

TSXETY4103 Firmware History

Version #	Date of Publication	Internal reference	Description
SV6.2	12/2019	PEP0428770R	Resolved an issue with ETY4103's using FW V6.0 in a Hot Standby System. Unplugging the RJ45 Ethernet cable from an ETY4103 in the primary rack will cause a HSBY switchover. Re-installing the RJ45 Ethernet cable caused the previous primary CPU to remain in 'Offline' status'. The fix now allows the rack to go to Standby when the RJ45 cable is reconnected.
		PEP0448845R	Resolved an issue where a power cycle of the Standby would restart in RUN Offline instead of RUN Standby.
		PEP0538368R	Resolved an unauthenticated Reflected XSS (Cross-site scripting) vulnerability.
		PEP0538374R	Resolved an unauthenticated HTTP Password Reset to Default
		PEP0538373R	Resolved an unauthenticated HTTP Password Change
		PEP0538372R	Resolved a Password change vulnerability to CSRF (Cross-site Request Forgery)
		PEP0539070R	Login/password change requirements. Minimum password characters size of 16, must at least contain 1 uppercase,1 lowercase, 1 number and 1 special character.
		PEP0556600R	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.
		PEP0558371R	Resolved a reboot vulnerability with an HTP script.
		PEP0558373R	Resolved a vulnerability where a Stack Buffer Overflow results in a crash.
PEP0558374R	Resolved a vulnerability to obtain information on an SMTP server configuration, including registration data of the user.		
SV6.0	7/2017	PEP0386678R	Resolves issue where disabling HTTP access would not block access to the web server.
SV5.9	4/2016	PEP0272325R	Random Ethernet communication failures were corrected with link status checks that could otherwise cause false error conditions.
		PEP0318881R PEP0314329R	Removed a web server vulnerability to a remote file inclusion attack. (ICS-ALERT-15-224-02).
		PEP0309176R PEP0318880R	Removed a Remote Code Execution vulnerability in the websSecurityHandler (Advisory ICSA-15-351-01).
SV5.8	8/2015	PEP0273858R	Upon bootup, the first write always fails with an error 12FF. The write was attempted before the connection was complete and an error was returned. The NOE will not attempt a write until completion of the connection.
		PEP0288965R	Java 8 issues with web page applets. The problems with the signing applet were corrected.
SV5.7	6/2014	PEP0225387R	Cyber Security vulnerabilities with FTP and HTTP. Option added to prevent FTP/HTTP access.
		PEP0250560R	In HTTP using directory traversals an attacker can bypass the basic authentication mechanism. Security Alert - ICS-VU-529542. Checks have been implemented so that this is no longer possible.
		PEP0251116R	Web page issue with Java Version 1.7. Files did not have security signature. The Java dialog box provides a warning indicating that this is a unsigned application. The files have all been properly signed.

SV5.5	11/2013		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. The MIB and MIG agent have been corrected.
			Unity allows the user to select the checkbox for 'Automatically adjust clock for Daylight Savings change.' When Daylight Savings Time (DST) was selected for New Zealand, the clock did not get adjusted. The DST date was corrected for New Zealand.
SV5.4	1/2013		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. 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.
			Standalone will not start if no link is present on Monitored ETY at start. CPU goes to off line when it realizes it does not have link. This is correct but after the link comes up it will never go on line until it is power cycled again with the switch up first. A flag was added to check link status on bootup that corrected the improper behavior.
			Inconsistency issue between products using Global Data. Under certain conditions, Global Data would not become active on a power up of the system or a link-up/ link-down event. It would only start on when a PLC stop>start was performed if the subscriber is a BMXNOE. One problem with task start-up timing while the controller was in a Run state timing was corrected and another problem with closing and cleaning up resources when the link was down and Global data was running was also corrected solving the problem.
SV5.3	9/2012		Response to ICS-ALERT-12-020-03. The module is vulnerable to HTTP server buffer overflows. An HTTP GET request with too-long filename causes overflow, device crash. The Get Request will be rejected if the number of characters is excessive.
SV5.2	6/2012		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. The password field was corrected to limit the user to 16 characters.
			A request was made to increase the TTL (Time To Live). The TTL was increased to 32.
			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. A more specific string comparing function was used allowing specifying number of bytes to compare. The FLASH files are now created.
			Increase performance with serial gateways. Serial gateways are slower to respond than ordinary devices. Enhanced to work more efficiently with gateways. There is now an option in Unity 7 to enable a different retransmission algorithm for gateways.
			Security issues with this device Cyber Security changes required. 1) Removed Telnet service 2) Removed Wind River debug service port 3) Removed unused logins/passwords from firmware
SV5.1	12/2011		Special Note TSXETY4103's with a PV of 14 or greater integrate a new hardware component and cannot be downgraded with Exec versions less than v5.1.
			Downloading via Ethernet using Unity 6.0, under some conditions, Unity returns an error, ' <i>Send message action failed. PLC is busy or request is invalid</i> ' error. The handling of new downloaded configurations in the device have been resolved to prevent Unity Pro TCP disconnections when updating the controller through the Ethernet module IP address.
			Fix for loss of web connection. Repeated access to the diagnostic statistics web page causes web server connection to break. Corrected a race condition that lead to a endless loop.
			I/O Scanning using a specific combination of Repetition Rate and Health Timeout was not supported. The combination of a 30ms repetition rate and 50ms Health Timeout leads to triggering Health Timeout in less than

