Allen-Bradley

MicroLogix 1400 Programmable Controllers FRN 21

Catalog Numbers 1766-L32BWA, 1766-L32AWA, 1766-L32BXB, 1766-L32BWAA, 1766-L32AWAA, 1766-L32BXBA

Contents

About This Publication

These release notes for FRN 21.006 supplement the existing documentation supplied with your product.

FRN 21.006 is intended for Series B and Series C controllers only and cannot be loaded on Series A controllers.

Before You Begin

See the MicroLogix™ 1400 Programmable Controllers User Manual, publication 1766-UM001, for instructions on using ControlFLASH™ to upgrade your controller firmware.

Rockwell Automation

Compatibility

You need RSLogix 500® or RSLogix™ Micro software, version 8.30 or later, to program MicroLogix™ 1400 controllers.

You need RSLogix 500 or RSLogix Micro software, version 11 or later, for the password implementation enhancement introduced in FRN 21.000.

Enhancements

Enhancement for 21.006 (Series B and Series C only)

Enhancement	Description
Option to disable the Ethernet channel.	Users can select to enable or disable the Ethernet channel. For more information, see the MicroLogix 1400 Programmable Controllers User Manual, publication 1766-UM001.
Removed Write access for data files.	Users are prohibited to modify the data files from the web server. For more information, see the MicroLogix 1400 Embedded Web Server User Manual, publication 1766-UM002.
Requirement to change default password for first-time logins.	Users are not allowed to navigate through the web browser without changing the default password. For more information, see the MicroLogix 1400 Embedded Web Server User Manual, publication 1766-UM002.

Enhancement for FRN 21.005 (Series B and Series C only)

Enhancement	Description
Improvement to SNMP server behavior in RUN mode.	The SNMP (Simple Network Management Protocol) MIB (Management Information Base) data items can no longer be changed when the controller is in RUN mode.
Increase DNP3 event logging to up to 10K events.	Users can select the option for the DNP3 event logging to: • log up to 6013 events. • log up to 10,000 events by using the memory space of the Recipe and Data log. For more information, see the MicroLogix 1400 Programmable Controllers User Manual, publication 1766-UM001.

Enhancement for FRN 21.000 (Series B and Series C only)

Enhancement	Description
New password implementation for controller	This new password implementation provides enhanced security to a password-protected controller.
	Note that the LCD Password option works differently in FRN 21.000 or later.
	You need RSLogix 500 or RSLogix Micro software, version 11 or later, for this enhancement.
	For more information, see the MicroLogix 1400 Programmable Controllers User Manual, publication 1766-UM001.

Enhancement for FRN 16.0 (Series B only)

Enhancement	Description
Default user name can be changed	Default user names (*administrator* and *guest*) in the web server can be changed through the User Management page.
Default CIP Inactivity Timeout	To comply with ODVA CT13 standards, the default CIP Encapsulation Inactivity Timeout of 120 seconds is introduced.

Enhancement for FRN 15.5 (Series B only)

Enhancement	Description
Improved behavior to set IIN1.7 restart bit	Users can select the option for the IIN1.7 restart bit to be set and sent: • Immediately after channel configuration, program download, or at power cycle. • At power cycle only.
Improved behavior for DNP3 Hold Time after Events	Users can select the option for the DNP3 hold-timer to: • Re-trigger for each new event detected (increased possibility of capturing all the changes in a single response). • Not re-trigger (giving the master a guaranteed update time).

Enhancement for FRN 15.3 (Series B only)

Enhancement	Description
Notification to change default administrator account password	To enhance web server security, upon logging in to the MicroLogix 1400 Web Server page with the default administrator account and default password, a warning displays to notify the user to change the default password.

Enhancement for FRN 15 (Series B only)

Enhancement	Description
LCD menu option for Modbus RTU Slave node address modification	The user can modify the Modbus RTU Slave node address through the LCD Menu under Advanced Set option. You need to power cycle the controller for the change to take effect.

