Quantum Copro Firmware History

140CPU65150, 140CPU65160, 140CPU65260, 140CPU65860

Version #	Date of Publication	Internal reference	Description
SV6.1	**12/2019**	PEP0555453R	Resolved and issue where retransmissions caused a delay in the communications. The retransmissions were caused due to the Master cycle time being greater than the IO Scanner 'Rep rate'. The code was modified to drop the retransmission packets.
		PEP0557748R	Resolved a reboot vulnerability with an HTP script.
		PEP0557749R	Resolved a vulnerability where a Stack Buffer Overflow results in a crash.
		PEP0557750R	Resolved an unauthenticated Reflected XSS (Cross-site scripting) vulnerability.
		PEP0557769R	Resolved an unauthenticated HTTP Password Reset to Default
		PEP0557767R	Resolved a Password change vulnerability to CSRF (Cross-site Request Forgery)
		PEP0557768R	Resolved an unauthenticated HTTP Password Change
		PEP0540655R	Resolved a vulnerability to obtain information on an SMTP server configuration, including registration data of the user.
SV6.0	**11/2018**	PEP0425771R	Resolved an IO scanning communication issue between a Quantum CPU Copro and PRM (TCSEGPA23F14F) Profibus Gateway module.
SV5.9	**6/2018**	PEP0455702R	Resolved an issue where the Copro server responded with a Modbus 'Exception code 6' – Slave device busy. An external client using I/O Scanner control bits caused the Copro server Modbus handler to become non-responsive.
SV5.8	**3/2016**	PEP0318880R	Removed a Remote Code Execution vulnerability in the websSecurityHandler (Advisory ICSA-15-351-01)
		PEP0318881R	Removed a web server vulnerability to a remote file inclusion attack. (ICS-ALERT-15-224-02)
SV5.7	**4/2015**	PEP0271552R	Resolved an issue where if an MBP_MSTR function 16 is issued after a break in communications, the Quantum CoPro could take up to 90 seconds or more to recover. A parameter was missing on a function call so no error message was sent to the function block. This has been corrected and the CoPro will recover in under 40 seconds.
		PEP0277388R	Web pages now meet requirements to work with Java version 1.8.
		PEP0275523R	Data Editor web page functionality is misleading and implies that unlocated symbols can be used. Only modules that are FactoryCast capable can use symbols in the Data Editor web page. The apparent use of symbols was removed from the web pages of non-FactoryCast modules.
SV5.6	**11/2014**	PEP0271979R	Resolved an issue where the I/O Scanner communications could take at least 40 seconds or more to recover if a link down/up event occurs on the client (Copro) side of the switch. A link down/up event (without a duplicate IP on the network) will restart the I/O Scanner in 2-3 seconds.

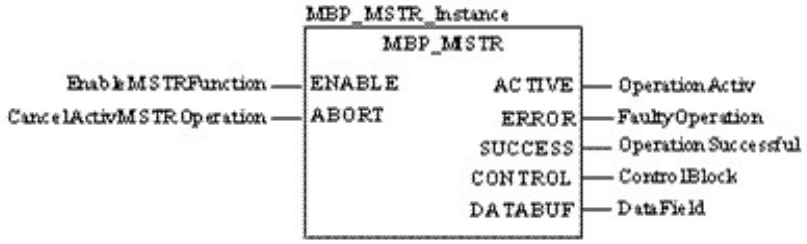
SV5.5	**6/2014**	PEP0250560R	Removed a vulnerability in HTTP, using directory traversals, an attacker could bypass the basic authentication mechanism. (Advisory ICSA-14-273-01)
		PEP0242058R	Added support for RackViewer for the 140CPU65860 and 140CPU67861.
		PEP0240305R	Revised web pages were added to the 140CPU65860 and 140CPU67861 Copro's.
		PEP0251116R	The Java dialog box displayed a warning indicating an unsigned application. Web page files with Java Version 1.7 now have security Signature.
		PEP0251045R	A slot management issue was corrected that could lead to CPU crash and cause EC0x error.
SV5.4	**3/2014**		Corrected an uninitialized variable that had the potential to cause a CPU EC0E crash.
SV5.1	**11/2013**		The MIB and MIG agent have been corrected where SNMP webFailedAttempsts(1.3.6.1.4.1.3833.1.5.4) and webSuccessfulAccess (1.3.6.1.4.1.3833.1.5.4) did not increment.
			Resolved an issue Web RackViewer incorrectly displayed a 140CRP31200 as a 140CRP931xx.
SV5.0	**3/2013**		Changed the default behavior of enabled FTP/TFTP and HTTP Service at module boot up. On power up, the Quantum Copro will have the FTP/TFTP and HTTP services enabled when in non-configured mode, or when configured by an older version of Unity Pro/DTM that does not have FTP/HTTP Cyber Security control.
			The MSTR block now supports the OpCode 0xFFF0 to be used by the user to enable and disable FTP/TFTP and HTTP services in the module on-the-fly, when Unity has enabled the service. Once the enabled state of the services are changed by a MSTR, they remain unchanged until the next MSTR block call with OpCode 0xFFF0, or the load of a new application, or the module is reset/power cycled. This OpCode works on Concept and Unity controller installations. When FTP/TFTP is disabled, the corresponding ports 21(FTP) and 69 (TFTP) are closed. If the ports have an open connection when the MSTR is executed to disable FTP, the connection will be closed. Refer to the Note at the end of this document that describes how to enable/disable these services.
			Unity Software can now enable/disable FTP/TFTP or HTTP services in the configuration. Unity 7 with Hotfix HF20050608 and a CPU OS 3.12 or greater. Configuring the FTP/TFTP or HTTP services will have precedence over the MSTR to control the enabling/disabling of the services.
			NOTE: Concept Software will not have any changes to enable/disable FTP/TFTP or HTTP services in the configuration. When using Concept, both FTP/TFTP and HTTP services will always be enabled in the configuration allowing only the MSTR to control the enabling/disabling of the services.
			New functionality added to log out users from the PLC programming via web page. To access this functionality, go to the Diagnostics page then select Rack Viewer. Next, right-click on the controller image and select Controller Status. Clicking on the Log Out button will creat a new pop up confirming the users request.
			Web Restrictions: When the FTP is disabled and HTTP is enabled, there will be some Web restrictions as they require an FTP access. • The Data Editor/Viewer is not fully functional: The user does not have the ability to save or retrieve tables, or get variables from the namespace. • Graphic Editor is not functional: Not able to save or get graphics. • Change FTP password page: Not functional • Web Designer: Not possible to transfer
SV4.2	**12/2012**		Resolved an issue when using I/O Scanning could cause excessive ARP traffic for a gateway. Each line of an I/O scanner issued its own ARP prior to establishing a connection, resulting in excessive traffic for a router or gateway. Now, the I/O Scanner will issue an ARP for each IP address rather than for each line of the scanner. This will eliminate multiple ARPS to the same device.