		<p>50ms. This is due to a slight delay in the CPU while it is handling FDR synchronization. The priority of the task controlling the Health timeout was raised eliminating the problem.</p> <p>Under certain conditions, the FDR server does not always save the correct backup file. This comes about because the time/date clock in the NOE is reset on each bootup and the saved file appears newer than subsequent files. When the NOE is rebooted, the stored files' time will now be overwritten by the NOE's new time. This insures that future files will have a newer date.</p> <p>I/O Scanner operation does not always trigger fast retransmission in target device. Fast Retransmission is triggered by three KEEP ALIVE messages. Under some circumstances, only two would be issued. The ETY will now issue three KEEP ALIVE messages to ensure that the target device will follow the fast retransmission algorithm.</p>
SV5.0	5/2011	<p>Special Note This ETY4103 v5.0 is a Premium Hot Standby only release to support the multitrack feature. The minimum Hot-standby firmware versions to support multitrack are:</p> <ul style="list-style-type: none"> - ETY4103 V5.0 - CPU V2.83 - CoPro V2.81
		<p>Enhancements and fixes to resolve <i>synchronous</i> Power cycle issues in Hot-Standby systems. (<i>Simultaneously powering off/on both system A and B</i>)</p> <ul style="list-style-type: none"> - The monitored ETY RUN and STS LED's blinking during synchronous power cycles - The monitored ETY I/O scanner enters a faulted condition during synchronous power cycles - The hot-standby system remains in Offline/Offline condition during synchronous power cycles <p>There were various bug fixes relating to improper management of the HSBY Status of the local CPU and remote ETY during the boot sequence of the ETY. These were identified during extensive power cycle testing.</p>
		<p>Enhancements and fixes to resolve <i>asynchronous</i> Power cycle issues in Hot-Standby systems. (<i>Power OFF/ON Primary System only</i>)</p> <ul style="list-style-type: none"> - The I/O scanner service of the monitored ETY enters a fault condition during asynchronous power cycles - The hot-standby system swaps abnormally after stopping asynchronous power cycle cut test - The hot-standby system remains in Primary/Offline mode during asynchronous power cycles - The non-monitored ETY crashed with both RUN and STS LEDs blinking during asynchronous power cycles - The Modbus server (port 502) of the non-monitored ETY is not available during asynchronous power cycles <p>Resolved memory management issues which, at times, caused improper protection of shared memory between tasks. This sometimes initiates exceptions to occur causing a crash. Resolved backplane interrupt handler issues during boot up and swap sequence which affected the Modbus Server.</p>
		<p>Enhancements and fixes to resolve both CPU and Ethernet cable disconnect/reconnect issues.</p> <ul style="list-style-type: none"> - The monitored ETY module errors after disconnecting the hot-standby CPU sync link cable and a COLD start (push reset button on CPU) on Standby CPU - The monitored ETY doesn't start (all LEDs off) when powered on with ETY Ethernet cable disconnected - Both hot-standby CPU's act as Primary during disconnection of hot-standby CPU sync link cable and power cycle of the Standby system - The non-monitored ETY remains in error after disconnect/reconnect of monitored ETY Ethernet cable - The monitored ETY reboots after disconnecting hot-standby CPU sync link cable - The Primary and Standby systems swap when removing the hot-standby CPU sync link cable <p>Improved: ·</p> <ul style="list-style-type: none"> - ETY-to-ETY data exchange mechanism. - Management of link status in the monitored ETY. - Server response time for servicing an explicit request (Example: Read_VAR, Write_VAR, etc.)
		<ul style="list-style-type: none"> • With a Stand-alone hot-standby system (single Primary system only), stopping the CPU causes the Unity Programming connection to disconnect.