Enhancements for FRN 12 (Series B only)

Enhancement	Description
I/O Force Protection	To enable/disable I/O Force settings, users can access the Status File in binary mode to SET/CLEAR bit S:1/5.
DNP3 Event Restore	DNP3 generated events can be restored after a power cycle.
DNP3 unsolicited channel switching through Ladder Program	Users can change DNP3 unsolicited channel run time using 485CIF write MSG instruction.

Enhancements for FRN 11 (Series B only)

Enhancement	Description
Timeout for Register Session/Reply message exchange cycle	Adds a timeout for the Register Session Request/Reply message exchange cycle when a Register Reply packet is not received within the specified time. The Inactivity timeout value that is configured through the RSLogix 500 software is used as the packet timeout value, with a default value of 30 minutes.
Improved Web Server security	If the controller receives two consecutive invalid authentication requests from any http client, the controller resets the Authentication Counter after 60 minutes. If the controller receives 10 invalid authentication request from any HTTP client, it will not accept any valid or invalid Authentication packets until a 24-hour HTTP Server Lock Timer timeout.

Enhancements for FRN 10 (Series B only)

Enhancement	Description
Support for DNP3 over Ethernet	Adds support for DNP3 TCP Server features over Ethernet and DNP3 TCP Client/UDP features to support unsolicited response message to a DNP3 Master station.
Support for Modbus over Ethernet	Adds support for Modbus TCP Server and Modbus TCP Client.

Enhancement for FRN 7 (Series A only)

Enhancement	Description
Improved Web Server security	If the controller receives two consecutive invalid authentication requests from any http client, the controller resets the Authentication Counter after 60 minutes.
	If the controller receives 10 invalid authentication request from any HTTP client, it will not accept any valid or invalid Authentication packets until a 24-hour HTTP Server Lock Timer timeout.

Enhancement for FRN 6 (Series A only)

Enhancement	Description
Timeout for Register Session/Reply message exchange cycle	Adds a timeout for the Register Session Request/Reply message exchange cycle when a Register Reply packet is not received in time. The Inactivity timeout value that is configured through the RSLogix 500 software is used as the packet timeout value, with a default value of 30 minutes.

Enhancement for FRN 5 (Series A only)

Enhancement	Description
Updated baud rate configuration	Updated baud rate configuration to MCF UART controller for greater accuracy.

Enhancement for FRN 4 (Series A only)

Enhancement	Description
Support for Connection Manager object in CIP subsystem	Adds instances and attributes for Connection Manager objects.

Corrected Anomalies

Corrected Anomalies for FRN 21.005 (Series B and Series C only)

Anomaly	Description
Controller faults with error code 7h when restoring a program from the memory module.	When restoring a program from the memory module, a message "Program in processor changed causing offline state." appears and the controller faults with error code 7h (Memory Module Transfer Error). This occurs when any floating point data file contains 38 or more elements.

Corrected Anomalies for FRN 21.004 (Series B and Series C only)

Anomaly	Description
User fault routine does not trigger when a xx79h non-recoverable fault occurs	The solution in this firmware now correctly triggers the user fault routine when a xx79h non-recoverable fault occurs.
Security vulnerabilities	This firmware revision addresses multiple security vulnerabilities. These vulnerabilities may affect the availability and/or integrity of these products and the data they transfer. An affected product requires manual intervention to recover. For more information on the vulnerabilities and the recommended mitigations, log on to the Rockwell Automation® Support Center at https://rockwellautomation.custhelp.com/app/home/ and search the Knowledgebase for Answer ID 1072942.

Corrected Anomalies for FRN 21.003 (Series B and Series C only)

Anomaly	Description
Modbus TCP server may be busy in an in error condition	The solution in this firmware revision resolves this anomaly. For more information on the vulnerabilities and the recommended mitigations, log on to the Rockwell Automation Support Center at https://rockwellautomation.custhelp.com/app/home/ and search the Knowledgebase for Answer ID 1067316.