SV4.0	**7/2012**		Response to ICS-ALERT-12-020-03. The CoPro was vulnerable to FTP buffer overflows. A problem due to FTP buffer overload was addressed and the vulnerability has been corrected.
SV3.8	**6/2012**		An invalid entry configured for the Address server in Unity prevented the address server from starting. The address service will now start regardless of whether or not there is a valid address configured.
			Two copies of FDR .prm files should be created in both RAM and FLASH. The FLASH version of the PRM file was not created. A change to an algorithm corrected the task to create the FLASH version.
			The I/P address is lost on a power cycle while in "No Cfg". When the CPU powers up in a "No Cfg" state, you can enter an I/P address via the key pad. But that configured address is lost after a power cycle and the I/P defaults back to MAC address. The keypad data stored in flash gets deleted before the Copro has a chance to check it on bootup. The fix was not to delete the data before the CoPro reads it on bootup.
			Response to ICS-ALERT-12-020-03. The CoPro is vulnerable to HTTP server buffer overflows. An HTTP GET request with a filename that is too long causes an overflow, device crash. A GET request with an excessive length will be dropped.
			Various Cyber Security changes were implemented: - Removed Telnet service. - Removed Windriver debug port. - Removed unused password access points.
			An enhancement was made to increase the TTL (Time To Live) to 32.
			An enhancement was made to the Modbus messaging capacity. Quantum was not able to send a frame greater than 100 registers, when Modbus max size is 256 bytes. This was corrected to allow it to send the maximum size.
			An option was added to the I/O Scanner to increase the timeout time when communicating through Gateways. This option was added to the I/O Scanner in Unity v7.0 and higher where the user can change the retry and retransmission rate when communication with gateways. Slower responding devices (Gateways) could cause a problem in communications.
SV3.7	**12/2011**		Repeated access to the diagnostic statistics web page causes web server connection to break. Repeated rapid access or refreshing of the Diagnostic Statistics web page can cause the web server to lose its connection. Corrected a race condition that led to an endless loop.
			On a Connexium ring break, the CoPro times out and resets the connections resulting in needless delay. When a ring of Connexium switches breaks, the CoPro times out and resets the connections. Improper timing on an ACK response in certain states was corrected.
			On a 'Loss of link', due to a cable disconnect for a long time, communications will not be restored on a reconnection. If an Ethernet cable is disconnected from the CoPro port and is not reconnected quickly, the communications will not be re-established when the cable is plugged in again. The timeout mechanism was corrected.
SV3.5	**6/2011**		I/O Scanner operation does not always trigger fast retransmission in the target device. Fast Retransmission is triggered by three KEEP ALIVE messages. Under some circumstances the NOE would only issue two. Keep-Alive ACKs from the I/O Scanner stack was increased to "3" to be more standard and close to other devices.
			Updated Rack Viewer Web page V5.0. Redesigned web pages using Microsoft SilverLight and new features added. • Faster page update times than the traditional FactoryCast web pages that use JAVA. • Pan and Zoom in the Rack Viewer to see a particular drop or module. • New Rack Viewer will allow for a “System View” where Remote I/O is included in the view (ERIO, RIO and MB+ DIO for Quantum)

