Allen-Bradley

MicroLogix 1100 Programmable Controllers FRN 15.2

Catalog Numbers 1763-L16AWA, 1763-L16BWA, 1763-L16BBB, 1763-L16DWD

About This Publication

Read this document before using MicroLogix™ 1100 controllers with Series B FRN 15.2 operating system firmware. Keep this document with your MicroLogix 1100 Programmable Controllers Instruction Set Reference Manual, publication number 1763-RM001.

IMPORTANT RSLogix 500/RSLogix Micro software version 8.10 or later is required to program the new functionality in MicroLogix 1100 Series B controllers FRN 15.2.

Enhancements

Enhancement with Firmware Revision 15

Enhancement	Description
Notification to change default Administrator account password	To enhance web server security, upon logging in to the MicroLogix 1100 Web Server page with the default Administrator account and default password, a warning page displays to notify the user to change the default password.

Enhancement with Firmware Revision 14

Enhancement	Description
I/O Force Protection	To enable/disable I/O Force settings, you can access the Status file in the binary mode to SET/CLEAR bit S:1/5.

Enhancements with Firmware Revision 10

Enhancement	Description
Timeout for Register Session/Reply message exchange cycle	Added 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.
Sending a Forward Close command to close the CIP connection prior to sending the Unregister session command	In previous implementations, CIP connection is automatically closed in the controller without transmitting out a Forward Close command after transmitting/receiving an Unregister Session command.
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 requests from any HTTP client, it will not accept any valid or invalid Authentication packets until a 24-hour HTTP Server Lock Timer timeout.

Enhancements with Firmware Revision 6

Enhancement	Description
User-defined web server packet timeout.	Changed Web server packet timeout from 1 sec (fixed) to a configurable value, which can be adjusted by changing the MSG Reply Timeout setting in Ethernet Channel Configuration.
Removed RTC access from Web server subsystem.	This change improves the system timer robustness and improves process time. After the change, the RTC value with the Web server is read from System status file, not directly from the RTC module.
Changed the maximum number of pending connections from 5 to 20 for Ethernet channels.	The Web Server sub-system supports just one connection at any one time. If many connection requests are received (SYN commands), the Web Server sub-system can preserve the connection requests. With a normal Web client, the connection requests cannot exceed 15.
Reduced maximum scan time when the Web server is connected to client.	When there is high communication traffic between the Web server and client, the Web server service is paused periodically to let the Ladder run.
Improved Web server performance for cellular modem connection.	
Modified Web server connection handling, and combined segmented HTML packets in the data view page.	
Simplified the data transfer through the Ethernet channel, and improved the firmware robustness.	Changed delay time from reply timeout to no wait for sending packets and disconnecting socket. Changed delay time from wait forever to reply timeout when allocating packets.
Added the Reply to List Servers command for UDP ports.	
Improved system recovery and maintenance.	MSG errors are reported when the Ethernet buffer overflows, instead of generating a Hard Fault.

Enhancements with Firmware Revision 5

Enhancement	Description
Improved handling for online editing errors.	DMA transfer errors during online editing no longer result in a hard fault, but an OLE error instead.
Reduced the system Interrupt delay for some instances.	In some instances, a long interrupt delay is caused while issuing an instruction to enable HSC, STI, or EII functions.

Corrected Anomalies

Corrected Anomalies in Firmware Revision 15.2

Anomaly	Description
Buffer overflow security vulnerability	This firmware revision addresses the security vulnerability detailed in Knowledgebase article KB765050. 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.

Corrected Anomalies in Firmware Revision 15

Anomaly	Description
Multiple Security Vulnerabilities	This firmware revision addresses 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.

Corrected Anomalies in Firmware Revision 14

Anomaly	Description
Negative values are accepted in 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.
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 14 and later.

Corrected Anomaly in Firmware Revision 13

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.

Corrected Anomalies in Firmware Revision 12

Anomaly	Description
BOOTP Error	This anomaly was introduced in FRN 11. If user configures static IP address and unchecks BOOTP and DHCP Enable, controller will still send out BOOTP requests after a power cycle. If a BOOTP/DHCP server responds to the request, the controller will use the new IP address instead of the statically configured address.
Hard Fault 08h on DF1	When channel 0 is configured for DF1 Full Duplex, a sequence of communication events occur resulting in the 8h Hard Fault and controller memory clear.
CIP generic Message Error	When a CIP generic MSG instruction is executed to certain third party devices, they may respond in a way that the controller does not expect, resulting in a MSG instruction timeout error.