Corrected Anomalies for FRN 21.002 (Series B and Series C only)

Anomaly	Description
Program is no longer password protected after being transferred, using a memory module, to a new controller with FRN 21	When the memory module is configured for "Load Memory Module Always" or "Load Memory Module on Memory Error" with an 'Enhanced Password Security' controller file that is password protected, and is installed in a new out-of-box controller with FRN 21, the program transfers but the controller password does not. This causes the program to no longer be password protected.
Unable to communicate with a password protected controller using MSG instructions	When the 'Enhanced Password Security' controller is password protected, communication through MSG instructions using the PLC-5® and 485CIF protocols is blocked.

Corrected Anomalies for FRN 16.002 (Series B only)

Anomaly	Description
DNP3 Serial Port Lock-up	The solution in this firmware revision resolves the serial link lock-up that is caused by a bad CRC packet.
DNP3 Short Floating Point Analog Output Object Write Errors	The solution in this firmware revision resolves the error when writing a Short Floating Point Analog Output Object if there is only a 16-bit Analog Output Object file configured.

Corrected Anomalies for FRN 16.001 (Series B only)

Anomaly	Description
Security vulnerabilities	This firmware revision addresses multiple security vulnerabilities.
	These vulnerabilities may affect the availability and/or integrity of these products and the data they transfer.
	An affected product requires manual intervention to recover.
	For more information on the vulnerabilities and the recommended mitigations, log on to the Rockwell Automation Support Center at https://rockwellautomation.custhelp.com/app/home/ and search the Knowledgebase for Answer ID 968962.
Unable to edit webserver administrator password if administrator is sole user in system	The Edit button on the User Management page is disabled if there is only one user with Administrator access in the system. Therefore the user cannot edit the user name and/or password.
	The solution in this firmware revision resolves the technical note with Knowledgebase Answer ID 998264.
TCP Reset response not sent when socket inactivity timeout expires	The solution in this firmware revision now sends the TCP Reset response correctly when socket inactivity timeout expires.

Corrected Anomalies for FRN 16.0 (Series B only)

Anomaly	Description
Security vulnerabilities	This firmware revision addresses multiple security vulnerabilities.
	These vulnerabilities may affect the availability and/or integrity of these products and the data they transfer.
	An affected product requires manual intervention to recover.
	For more information on the vulnerabilities and the recommended mitigations, log on to the Rockwell Automation Support Center at https://rockwellautomation.custhelp.com/app/home/ and search the Knowledgebase for Answer ID 968962.
Interrupt files not executed in MCR zone	User interrupts (EII, HSC, and STI) may not be executed if MCR zones are present in the ladder program.
Hard fault 08h during online edit	Editing the same rung more than once within a user program with LBL and JMP instructions may result in a 08h hard fault.
Controller loses communication with UPS when network module is replaced	The controller loses Modbus TCP connection and fails to re-establish connection with the UPS when the network module is replaced in the UPS. This is because ARP does not initiate after 300 seconds communication error timeout with new device MAC ID.

Corrected Anomalies for FRN 15.4 (Series B only)

Anomaly	Description
Remote Code Execution through Stack-based Buffer Overflow security vulnerability	This firmware revision addresses security vulnerability #1, as detailed further in Knowledgebase article KB732399.
	In addition to updating the product to this new firmware revision, KB732398 includes additional mitigations that may further protect your product. These mitigations should be evaluated, and if applicable, applied to your product installation and environment.
	For more information, log on to the Rockwell Automation Support Center at https://rockwellautomation.custhelp.com/app/home/ and search the Knowledgebase for Answer ID 732399 and 732398.

Corrected Anomalies for FRN 15.3 (Series B only)

Anomaly	Description
Multiple security vulnerabilities	This firmware revision addresses five of the six security vulnerabilities of varying severity, as detailed further in Knowledgebase article KB732399.
	In addition to updating the product to this new firmware revision, KB732398 includes additional mitigations that may further protect your product. These mitigations should be evaluated, and if applicable, applied to your product installation and environment.
	For more information, log on to the Rockwell Automation Support Center at https://rockwellautomation.custhelp.com/app/home/ and search the Knowledgebase for Answer ID 732399 and 732398.