			• An option is provided in Unity Pro 6.0 to disable the SilverLight Rack Viewer pages to save memory in the PLC. The legacy Rack Viewer pages will be used instead. • It will no longer be necessary to re-import the Unity program into Web Designer and download to the module after a program change.
			CoPro Reboots after Cable Break with Explicit Messaging. In some instances, the Copro reboots while Explicit messages are configured to devices that do not exist and a link loss event occurs at the Copro. The connection table management was improved.
			MSTR Function Block TCP connections take too long to free up for reuse. When an MSTR block is aborted, it takes 30 seconds before the socket is free. A new MBP_MSTR sub-function 16, Reset connection, allows the closing of any pending/active/semi-open Port502 and network level TCP/IP connections. Further details can be found in Unity Help versions 6 and higher.
SV3.3	**12/2010**		I/O scanner not scanning at configured Rep-Rate. The I/O Scanner may not operate at the configured Rep Rate if its configured rate is greater than 1 second. If the Rep Rate is configured for a value of 5 msec, the actual rep rate will vary between 1ms and the configured rate of 5 msec. Modified I/O Scanner task priorities.
			I/O scanner health bits will not return to healthy state (1) after a TesysPort is power cycled. Sometimes after power cycling a TesysPort, the respective I/O Scanner health bits in the CoPro changes to a state value of zero (0) and never changes back to a value of one (1) after power is re-applied to the TesysPort.
			Copro does not send a bootp request after it is powered on. The CoPro, with either version 2.5 or v2.7 Exec firmware, does not send a Bootp request after it is powered on if the new PLC was placed on the rack right out of the box with no configuration. Exec firmware version 2.1 did not experience this issue. Modified the firmware to send Bootp requests at power on. Requests are now sent every 5 seconds for 2 minutes.
			The WRITE_REG, READ_REG, CREAD_REG and CWRITE_REG Function Blocks do not return an error code if the Ethernet cable is disconnected. The CoPro Modbus handling does not properly handle Link down events on the CoPro Ethernet port. The appropriate messages are now returned by the function block.
			The copro port will not re-establish communications if the Link is lost for more than 1 hour. A stop/start of the CPU was required to recover communications. A link down condition is now detected and returns an error.
			I/O Scanner will not open a connection if the device being scanned has a slow response time (110-120ms). The Retransmission Timeout (RTO) algorithm was fixed.
			CoPro port unable to make connection through a router. Any client/server communications to the CoPro outside of the local subnet, could fail in some cases. The Round Trip time algorithm for retransmission was modified.
SV3.1	**5/2010**		Quantum CoPro stops I/O scanner communication with slow responding devices. I/O Scanning to devices with varying response times may stop if it receives a reset (RST) from the device. A fix was implemented so that when the Quantum CoPro receives a RST from the server on an established connection, it closes the existing connection and tries to establish a new connection on a different port.
			A Quantum CoPro can take up to 25 seconds to close a connection. The Quantum CoPro sends a set of six ACKS or Keep-alives followed by a RST. This can take up to 25 seconds before the connection is closed and allowing a new one to open. The code was modified to cancel the retransmit timer.
			The Quantum CoPro port stops operating if excessive UMAS and Modbus messages are received. The Quantum CoPro Ethernet port will stop operating if there is an excessive amount of UMAS (i.e., 4000 unlocated variables) and Modbus traffic (i.e., 20,000 variables) present. The Port 502 buffer configuration size was increased.

How to enable/disable FTP/TFTP and/or HTTP using MBP_MSTR FB

Definition



- MSTR block programming follows normal programming procedures in addition to a new format of the control block. Both the control block and return data field must be located to %MW in the application. The return data field must be at least one word in length but is not used.
- The control block must be at least nine words in length.
- The control block **MUST** be programmed as follows:

Word0 - OpCode 0xFFF0
Word1 - Error Return Code
Word2 - **MUST** be set to 1
Word3 - **MUST** be set to 1
Word4 - Must be set to slot number of NOE (high byte) and Destination ID to use (low byte)
Word5 – Bit 0 (LSB) FTP/TFTP Request Mode, 1 = Enable, 0 = Disable
Bit 1 HTTP Request Mode, 1 = Enable, 0 = Disable
Word6 - **MUST** be set to 0
Word7 - **MUST** be set to 0
Word8 - **MUST** be set to 0

Errors returned

The MSTR block returns the following status/errors:

- Success – 0x0000, when the MSTR block with OpCode 0xFFF0 is called and the enabled state of either HTTP or FTP/TFTP was changed .
- Busy – 0x5068, when the MSTR block with OpCode 0xFFF0 is called within 2 seconds of previous call regardless of success or error..
- Same State – 0x4001 when the MSTR block with OpCode 0xFFF0 is called to change the state of both HTTP and FTP/TFTP to the state that they are currently in.
- Invalid Data – 0x2004 when the data in the MSTR's control block is not as specified. In Concept if word 2 is set to 0 this error is set to 0x1001.
- Disabled – 0x5069, when the MSTR block with OpCode 0xFFF0 is called and Unity Pro has disabled FTP/TFTP or HTTP and the MSTR request is to changed the state of the disabled service.
- **IMPORTANT – No change of state will occur for either FTP/TFTP or HTTP if an error code other than success is returned.**