb/s.

3.6 Updating firmware or configuration information

Use the information in this section to update the firewall's firmware or its configuration. While you are performing an update, you can't see any device that is downstream of the Modbus TCP Firewall.

3.6.1 About firmware and configuration files

To obtain the firmware and configuration files, contact an authorized Honeywell representative who can help you get the files from Honeywell Online Support.

You can determine the firmware version currently on the Modbus TCP Firewall by viewing the FPGA Revision information on the Status Display. See Section “Modbus TCP Firewall faceplate and detail displays” on page 26, ' “Modbus TCP Firewall faceplate and detail displays” on page 26. '

3.6.2 Updating configuration or firmware

The USB Load function loads files containing firmware or configuration updates from a USB storage device.

1 Ensure the Modbus TCP Firewall has been powered for at least one minute.

2 Insert the USB storage device containing the prepared data into one of its USB ports.

3 Press and hold the Config button for 5 seconds.
The Mode-Event-Fault LEDs begin to flash, in an upward sequence, to indicate a 'Load. '

4 When the flashing sequence stops (but not before) remove the USB storage device.

5 If the load was successful, the Modbus TCP Firewall goes to OPERATIONAL mode, with the Mode LED showing a steady light.

3.6.3 Saving diagnostic information

The USB Save function copies diagnostic files from the Modbus TCP Firewall to the USB storage device. These files can then be sent to the Honeywell Solution Support Center for analysis.

1 Insert a USB storage device into one of the USB ports.

2 Press and hold the Config button for \ second (but less than 5).
The Fault-Event-Mode LEDs begin to flash in downward sequence, to indicate a 'Save'

3 When the flashing sequence stops, remove the USB storage device.

4 If the save was successful, the Modbus TCP Firewall LEDs revert to the state they were in prior to performing a save.

5 Send copies of these files to Honeywell Solution Support Center for analysis.

4 Monitoring the Modbus TCP Firewall

Related topics

“Modbus TCP Firewall in Configuration Studio” on page 24
“Modbus TCP Firewall in Station Displays” on page 25
“Modbus TCP Firewall faceplate and detail displays” on page 26

4.1 Modbus TCP Firewall in Configuration Studio

The Modbus TCP Firewall appears in the list of Control Firewalls, mapped by its MAC address, which is the same as a Honeywell Control Firewall (CF9) within Configuration Studio.

The Configuration Studio tools for the Modbus TCP Firewall are the same as those used for the Control Firewall and can be used in the same manner.

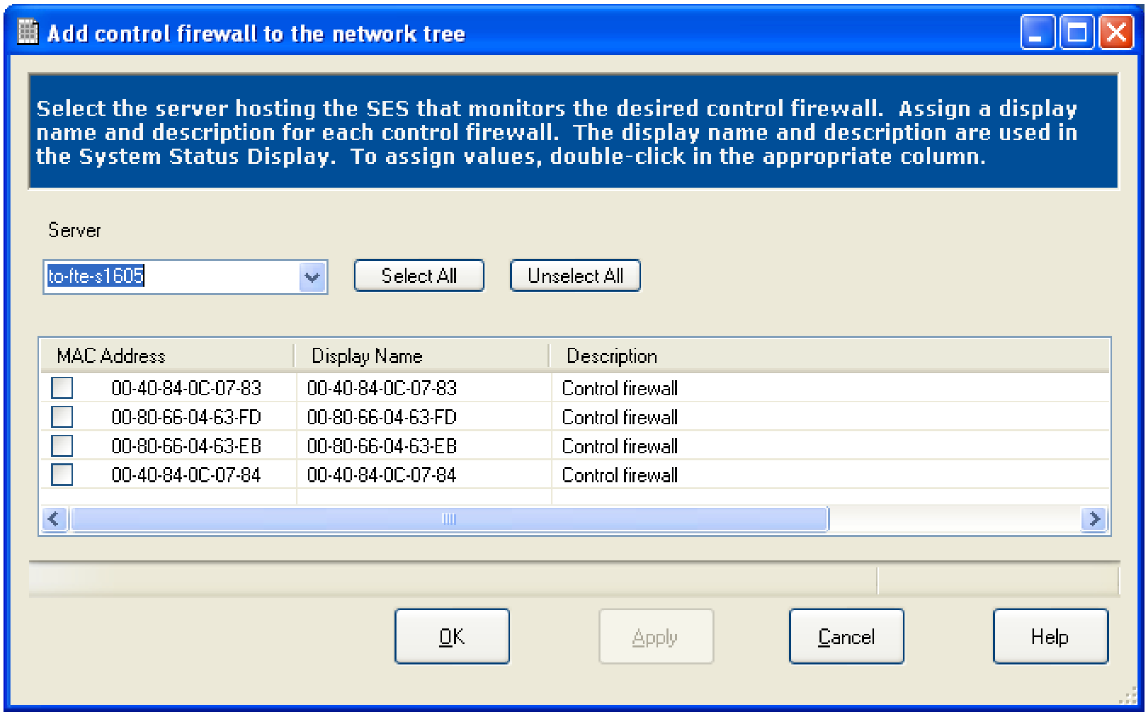
4.1.1 Identifying the Modbus TCP Firewall