Corrected Anomalies for FRN 15.2 (Series B only)

Anomaly	Description
In DHCP mode, the IP address cannot be configured in a network with more than three DNS servers.	The solution included in this firmware revision enables IP address configuration in DHCP mode when there are more than three DNS servers in the network.
Input word I1:7.0 does not appear in Web Server Data Views page.	The solution included in this firmware revision corrects the issue where the input word I1:7.0 was being skipped on the Web Server Data Views page.
High-Speed Counter (HSC) preset interrupt bits HPI and LPI do not always turn on when expected.	The solution included in this firmware revision corrects the inconsistent operation of the HSC preset interrupt bits HPI and LPI.
The controller broadcasts ARP packets even when the Duplicate IP Address Detection function is disabled.	The solution included in this firmware revision stops the controller from broadcasting ARP packets to detect if there is another device on the network with the same IP address, when the Duplicate IP Address Detection function is disabled.
CIP Generic MSG instruction faults with a 21H error.	The solution included in this firmware revision addresses an issue in the CIP Generic MSG setup that changes LOCAL setting to REMOTE (which is not accessible from the user interface), causing the 21H error.

Corrected Anomaly for FRN 15.1 (Series B only)

Anomaly	Description
MLX1400 DNP3 command input validation improvement	The solution included in this firmware revision improves the DNP3 parser mechanism to handle the malformed packets received on the Ethernet network.

Corrected Anomalies for FRN 15 (Series B only)

Anomaly	Description
Processor memory can be cleared using the RSLogix 500 software	The solution included in this firmware revision no longer allows you to select the option to clear the processor memory in FRN 15 and later.
LCD displays invalid characters at a certain button sequence	LCD displays invalid characters when the user presses the left or right button, while the cursor position is on the LCD Setup.
DNP3 TCP communication not responding under congested network	DNP3 through Ethernet communication does not get restored when network is congested.
Negative values are accepted for the Timer file.	The solution included in this firmware revision no longer allows negative values for the ACC and PRE fields of the Timer file, through the RSLogix 500 software or any Human Machine Interface connected to the controller.

Corrected Anomalies for FRN 14.2 (Series B only)

Anomaly	Description
CIP Generic Messaging: Hard Fault 08h error in Socket Object	Controller goes into fault mode when attempting to write to a socket and the Read Timeout Interrupt occurs.
Unable to set IP address using 169.254.XXX.XXX range	Controller does not allow the user to set the static IP address in the range of 169.254.XXX.XXX and reports a port configuration error.

Corrected Anomalies for FRN 14 (Series B only)

Anomaly	Description
Status file vulnerabilities: • S2:1/13 • S2:3/8-15 • S2:5/0 • S2:5/2 • S2:5/3	Status file bits (S2:1/13, S2:5/0, S2:5/2, S2:5/3) and watch dog bits (S2:3/8-15) were writable through communication messages which allowed the possibility to force the controller to go into fault. The solution included in this firmware revision allows users to CLEAR these bits (S2:1/13, S2:5/0, S2:5/2, S2:5/3) but does NOT allow them to SET using Communication messages. The watch dog bits (S2:3/8-15) will be Read Only in non-transfer mode.
Hard Fault 08h error in Serial Modbus Slave	Controller goes into fault when a character is received before an inter-frame delay by Modbus slave over serial link.
DNP3 static data not reported	DNP3 static data is not reported if integrity poll is issued in the middle of unsolicited response.
DNP3 TCP connection not restored over congested network	DNP3 TCP connection does not get restored when network is congested or network undergoes frequent cable break.
DNP3 Secure Authentication: Slave is sending same response even if master has replied with confirmation	When a CONFIRM function code is configured as critical and aggressive mode is enabled, the controller may, at times, send the same response.
Invalid error when DNP3 Data-Set™ is configured with Data type: NONE	When a descriptor is configured with data type: NONE, the response of Data-Set Read (g87v1) is not completely received. The Configuration Corrupt bit is also set.
DNP3 Data-Set: 32b frozen counter event is generated even if it is not configured for event	When analog point is configured for an event occurrence condition, Data-Set Events is also generated for 32b frozen counter.
DNP3 Data-Set: Data-Set Events is generated even if the EV bit is reset	Dataset events are generated even if EV bit of descriptor characteristics is reset (OFF).
Failure to release IP address, when IP address conflict is detected	Firmware Revision 14 implements the recommended IP Address Collision Detection algorithm and duplicate IP address policy, in accordance with CIP vol2, Ed3.12.