		<ul style="list-style-type: none"> • The CPU communications fails when connecting via TCP/IP and opening ETY web page debug screen on the monitored ETY. • The IP address of the monitored ETY within standby system reports IP address in ETY debug screen (should report IP+1). • Under continuous excessive traffic conditions, the Modbus port502 server of the monitored ETY may become inoperable. • After an online modification is made to a hot-standby system, the hot-standby system enters Primary/Offline condition. • Both system A and B CPU's act as Primary after removing the Primary PCMCIA card from CPU. • ETY IO scanner service sometimes not operational after application download via CPU USB port. <p>Resolved:</p> <ul style="list-style-type: none"> - IP status that was incorrectly returned from the ETY. - Improved Modbus server connection management.
SV4.9	12/2010	<p>Special Note For Premium Hot Standby users: ETY4103 firmware v4.9 is only intended for use with CPU (TSXH57xxM) firmware v2.5.</p>
		<p>I/O scanner not scanning at configured rep-rate.</p> <ul style="list-style-type: none"> - 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. <p>Modified I/O Scanner task priorities. The Rep rate is correct.</p>
		<p>Function code 23 not supported in server mode. The ETY will now respond to FC23 requests with a FC23 response which will decrease the response time from the PLC.</p>
		<p>TSXETY4103 will lockup if another device on the network is present at IP address 192.168.2.1. Suppressed ARPing for IP address 192.168.2.1 at bootup.</p>
		<p>I/O scanning can take 4-6 seconds to start after a Hot Standby swap over. After a HSBY swap, the number of retries were reduced and the RST algorithm was modified so client connections would close quicker.</p>
		<p>Sometimes after power cycling a TesysPort, the respective I/O Scanner health bits in the ETY 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.</p>
		<p>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. Round Trip Time algorithm for retransmission was corrected.</p>
SV4.8	5/2010	<p>An ETY4103 will not go into run mode if the link is not established on an operational network. The issue was resolved by increasing the size of the status buffer.</p>
		<p>If an I/O Scanner is configured for 'Hold Last Value' in a Premium HSBY system, the ETY4103 I/O scanner did not always hold the last value on a swap over. The PLC will sometimes read I/O scanner information in the middle of the ETY I/O scanner update. Therefore, only the health has been updated while the data is still in the process of being updated. The issue was resolved in the ETY firmware by writing the data first and then setting the health values.</p>
		<p>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 ETY on a connection it can cause the I/O Scanner entry to stop communicating. The firmware was changed so that when the ETY5103 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.</p>
		<p>I/O Scanning client stops communicating when a gateway device (i.e, TesysT, Exemys, Emerson Fieldbus Gateway) loses a packet. The loss of a packet results in a packet with an incorrect sequence number, thus stopping communications.</p>

			<p>ETY I/O Scanning a gateway. The gateway may occasionally drop a packet (query). The gateway waits a period of time, and then re-transmits the previous response. The ETY ACKs the response and continues ACKing (set of 6), based on the round trip time, but never retransmits the query. In the code, the timer responsible for the retransmission was canceled thus stopping the retransmission from triggering. The code to cancel the retransmit timer was modified.</p>
			<p>The following conditions will cause a 921 Crash code:</p> <ol style="list-style-type: none"> 1. The CPU sends an incorrect Modbus response message to the ETY. 2. The CPU sends an invalid packet across the Premium backplane to the ETY. 3. The ETY will reset if it detects that a new Modbus message received from a device on the network contains the same Modbus message transaction ID as a message already being processed within its internal buffers. <p>Changes have been incorporated into the CPU and the ETY to enhance the communications between the modules across the backplane. In the event that one of these conditions occurs, the ETY will discard the incorrect or invalid message and continue to operate without resetting.</p> <p>Both the ETY and Premium CPU firmware must be upgraded when used in a Premium Hot Standby system. The requirements are:</p> <ul style="list-style-type: none"> - When using the ETY4103 in a Hot Standby system, the Hot Standby CPU's TSXH5744M and TSXH5724M require a minimum CPU OS version of 2.50. - When using the ETY4103 in a non-Hot Standby system, the non-Hot Standby CPU's OS require a minimum version of 2.80.
			<p>ETY5103 can take up to 25 seconds to close a connection. The ETY sends a set of 6 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. In the code, the timer responsible for the retransmission was canceled thus stopping the retransmission from triggering. The code to cancel the retransmit timer was modified.</p>