The MAC address for each Modbus TCP Firewall is located on a label on the front of the device. For this initial release of the Modbus TCP Firewall, the device description appears as **Control Firewall** within Configuration Studio and on any displays.

You can distinguish between a Honeywell Control Firewall and a Honeywell Modbus TCP Firewall by looking at the MAC addresses displayed in Configuration Studio:

- Honeywell Control Firewall MAC addresses start with 00-40-84
- Honeywell Modbus TCP Firewall MAC addresses start with 00-80-66

In the following figure, the first and fourth devices are Control Firewalls; the second and third devices are Modbus TCP Firewalls.



Add control firewall to the network tree

Select the server hosting the SES that monitors the desired control firewall. Assign a display name and description for each control firewall. The display name and description are used in the System Status Display. To assign values, double-click in the appropriate column.

Server: to-fte-s1605

MAC Address	Display Name	Description
□ 00-40-84-0C-07-83	00-40-84-0C-07-83	Control firewall
□ 00-80-66-04-63-FD	00-80-66-04-63-FD	Control firewall
□ 00-80-66-04-63-EB	00-80-66-04-63-EB	Control firewall
□ 00-40-84-0C-07-84	00-40-84-0C-07-84	Control firewall

4.2 Modbus TCP Firewall in Station Displays

From Station, the Modbus TCP Firewall appears in the System Status Network Tree under Devices the same as a Honeywell Control Firewall (CF9).

4.2.1 Modbus TCP Firewall alarm description

Modbus TCP Firewall alarms include conditional alarms for Port link down and when the Control Firewall can no longer be heard (65 second timeout). Port link up generates an event.

Modbus TCP Firewall alarm descriptions are formatted as follows:

<Switch Name> <Display name> (MAC Address) port-id message

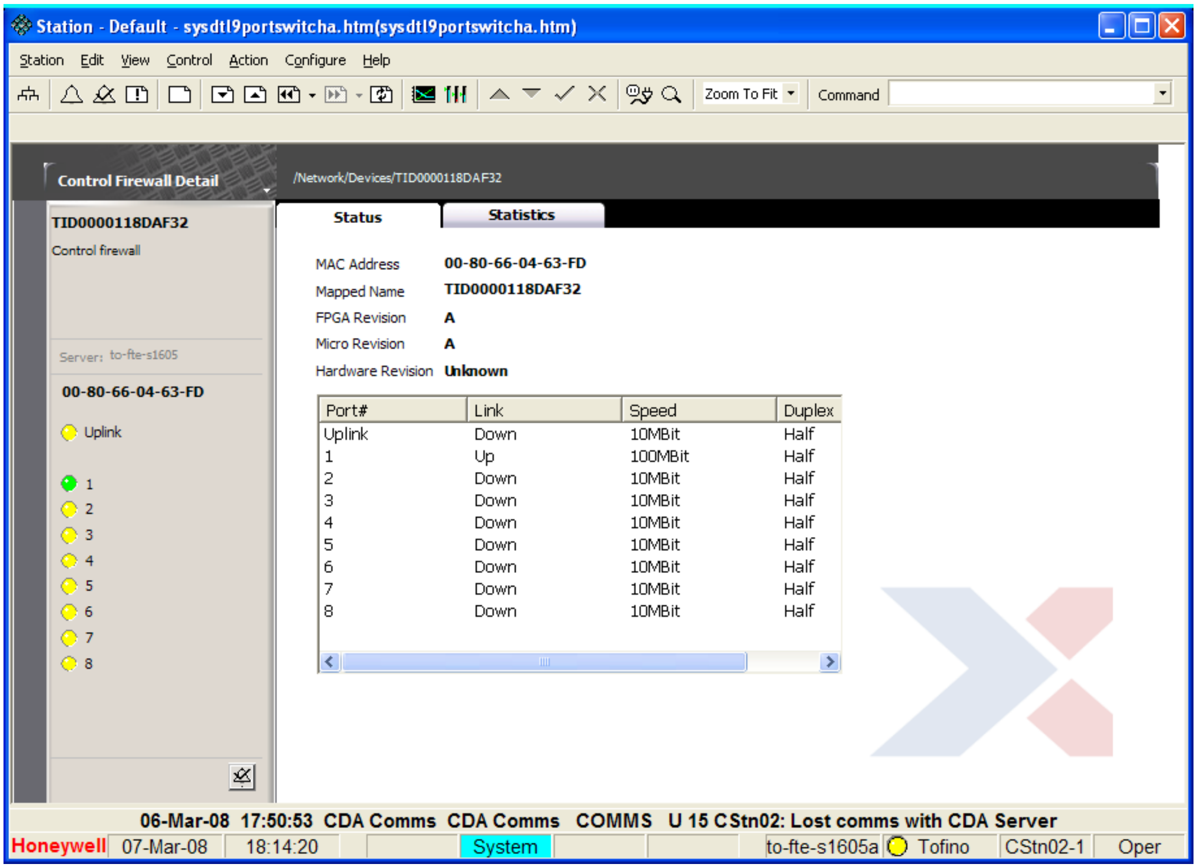
For example:

TID0000118DAF32 Boiler#2Y (address 00-80-66-04-63-FD) port 0 link status is up

Name	Description of value
Switch Name	Hardcoded identifier reported by the Modbus TCP Firewall. The identifier consists of the constant characters 'TID ' plus the 12 character unique hardware identifier printed on the front label of the Modbus TCP Firewall.
Display Name	Name mapped to the Modbus TCP Firewall MAC Address in Configuration Studio. This is the name displayed in the Network tree.
MAC Address	MAC Address printed on the label on the front of the Modbus TCP Firewall.
Port-id	If the alarm is for Port 0 (unsecured upper), ‘uplink’ appears in the alarm description. If the alarm is for Port 1 (secured lower), ‘no longer being heard by the FTE’ appears in the alarm description. This occurs when the Control Firewall cannot be heard for longer than 65 seconds. This is expected because when the secured port is removed, the firewall no longer has a path to the server.

4.3 Modbus TCP Firewall faceplate and detail displays

For the initial release of the Modbus TCP Firewall, it appears in faceplates and detail displays as a Honeywell Control Firewall (CF9) with 1 uplink port and 8 additional ports as shown in the following figure.


Station - Default - sysdtl9portswitcha.htm(sysdtl9portswitcha.htm)
Station Edit View Control Action Configure Help
Zoom To Fit
Command
Control Firewall Detail
/Network/Devices/TID0000118DAF32
Status
Statistics

TID0000118DAF32
Control firewall

Server: to-fte-s1605

00-80-66-04-63-FD

○ Uplink

● 1
○ 2
○ 3
○ 4
○ 5
○ 6
○ 7
○ 8

MAC Address 00-80-66-04-63-FD
Mapped Name TID0000118DAF32
FPGA Revision A
Micro Revision A
Hardware Revision Unknown

Port#	Link	Speed	Duplex
Uplink	Down	10MBit	Half
1	Up	100MBit	Half
2	Down	10MBit	Half
3	Down	10MBit	Half
4	Down	10MBit	Half
5	Down	10MBit	Half
6	Down	10MBit	Half
7	Down	10MBit	Half
8	Down	10MBit	Half

06-Mar-08 17:50:53 CDA Comms CDA Comms COMMS U 15 CStn02: Lost comms with CDA Server