Corrected Anomalies for FRN 13 (Series B only)

Anomaly	Description
CIP Generic Message Error	When a CIP generic MSG instruction is executed to certain devices, the response may be incompatible with the expected response in the controller.
DNP3 Slave does not respond properly to back up DNP3 Master	DNP3 Slave always sends unsolicited responses to First master IP and node address. If First master does not exist or communicate with Slave, the Slave never sends the confirmation. During unsolicited confirmation time, if Slave receives read request from backup master (other than first node address), it always replies back to first node address.
DNP3 events are getting cleared even if confirmation is not received	DNP3 Slave does not push back events into event buffer in the following conditions: 1. During solicited confirmation time, if Slave receives any broadcast message or any other request or same request instead of confirmation. 2. During unsolicited confirmation time, if device receives read request and confirmation timer timeout.
Force LED misbehavior	This is a known anomaly on FRN 12. When all forces are removed through RSLogix 500, Force LED does not turn OFF and Forces Installed bit (S:1/6) is not reset.
Hard Fault 08h error	This is a known anomaly on FRN 12. Device goes into hard fault when FRN12.1-OS boots up for the first time. This anomaly occurs when the device tries to restore DNP3 events. It may also happen when the battery is removed or damaged.

Corrected Anomalies for FRN 12 (Series B only)

Anomaly	Description
Hard fault 08h on DNP3	When channel 0/1/2 is configured as DNP3, 08h hard fault error occurs due to a DNP3 application buffer overflow.
DNP3 Application Layer lockup	Device stops responding to DNP3 read request when the event buffer is full. Device does not fail to respond to any other DNP3 request types except read requests.
DNP3 Data Link Layer lockup	When Channel 2 is configured for DNP3, with communication channel status file CS2:17 having Link Layer Error Code 1, the device does not respond to any external requests from the DNP3 master nor transmit any unsolicited event data.
DNP3 Slave sends a response on only the first 120 events of respective class poll	The device does not send all the DNP3 class 1, 2, 3 events in one solicited response but sets respective Internal Indication (IIN bits) bits to indicate that respective class events are available so that the Master can poll again until the events are finished.
Hard fault 08h on DF1	An 08h hard fault error occurs when channel 2 is configured for DF1 full-duplex.
Modbus TCP UID and MSG anomalies	A responding MicroLogix 1400 controller sends an improperly formatted Modbus packet (with no data included) after it receives Unit Identifier with 0 value in the command packet. When the initiating MicroLogix 1400 controller receives the improperly formatted response, it sets the MSG Done bit, instead of the MSG Error bit.

Corrected Anomalies for FRN 11 (Series B only)

Anomaly	Description
DNP3 Cold Restart does not execute	DNP3 Cold Restart command is not executed when controller is in Run mode.
Ch0 does not respond when configured for DF1 Radio Modem protocol	After being configured for DF1 Radio Modem protocol, channel 0 becomes unresponsive after running for some time.
Ch1 goes to 'Lock-up' state	The controller locks channel 1 when it is configured as any of the following configurations in RSLogix 500 software, and then power cycled: - Static IP Address, - Select DNP3 over IP Enable, - End Point Type selected as "Datagram Only", - Master IP0 (apart from 0.0.0.0), - Master UDP Port Number (Init Unsol) [apart from 0] - Select "Send Init. Unsol. Null Resp. on Reset"
Controller restarts when invalid user name and password entered	The controller restarts unexpectedly when an invalid user name and password is used several times to access the Web Server Administrative settings.
Web Server lockout message does not appear on some browsers	When the Web Server is in a locked state, the "Web Server is locked. Contact Administrator" message does not appear on these browsers: • IE8 • Opera 11.1
DNP3 channel 1 locks up	The DNP3 channel 1 locks up when the Ethernet cable is pulled out for 24 hours and the SCADA initiates a poll for class 0/1/2/3 data, and if the application layer max response size has been configured to 2048.

