

Quantum 140NOE77111 Firmware Release Notes



Exec Revision History

V6.8	4/11/2017	Problem fixed / Enhancement • The web page could be accessed after multiple attempts using an IE browser even though web access was disabled in the configuration. (specific to firmware version 6.7)	Details Corrected file that disables http access.
V6.7	2/24/2016	Problem fixed / Enhancement • Improves Global Data and IO Scanner performance after a swap over in a Hot Standby System • Removed a Remote Code Execution vulnerability in the websSecurityHandler (Advisory ICSA-15-351-01)	Details
V6.6	9/30/2015	Problem fixed / Enhancement • Removed a web server vulnerability to a remote file inclusion attack. (ICS-ALERT-15-224-02) • When using I/O Scanner control bits to turn On/Off I/O Scanner entries, it can intermittently cause the NOE to reboot causing a 20 second outage of Ethernet communications.	Details Corrected the control bit disable feature from forcing the I/O Scanner state machine to finish.
V6.5	8/15/2015	Problem fixed / Enhancement • In a Hot Standby system, Global Data services may stop after a switchover of the PLC. • Resolves Java 1.8 issues.	Details Issue has been managed with updated code. Refer to the Global Data Addendum for further details.
V6.4	12/12/2014	Problem fixed / Enhancement • After an application download via Concept, the NOE77111 IO Scanner communications does not restart. • The IO Scanner Health bits are not working on Link Down.	Details In Unity PLC the NOE will ARP for DUP IP after every Application down load. In Concept the NOE will only ARP if the IP parameters have changed when Concept logs out. The Health Timeout timer is stopped on a Link Down, so the Health bits are not updated in the CPU. Now the IO Scanner Health Bits will go unhealthy on link down and not glitch on Link Up.

V6.3	9/5/2014	Problem fixed / Enhancement • MBP_MSTR block reports an error 1001 after an application download.	Details During an application download, the IP component was temporarily applying the broadcast IP which disrupted the MSTR block. Code modifications were made and the MSTR block works as expected.
V6.2	6/30/2014	Problem fixed / Enhancement • In HTTP using directory traversals an attacker can bypass the basic authentication mechanism. (Advisory ICSA-14-273-01) • Web page issue with Java Version 1.7. Files did not have • On Hot Standby switchover, under extremely high traffic • With a Concept Hot Standby application, under unusual test conditions, there is a chance an NOE could lose its IP address. • Quantum CPU may crash with error EC0E after completing a download of an application.	Details Checks have been put in so that this is no longer possible. The files all have been properly signed. Situation was corrected and the NOE comes online regardless The NOE module will configure its IP address under those conditions. Fixes a potential CPU EC0E crash issue where configuration data was not cleared when a smaller program was downloaded over a larger one that was previously installed. I/O Scanner configuration data is now cleared before the new data is downloaded and reconfigured.
V6.1	11/7/2013	Problem fixed / Enhancement • Unity allows the user to select the checkbox for 'Automatically adjust clock for daylight savings change.' however, when you open the NTP webpage after transferring the application to the PLC, it will show the DST Status as 'OFF'. When the time for daylight savings change occurs, the clock does not get adjusted.. • SNMP webFailedAttempts (1.3.6.1.4.1.3833.1.5.4) and webSuccessfulAccess (1.3.6.1.4.1.3833.1.5.4) do not increment • Client communications do not start on swap over in HSBY system	Details Daylight savings time works as designed. The MIB structure and MIB Agent have been corrected. On swap over, the communications now start as soon as possible after the switchover