Honeywell 07-Mar-08 18:14:20 System to-fte-s1605a ○ Tofino CStn02-1 Oper

4.3.1 Modbus TCP Firewall status

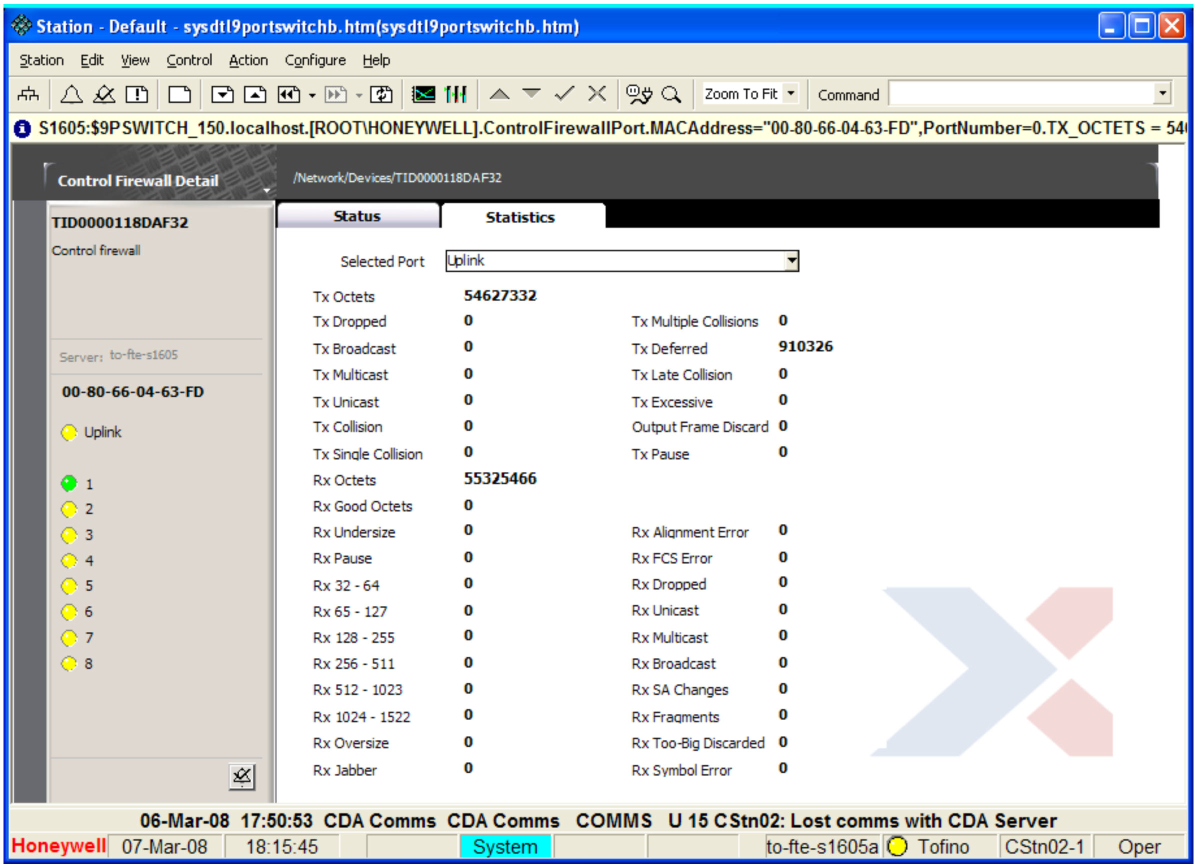
The following table describes the Modbus TCP values as they are displayed on the Status faceplate.

Faceplate Label	Description
Uplink*	Corresponds to the top Ethernet port on the Modbus TCP Firewall, which is the Unsecure port. This port connects to the Modbus Device network, usually through the uplink port on a Cisco switch.
Port 1*	Corresponds to the bottom Ethernet port on the Modbus TCP Firewall, which is the Secure port. This port connects to the Experion system through the Level 2 switch.
FPGA Revision	Revision letter for the Modbus TCP Firewall firmware.
Micro Revision	Revision letter for the Modbus TCP Firewall firmware.
Hardware Revision	1.0
* Only these two ports are significant for the Modbus TCP Firewall.	