Corrected Anomalies for FRN 7 (Series A only)

Anomaly	Description
Ch0 does not respond when configured for DF1 Radio Modem protocol	After being configured DF1 Radio Modem protocol, channel 0 becomes unresponsive after running for some time.
Controllers restarts when invalid user name and password entered	The controller restarts unexpectedly when an invalid user name and password is used several times to access the Web Server Administrative settings.
Web Server lockout message does not appear on some browsers	When the webserver is in a locked state, the "Web Server is locked. Contact Administrator" message does not appear on these browsers: • IE8 • Opera 11.1

Corrected Anomalies for FRN 6 (Series A only)

Anomaly	Description
Up to 10 minutes taken to successfully set up Ethernet communication after power cycle	When a CompactLogix™ controller messages a MicroLogix 1400 controller over Ethernet, and the MicroLogix 1400 controller is power cycled, it can take up to 10 minutes to successfully set up Ethernet communication.
No unsolicited response sent at power up	DNP3 slave unsolicited message is not sent at power up when option is enabled.
Data log record lost	During data logging, the transmitted record is deleted without a check for successful transmission.
08h Hard Fault in RUN mode	With indirect addressing, the controller generates a 08h Hard Fault instead of a 29h fault while in RUN mode.
AWT, AWA instruction does not work correctly for Channel 2	Due to a defect in Channel 2 ASCII driver initialization, AWT, AWA instructions may not work correctly for Channel 2.
Logged records lost when restoring from the Memory module	Restoring overflowed data log records from the Memory module was unsuccessful, and data log records were lost.

Corrected Anomalies for FRN 6 (Series A only)

Anomaly	Description
Residual data logs not cleared	Fixed defect for Data Log Auto-Load sequence at power-up. Data logs are not cleared when there is a new ladder program in the controller.
LCD contrast not adjustable	Pressing the ESC+Up or ESC+Down keys does not adjust LCD contrast.
Data log timer does not reset	Data log timer does not reset when a new user program is downloaded.

Corrected Anomalies for FRN 5 (Series A only)

Anomaly	Description
Web Server Password Error	An error occurs when attempting to change the administrator password in Web Server.
Serial Baud Rate	Poor accuracy of serial baud rate occurs at higher speeds.
Hard Fault 08h in Serial Communication	Hard Fault 08h fault error occurs when channel 0 and/or 2 are configured for DF1 Half-duplex Slave, Modbus RTU Slave or ASCII.
Data file protection error	Data file protection does not work as documented when the memory module is configured to transfer program at power-up.
Hard Fault 08h in Ethernet Channel Configuration	Hard fault 08h occurs when the Ethernet cable is plugged in after power cycle.
Subnet mask LCD display error	When the gateway address is configured as all zeroes, the LCD displays the gateway address as 255.255.255.0.
Gateway address LCD display error	When the subnet mask is configured as all zeroes, the LCD displays the subnet mask as aaa.bbb.ccc.1, where aaa.bbb.ccc represents the first three octets of the IP address.
Pre-transmit delay error in Serial communication	Pre-transmit delays greater than 6553 ms do not work properly in DF1 Half-duplex Master, Modbus RTU Master and Modbus RTU Slave drivers.
33h fault in FFL/FFU/LFL/LFU	A 33h fault occurs when FIFO/LIFO instructions are programmed and data table memory words used are greater than 5 K.
LCD:0/WND bit error	LCD:0/WND bit remains set even though the LCD has switched to the I/O Status screen when the user input time expires within the User Display.

Corrected Anomalies for FRN 5 (Series A only)

Anomaly	Description
IP address detection non-conformance	Duplicate IP address detection does not match ODVA guidelines.
3Bh fault with PTO error 4	A 3Bh fault ("PTO error") with PTO error=4 ("Accel/Decel error") occurs due to an underestimation of the S-curve limit for PTO Accel/Decel pulses.
Invalid operation in "Store to MM/Load from MM" in LCD display	Issues with Memory Module transfers occur when initiated through the LCD display.
02h hard fault with power cycle	A 02h hard fault occurs due to multiple power fail interrupts being accepted.
DNP3 timestamp error	DNP3 timestamp is off by a day after power-up and before being synchronized with the DNP3 master time.
Embedded analog input freeze	Embedded analog input values "freeze", requiring a power cycle to recover.
Incorrect attribute 9 in Connection Manager Object of CIP	The number of Connection entry information (attribute 9) for Connection Manager Object in Ethernet subsystem does not display properly.