		• When Using code 15 in a MBP_MSTR function block the first request fails with error 16#5055	Fixed the first request fault condition.
		• When the IO Scanner breaks out FC23 to FC16 and FC3, any change to the data being written in FC16 will toggle between the old and new data for a number of scans.	The function sends the correct data in all messages.
		• I/O scanner using a Radio Modem cannot establish contact.	The timeout algorithm was adjusted to accomodate low communication data rates.
		• After a cable pull, communications does not re-establish with certain Moxa or Sixnet switches	Communications now resumes when the cable is reinserted.
V6.0	3/30/2013	This is a special security release. The features listed require Unity hotfix V7.0_HF20050608 Problem fixed / Enhancement • The default behavior of enabled FTP/TFTP Service at module boot up has changed	Details On power up the NOE module will have the FTP/TFTP servers and HTTP service 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.
		• Concept will not have any changes to enable/disable FTP/TFTP or HTTP in the configuration.	When using Concept both FTP/TFTP and HTTP will be enabled in the configuration at all times allowing MSTR to control the enable/disable of the services.
		• The MSTR block now supports the OpCode 0xFFFF0 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 0xFFFF0, or the load of a new application, or the module is reset/power cycled. This OpCode works on Concept and Unity controller installations. In Concept the Web server/pages must be updated by the user to be able to control HTTP state of enable/disable, using the file NOE77101_WEB.zip. Bring the Web version up to V5.00 or above. * SEE Note below on how to enable/disable these services.
		• New Log Out Web Page	Users click on Diagnostics and go to Controller Status in the side menu. Below the applet is the logout button.

- Web Restrictions: When the FTP is disabled and HTTP is enabled there will be some Web restrictions as they require a FTP access.

- 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 is functional
- Web Designer: Not possible to transfer
- When FTP/TFTP is disabled the corresponding ports 21(FTP), and 69(TFTP) are be closed . If the ports have an open connection when the MSTR is executed to disable FTP, the connection is be closed

V5.6

12/20/2012

Problem fixed / Enhancement

- NOE77111 connection closure mechanism Can cause error 6003 in M1E MSTR function block

Details

A special socket option was added to all Modbus server connections called "No Linger" to facilitate HSBY switchovers. However that state was inadvertently added to two paths which caused the problem seen.

- Communications gradually degrades then stopr after running for about 16 months.

Due to mishandling of a 32 bit timer overflow in the stack as the timer approached the overflow point the performance of the NOE would degrade and at the point of overflow it would stop. It would recover on its own.

- In Quantum Ethernet modules I/O Scanning causes excessive ARP traffic when using a gateway.

Each line of an I/O scanner issues its own ARP prior to establishing a connection, This can cause excessive traffic for a router or gateway.

- Cannot ping The NOE77111 Ethernet port

If the cable is pulled from the Ethernet port and not reconnected for approximately 70 hours the connection is not reestablished.

- OpCode 16 to close connections needed for Concept.

Customer requested functionality similar to Unity where OpCode 16 in the MBP_MSTR block aborts the Ethernet connections.

V5.5	9/20/2012	Problem fixed / Enhancement	Details
		• The Web page allowed the user to enter more than 16 characters as a password but only 16 were used.	If you entered a new password as 17 characters in the http password web page, the NOE returned a page saying that the password change was successful. When you try to use the new password, it fails.
		• Unless there is a valid entry in the address table the FDR server will not start.	The address service will not start unless there is at least one valid entry with a valid MAC address configured in Unity.
		• Two copies of FDR .prm files should be created in both RAM and FLASH. The FLASH version of the PRM files in the patch is not created	The problem is in the algorithm when it attempts to parse the extension names of the FDR files on RAM (.prm). It is due to an existing method coding when comparing strings. The strings do not have the proper number of bytes so the Flash version of the .prm files could not be created.
		• Response to ICS-ALERT-12-020-03. The NOE is vulnerable to HTTP server buffer overflows	An Http GET request with too-long filename causes overflow, device crash.
		• Various Security issues Removed Telnet service. Removed Windriver debug port. Removed unused password access points	Cyber Security changes necessary in the following 1) Telnet service 2) Wind River debug service port 3) unused logins/passwords from firmwar
		• PLC Viewer web page does not show the SFC transition contact status correctly.	The values shown for the status of the contact in the web page may not be the correct value of the contact. This was due to the fact that changes made to plcprograms.jar file was not included in build.
		• Response to ICS-ALERT-12-020-03. FTP buffer overload	A possible problem due to FTP buffer overload.
		• PLC Program Viewer variable display performance decreases as the application grows	For large applications with a mixture of located and unlocated variables, PLC Program viewer sections would display "N/A" for various variables rather than their values.