Corrected Anomalies in Firmware Revision 11

Anomaly	Description
Unable to display firmware revision in RSLinx	User is unable to read the firmware information using the RSLinx software.
Update System Information display on controller LCD	Due to a limitation of the LCD, the system information display is modified: • OS FRN appears as OSFRN • BT FRN appears as BTFRN
Hard Fault in Ethernet Channel Configuration	Under the following case, the controller causes Hard Fault 8h: 1. Set Ethernet configuration to BOOTP or DHCP. 2. Disconnect Ethernet cable. 3. Power-cycle. 4. Change IP address to static IP through Serial communication. 5. Connect Ethernet cable. This controller causes 8h fault.

Corrected Anomalies in Firmware Revision 10

Anomaly	Description
Controller restarts when invalid user name and password entered	The controller restarts unexpectedly when an invalid user name and password are entered 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 the following browsers: • IE8 • Opera 11.1

Corrected Anomalies in Firmware Revision 9

Anomaly	Description
Fragmentation 2h fault	This anomaly is observed when MicroLogix 1100 receives large data packets.
Ethernet packet loss	During ARP aging, packets are dropped when the physical mapping with IP and MAC address is absent for a packet that has just arrived.
Packet loss in BOOTP port for invalid packets.	If some invalid BOOTP reply packets are received by MicroLogix 1100, the Ethernet buffer corresponding to its socket port will be locked.
Ethernet I/P list identity request	The Sender's Context field was truncated in the reply packet of a list identity request. The Sender's Context field is fixed for the following: • List Identity Request • List Interface Request • List Server Request • List Services Request • UCMM respond register session • UCMM Connected Object response

Corrected Anomalies in Firmware Revision 8

Anomaly	Description
User Memory Clear 02H fault	This anomaly is observed when Modbus master protocol is selected for MicroLogix 1100 Channel 0, and high speed STI (1ms) is implemented.
DF1 command reply	There is a failure in the reply DF1 command when an ASCII write instruction is executed in the ladder program.
SMTP email server re-connection	With regards to message instruction, MicroLogix 1100 may be used as an SMTP client. If the SMTP server is killed by the user or by Microsoft Windows, and after Windows sends an RST packet, MicroLogix 1100 does not detect it, and error 5DD is detected. In such a case, there is no way of clearing it except by cycling power to the processor.
SCP math instruction	Fixed the SCP math Indirect Addressing anomaly.

Corrected Anomalies in Firmware Revision 7

Anomaly	Description
MicroLogix 1100 goes to fault mode and user program is cleared.	This anomaly may occur during online editing through Ethernet/IP port, when you use a SVC instruction inside the application.

Corrected Anomalies in Firmware Revision 6

Anomaly	Description
Ethernet port locks up.	This anomaly may occur when Ethernet communication traffic is heavy. The Ethernet data transmission can stop due to internal Ethernet buffer overflow.
Receiving invalid packets causes a hard fault.	When invalid packets are received over the Ethernet channel, a buffer overflow and hard fault may occur. Invalid packets are now ignored.
The reply to an NOP command was generated on the UDP port.	The reply to an NOP command should not be generated on both TCP and UDP ports.
Ethernet buffer overflow.	The outside inbound socket is closed after sending request to the controller. In FRN 5, this may cause an Ethernet buffer overflow. This is fixed by prompt Ethernet buffer release for such connections.
02h hard fault or 22h user watchdog fault for consecutive broadcast messages received.	When the consecutive broadcast messages are received, the high frequency of Ethernet data packet processes may limit the time available for the ladder program to run. This may cause the user watchdog fault or even a hard fault. This is fixed by reducing frequency of the Ethernet data receiving process.

Additional Resources

This document contains additional information concerning related Rockwell Automation products.

Resource	Description
MicroLogix 1100 Programmable Controllers Instruction Set Reference Manual, publication 1763-RM001.	Contains instruction sets and other information specific to 1763 controllers.

Notes:

Notes:

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/.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1763-RN003K-EN-P - January 2016
Supersedes Publication 1763-RN003J-EN-P - October 2015