4.3.2 Modbus TCP Firewall port statistics

Statistics are only available for the Uplink port and Port 1. Port 2 through Port 8 display bad-quality data. Additionally the Transmit and Receive statistics available for the Modbus TCP Firewall are a subset of those available for the Control Firewall (CF9). Unavailable statistics display 0. Following are the available statistics:

Transmit	Receive
TX_OCTETS	RX_OCTETS
TX_DROP	RX_UNDERSIZE
TX_MULTICAST	RX_OVERSIZE
TX_COLLISION	RX_ALIGN_ERROR
TX_SINGLE_COLLISION	RX_FCS_ERROR
TX_MULTI_COLLISION	RX_DROPPED
TX_DEFERRED	
TX_LATE_COLLISION	


Station - Default - sysdtl9portswitchb.htm(sysdtl9portswitchb.htm)
Station Edit View Control Action Configure Help
Zoom To Fit
Command
Control Firewall Detail
Status
Statistics

S1605:$9PSWITCH_150.localhost.[ROOT\HONEYWELL].ControlFirewallPort.MACAddress="00-80-66-04-63-FD",PortNumber=0.TX_OCTETS = 54

/Network/Devices/TID0000118DAF32

TID0000118DAF32
Control firewall
Server: to-fte-s1605
00-80-66-04-63-FD

- ● Uplink
- ● 1
- ● 2
- ● 3
- ● 4
- ● 5
- ● 6
- ● 7
- ● 8

Selected Port: Uplink

Tx Octets	54627332		
Tx Dropped	0	Tx Multiple Collisions	0
Tx Broadcast	0	Tx Deferred	910326
Tx Multicast	0	Tx Late Collision	0
Tx Unicast	0	Tx Excessive	0
Tx Collision	0	Output Frame Discard	0
Tx Single Collision	0	Tx Pause	0
Rx Octets	55325466		
Rx Good Octets	0		
Rx Undersize	0	Rx Alignment Error	0
Rx Pause	0	Rx FCS Error	0
Rx 32 - 64	0	Rx Dropped	0
Rx 65 - 127	0	Rx Unicast	0
Rx 128 - 255	0	Rx Multicast	0
Rx 256 - 511	0	Rx Broadcast	0
Rx 512 - 1023	0	Rx SA Changes	0
Rx 1024 - 1522	0	Rx Fragments	0
Rx Oversize	0	Rx Too-Big Discarded	0
Rx Jabber	0	Rx Symbol Error	0

06-Mar-08 17:50:53 CDA Comms CDA Comms COMMS U 15 CStn02: Lost comms with CDA Server

Honeywell 07-Mar-08 18:15:45 System to-fte-s1605a ○ Tofino CStn02-1 Oper

5 Troubleshooting the Modbus TCP Firewall

Use the information in this section to help you troubleshoot the device.

Related topics

“Diagnosing issues using the LED indicators” on page 30

5.1 Diagnosing issues using the LED indicators

Related topics

"LED descriptions" on page 30

"Load/Save LED Activity" on page 30

5.1.1 LED descriptions

The Modbus TCP Firewall has LEDs on the front of the device that indicate normal and other modes of operation.

LED	Description for LED state
Pwr	**Off**: Indicates power less than 9V dc **On**: Indicates power is greater than or equal to 9V dc
Fault	**Off**: Normal function **On**: Indicates a hardware problem and is unable to start. **Short flash of .5 seconds**: Indicates the Loadable Security Module (LSM), which occurs with a USB Configuration Loading or Diagnostic Saving fault. **Long flash of 2 seconds**: Indicates the Modbus TCP Firewall OS did not start properly.
Event	**On but steady**: Normal function **Flashing**: Event or alarm generated - details sent to CMP
Mode	**On**: Normal function

5.1.2 Load/Save LED Activity

Use the information in this table to diagnose the fault from the number of Fault LED flashes and determine the appropriate course of action.

No. of Flashes	During Load Sequence	During Save Sequence
1	The USB ports are disabled Contact Honeywell Solution Support Center.	No USB storage device in the USB port or the USB storage device is not formatted with the standard Fat32 format.
2	No USB storage device in the USB port or the USB storage device is not formatted with the standard Fat32 format.	The Modbus TCP Firewall was unable to create the diagnostics files. Contact Honeywell Solution Support Center.
3	The files on the USB storage device are not valid.	The Modbus TCP Firewall was unable to encrypt the diagnostic files. Contact Honeywell Solution Support Center.
4	The Modbus TCP Firewall was unable to read the configuration files. The files may be corrupt.	The Modbus TCP Firewall was unable to copy the encrypted diagnostics files to the USB storage device. The USB storage device may be full.
5	The Modbus TCP Firewall was unable to decrypt the files.	The Modbus TCP Firewall was unable to shut down the USB port. Contact Honeywell Solution Support Center.
6	The Modbus TCP Firewall was unable to shut down the USB port. Contact Honeywell Solution Support Center.	N/A