		• Incorrect "Invalid Address" warnings Appear in the PLC Viewer. Variable's address initially set to "UNLOCATED", which is incorrect.	
	Enhancement	• Add option for slower retries when communicating with Gateways	Slower responding gateways can cause a problem in communications.
V5.1	12/15/2011	Problem fixed / Enhancement Special Note This NOE77101 V5.0 Integrates A new Hardware component. The NOE77101 with a PV of 22 or greater cannot be downgraded to Exec versions less than Version 5.0. • On an ethernet download using unity 6.0 Under some conditions Unity returns an error • NOE resets and goes into kernel mode during saving a PLC program to flash. • I/O Scanning Specific combination of Repitition Rate and Health Timeout not supported • IO scanner operation does not always trigger fast retransmission in target device	Details Unity 6 returns a 'Send message action failed. PLC is busy or request is invalid error. There was a problem when downloading using ProWorx or Concept. The backplane watchdog timer was being overrun. The combination of a 30ms repetition rate and 50ms Health Timeout leads to triggering Health Timeout in less than 50ms. This is due to a slight delay in the CPU while it is handling FDR synchronization. Fast Retransmission is triggered by three KEEP ALIVE messages. Under some circumstances the NOE would only issue two.
	Enhancement	• Increase in the TTL (Time to Live)	The customer had a large project involving many routers and he needed the Time To Live to be increased.

V5.0	6/24/2011	Problem fixed / Enhancement	Details
		• The MSTR Function Block in Unity was modified to Allow it to read 0x, 1x, and 3x registers	There is no method of reading 3x, 1x or 0x registers from devices that do not support 4x registers.
		• The Modbus client messaging capacity was Extended	Additional registers are required to access diagnostic information in the PRM (Profibus Remote Master module) in a single Modbus request. Quantum is limited to 100 registers per Modbus request.
		• MSTR 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.
		• Updated Rack Viewer Web page V5.0	Redesigned web pages using Microsoft SilverLight and new features added.
V4.8	12/22/2010	Problem fixed / Enhancement	Details
		• 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.
		• 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 NOE 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. If a response is not received within 3x times the configured health timeout, then the IO scanner connection is re-initialized.

• I/O Scanner communications will take 600ms to recover on loss of a TCP reply packet from a gateway	The I/O scanner fast retransmission algorithm may not be supported by all gateway devices causing message sequencing issues.
• After multiple consecutive swaps of a Quantum Hot Standby system, the NOE771x1 does not restart	After performing 3 or more immediate swaps of a Hot Standby system, the NOE does not restart.
• Network statistics incorrectly reporting Link status when the Ethernet cable is removed	Within the MBP_MSTR block, there is a Function Code 3 that can be used to 'Get Local Statistics' from an NOE. It returns the 'TCP/IP Ethernet Network Statistics' in a data buffer array. Word 3 of the data buffer array is used for the 'Board Status Word'. Bit 15 of Word 3 is used to monitor the status of the Link which is represented by the LINK LED on the front of the NOE module. The bit changes to a value of 1 when the Ethernet cable is plugged in. Then, if the Ethernet cable is removed from the NOE module, the LINK LED on the NOE goes off but bit 15 of word 3 of the data buffer array incorrectly flickers between values 1 and 0.
• I/O Scanner stops communications with a gateway device	Termination of the IO Scanner connection by the server may result in a condition where the I/O Scanner does not restart.
• I/O Scanner will not open a connection if the device being scanned has a slow response time	If the device being IO scanned has a slow response time (110-120ms), then the IO scanner will not be able to open a connection.