Corrected Anomalies for FRN 4 (Series A only)

Anomaly	Description
71h fault with I/O expansion modules	Under the following conditions, a 71h fault may occur within a few minutes: • a 1762-OF4 (Series A, Revision B/C) or 1762-IF2OF2 (Series A, Revision D/E) expansion module is used, and • scantime hits less than approximately 390 ìs (usually when user ladder program is empty).
MSG instruction for socket interface message	Open Connection message sometimes does not work correctly with the error code 17DEh when the configured buffer size is larger than transmitted data.
Error in generating DNP3 events in DNP 3 protocol	User Manual states that Binary file 3 can be used for Binary Input, Double Binary Input and Binary Output objects. However, events were not generated when Binary file 3 was configured for these 3 objects.

Corrected Anomalies for FRN 4 (Series A only)

Anomaly	Description
Error in behavior of Internal Indication bits IIN1.1 to IIN1.3 in DNP 3 protocol	In response to a request, when events are contained in the response and no more events exist to be reported in the controller, IIN1…1IIN1.3 are cleared. When the master sends Read request only for the static object, the bits were not turned on in the response IIN correctly, although there are some events logged. If the master sends a request other than a Read, the bits were not turned on in the response IIN correctly although there are some events logged.
Occurrence of DNP3 Link Layer Error Code in DNP 3 protocol	Under a DNP3 Full-Duplex environment, a Link Layer Error Code 8 (UNKNOWN_CHAR) in the Link Layer Diagnostic counter of the Channel Status file may occur.
Error in DNP3 file object in DNP 3 protocol	When the data file size in a user program is too big, the user program is not downloaded over the DNP3 protocol.
Default Variation for Double Bit Binary Input Event object in DNP 3 protocol	The returned object/variation was g4v2. It should be g4v3 to be consistent with Binary Input Event object (g2v3).
Error in event flush in DNP 3 protocol	The logged events were not cleared correctly when the master sent a request to read the specific event object(s) and the class level was configured to 1.
Error in event reporting in DNP 3 protocol	Logged events were not reported when the master sent a request to read the specific event object(s) and the class is configured to Class 2 or 3 (other than 1).
Error in multi-fragment response processing in DNP 3 protocol	When a master's Read request contains several objects and the response is made into multi-fragments, the response was not processed correctly.
Error in behavior of unsolicited responses in DNP 3 protocol	The controller may send NULL unsolicited responses if there are many events logged and they are reported to the master.

Additional Resources

This document contains additional information concerning related Rockwell Automation products.

Resource	Description
MicroLogix 1400 Programmable Controllers Installation Instructions, publication 1766-IN001.	Contains information on mounting and wiring the MicroLogix 1400 Programmable Controller, including a mounting template and door labels.
MicroLogix 1400 Programmable Controllers User Manual, publication 1766-UM001.	Contains detailed information on planning, mounting, wiring, and troubleshooting your MicroLogix 1400 system.
MicroLogix 1400 Programmable Controllers Web Server User Manual, 1766-UM002.	Contains information on MicroLogix 1400 embedded web server capability.
MicroLogix 1400 Programmable Controllers Instruction Set Reference Manual, publication 1766-RM001.	Contains instruction sets and other information specific to 1766 controllers.

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support/, you can find technical manuals, a knowledge base of FAQs, technical and application notes, sample code and links to software service packs, and a MySupport feature that you can customize to make the best use of these tools.

For an additional level of technical phone support for installation, configuration, and troubleshooting, we offer TechConnect support programs. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/support/.

Installation Assistance

If you experience a problem within the first 24 hours of installation, please review the information that's contained in this manual. You can also contact a special Customer Support number for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/support/americas/phone_en.html, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

www.rockwellautomation.com