V4.7

5/26/2010

Problem fixed / Enhancement

- The NOE goes into detected fault mode if the primary HSBY plc is stopped
- NOE stops i/o scanner communication with slow responding devices
- I/O scanner may not hold last value during a HSBY swap
- NOE can take up to 25 seconds to close a connection
- The NOE is incorrectly assigned an address of 'configured IP+1' instead of the 'configured IP' in a standalone 140CPU6716x

Details

If the Primary PLC (HSBY configuration) is stopped, the NOE in the new Primary goes into detected fault mode for 20 seconds. This happens when there is more than one NOE. The HSBY system has a narrow window of time when Primary and standby change IP address. In some cases this leads to a duplicate IP conflict.configured.

I/O Scanning to devices with varying response times may stop if it receives a reset (RST) from the device. If a RST is received by the NOE on a connection it can cause the I/O Scanner entry to stop communicating.

The NOE771xx IO scanner may not hold the last value on a swap over of the Hot Standby. The I/O scanner values become zero for one scan.

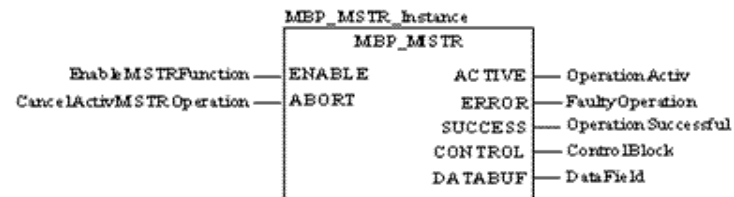
The NOE sends a set of six ACKS or Keep-alives followed by a RST. This can take up to 25 seconds before the connection is closed and allowing a new one to open.

The 140NOE77101 incorrectly returned an address of 'configured IP+1' unless there was a remote drop configured with a '140 CRP 93x xx' in the same rack as the '140CPU6716x'. This only happened when the Hot Standby CPU was used as a standalone/offline configuration.

NOTE :TP/TFPT/HTTP using the MBP_MSTR FB

How to enable/disable FTP/TFPT 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 0xFF0

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 DestinationID to use (low byte)

Word5 - Bit 0 (LSB) FTP/TFPT 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

How to Enable/Disable FTP/TFPT/HTTP using the MBP_MSTR FB

Errors returned

The MSTR block returns the following status/errors:

- Success – 0x0000, when the MSTR block with OpCode 0xFFFF0 is called and the enabled state of either HTTP or FTP/TFPT was changed.
- Busy – 0x5068, when the MSTR block with OpCode 0xFFFF0 is called within 2 seconds of previous call regardless of success or error..
- Same State – 0x4001 when the MSTR block with OpCode 0xFFFF0 is called to change the state of both HTTP and FTP/TFPT 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 0xFFFF0 is called and Unity Pro has disabled FTP/TFPT or HTTP and the MSTR request is to change the state of the disabled service.
- **IMPORTANT – No change of state will occur for either FTP/TFPT or HTTP if an error code other than success is returned.**

Global Data Addendum

Impact of using Global Data in a Quantum Hot Standby System 140NOE771x1 Firmware version 6.5

Swap is defined as the time the system uses to switch from Primary to Standby with all configured services started.

IP-Swap is defined as the time the system uses for the Primary (old Standby) to issue a gratuitous address resolution protocol (ARP), which helps detect IP conflict, showing the Primary is using IP, not IP+1.

Hot Standby with Global Data

 WARNING
UNINTENDED EQUIPMENT OPERATION The global data must not be used in systems that require periodic command swapping. Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTE: It is recommended that if periodic swapping must be used in the Hot Standby system, IO scanner be used in place of Global Data.

- IP-Swap can take up to **6 seconds** when Global Data is configured.
 - During this time the new Primary continues to use IP+1 which may cause a BUMP in the system.
- If you use Global Data in a Hot Standby system configure device hold up time as;
 - **4 * (watchdog) + 6 seconds.**
- If Global Data and IO Scanner are used in a Hot Standby system it can take up to
 - **7 seconds** for IO Scanner to start
 - **30 seconds** for Global Data to start